



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



ANNUAL REPORT 2019

DOCUMENT 7:1 (2019–2020)



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 2019 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Security Act, the issuer decides whether or not information is classified. Before the report is submitted to the Storting, we send the relevant sections of the report to each of the respective services for them to clarify whether the report complies with this requirement. The services have also been given the opportunity to check that there are no factual errors or misunderstandings.

Oslo, 31 March 2020


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 during the last six months of 2019: 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

1.	The Committee's remit and composition	6
2.	Overview of the Committee's activities in 2019	9
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	11
3.	Developments, framework conditions and international oversight cooperation	12
3.1	About the resource situation in the EOS Committee's secretariat	13
3.2	International oversight cooperation	13
3.3	Cooperation with the Communications Surveillance Control Committee	14
4.	The Committee's consultation submissions	15
4.1	Introduction	16
4.2	Consultation submission on lawful interception of communication in emergencies	16
5.	The EOS Committee is investigating the Frode Berg case	16
6.	The Norwegian Police Security Service (PST)	17
6.1	General information about the oversight	18
6.2	PST's registration of members of the Storting	18
6.2.1	Introduction	18
6.2.2	PST's explanation to the Committee	18
6.2.3	Legal basis	18
6.2.4	The Committee's assessment	19
6.2.5	Follow-up of the Committee's criticism	19
6.3	Registration of a journalist	20
6.4	Storage of documents at PST's premises in Møre og Romsdal	20
6.5	Follow-up of PST's disclosure of information for use in security clearance cases	20
6.6	About the special report on PST and information about airline passengers	20
6.7	Non-conformity report from PST	21
6.8	Complaint cases against PST	21
7.	The Norwegian Intelligence Service (NIS)	22
7.1	General information about the oversight	23
7.2	The NIS omitted to inform the Committee about a counterterrorism tool	23
7.3	National control over Norwegian intelligence information	24
7.4	Intelligence cooperation with states with human rights challenges	25
7.5	Differences between how PST and the NIS process information about deceased persons	26
7.6	Obligation to keep a list of Norwegian persons about whom the NIS is collecting information abroad	27
7.7	Cooperation between PST and the NIS and information collection from open sources	27
7.8	Complaint cases against the NIS	28
8.	The National Security Authority (NSM)	29
8.1	General information about the oversight	30
8.2	Investigation into security interviews in NSM and FSA	30
8.3	Follow-up of the special report on differing practices in security clearance cases	31

8.4	Complaint cases	32
8.4.1	Introduction	32
8.4.2	Complaint case 1 – Invalid decision to refuse security clearance on grounds of inadequate elucidation of the case	32
8.4.3	Complaint case 2 – Inadequate grounds to the principal person in a security clearance case	32
8.5	Case processing times in security clearance cases	33
9.	The Norwegian Defence Security Department (FSA)	34
9.1	General information about the oversight	35
9.2	Follow-up of the special report on differing practices in security clearance cases	35
9.3	The use of written statements from persons for whom security clearance is applied for to elucidate security clearance cases	35
9.3.1	General information	35
9.3.2	Criticism in a specific case	37
9.4	Complaint cases against FSA	37
9.4.1	Introduction	37
9.4.2	Long case processing time	37
9.4.3	FSA's handling of a request for access to documents in a complaint case concerning security clearance	37
9.5	Case processing times in security clearance cases	38
10.	Oversight of other EOS services	39
10.1	General information about the oversight	40
10.2	Inspection of the Army Intelligence Battalion	40
10.3	Inspection of the Norwegian Naval Special Operations Commando - MJK	40
10.4	Technical equipment on loan from the Norwegian Special Operation Forces to PST	40
10.5	The Norwegian Civil Security Clearance Authority (SKM)	41
10.5.1	Inspection	41
10.5.2	Case processing times in security clearance cases	41
10.6	Follow-up of inspection of the Office of the Auditor General of Norway	42
11.	Communication and external relations in 2019	43
11.1	Introduction	44
11.2	External relations	44
11.3	Nordic meeting for oversight bodies	44
11.4	The EOS Committee's annual conference	44
12.	Appendices	45
	Appendix 1 – Meetings, visits, lectures and participation in conferences etc.	46
	Appendix 2 – News from foreign oversight bodies	48
	Appendix 3 – Report on the security interviews project	49
	Appendix 4 – Consultation submission on lawful interception of communication in emergencies	54
	Appendix 5 - Signed charter for the Intelligence Oversight Working Group	56
	Appendix 6 – Letters to and from the Ministry of Justice and Public Security and the Ministry of Defence concerning sharing of information with other oversight bodies	59
	Appendix 7 – Act relating to oversight of intelligence, surveillance and security services	72

The background of the slide features a blurred image of a person in a dark suit standing in a modern office environment. A semi-transparent blue overlay covers the entire image. Overlaid on this is a network diagram consisting of several circular nodes connected by thin white lines, creating a web-like structure across the right and bottom portions of the slide.

1.

The Committee's remit and composition

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

Pursuant to the Oversight Act² 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 the oversight purposes,³ and shall insofar as possible show consideration for 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 the services' current activities.

The Committee may not instruct the EOS services it oversees or be used by them for consultations 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.⁴

The Committee conducts reviews of legality. This means that we do not review the services' effectiveness, how they prioritise their resources etc.

The Committee has seven members. They are elected by the Storting in plenary session on the recommendation of the Storting's Presidium for terms of up to five years.⁵ No deputy members are appointed. Following a statutory amendment in 2017, the members may be re-appointed once and hold office for a maximum of ten years.

The Committee is independent of both the Storting and the Government.⁶ 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 the highest level of security clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory.⁷ This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET, respectively.

- 1 References to the Oversight Act are found in the Act relating to National Security (the Security Act) Section 11-1, Act No 11 relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 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 2017.
- 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 for a special procedure to 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 by 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 cooperating foreign services. In 2013, the EOS Committee asked the Storting to clarify whether the Committee's right of inspection as enshrined in the Act and Directive shall apply in full also in relation to the Norwegian Intelligence Service, or if the Storting's decision from 1999 shall be upheld. At the request of the Storting, this matter was considered in the report of the Evaluation Committee for the EOS Committee, submitted to the Storting on 29 February 2016, see Document 16 (2015–2016). When the Evaluation Committee's report was considered in 2017, the limitation on access to 'particularly sensitive information' was upheld 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 precedent, partially through case law, but also through customary law.

Classified information

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

Review of legality

Review 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.

Committee members and their respective terms of office for 2019:

The Committee during the first six months of 2019:

Eldbjørg Løwer, Kongsberg, chair
1 July 2011 – 30 June 2019

Svein Grønnern, Oslo, deputy chair
13 June 1996 – 30 June 2021

Theo Koritzinsky, Oslo
24 May 2007 – 30 June 2019

Håkon Haugli, Oslo
1 January 2014 – 30 June 2019⁸

Øyvind Vaksdal, Karmøy
1 January 2014 – 30 June 2021

Inger Marie Sunde, Bærum
1 July 2014 – 30 June 2019

Eldfrid Øfsti Øvstedal, Trondheim
1 July 2016 – 30 June 2021

The Committee during the last six months of 2019:

Svein Grønnern, Oslo, chair
13 June 1996 – 30 June 2021

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

Øyvind Vaksdal, Karmøy
1 January 2014 – 30 June 2021

Eldfrid Øfsti Øvstedal, Trondheim
1 July 2016 – 30 June 2021

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

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

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

Of the seven board members, five have political backgrounds from different parties while the other two have professional backgrounds within either law or technology.

The Committee is supported by a secretariat. At year end 2019, the Committee Secretariat consisted of fourteen full-time employees – the head of the secretariat (who has a law degree), five legal advisers (one vacant position), three technological advisers, one head of security, one communications adviser as well as two administrative advisers. Two technological advisers and one legal adviser (to fill the vacant position) will be appointed in 2020.

The Committee's expenses amounted to NOK 22,301,259 in 2019, compared with a budget of NOK 22,798,000, including transferred funds. The Committee has applied for permission to transfer NOK 496,741 in unused funds to its budget for 2020.

In 2019, the Committee was allocated NOK 29,000,000 for new premises. Unused funds in the amount of NOK 4,226,275 from the relocation project can be transferred to 2020 and 2021 to cover the remaining costs related to the project. We are very pleased with our new premises, which will ensure that the Committee can carry out its oversight work under safe and secure conditions.

⁸ Håkon Haugli's original term of office was until 30 June 2021, but he chose to withdraw from the Committee two years before the end of his term.



2.

Overview of the Committee's activities in 2019

2.1 Summary – main issues in the oversight of the services

The Norwegian Police Security Service (PST):

- The Committee has criticised PST for having registered members of the Storting based solely on their membership of a parliamentary friendship group that makes them potential targets for foreign intelligence activities. The discretionary judgement exercised by PST in registering these members of the Storting, was blameworthy. PST has informed the Committee that the registered information will be deleted.
- A journalist was registered by PST because he was invited to dinner by someone with links to foreign intelligence. Despite the fact that five years had passed without any new information in the case, PST considered it necessary to keep the registration, as the person could still be a target of foreign intelligence activities. The Committee did not agree that PST had a basis for retaining the registered information. PST has subsequently informed the Committee that the registered information will be deleted.
- In a special report to the Storting submitted in December, we strongly criticised PST for having collected a large quantity of information about Norwegian citizens' air travel.

The Norwegian Intelligence Service (NIS):

- The Committee criticised The NIS for failing to inform it about a tool for collating counterterrorism information, including information about Norwegian foreign fighters. We cannot exercise real oversight of the service's processing of information about Norwegians if we are not aware of all the systems, registers and tools where such information is processed.
- In 2019, the Committee requested verbal and written briefings from The NIS about how the service ensures national control of what intelligence information is disclosed to foreign collaborative partners. The answers received have been satisfactory.

The National Security Authority (NSM):

- The Committee has conducted an investigation of security interviews in NSM and FSA. In our opinion, the overall quality of such interviews is better than in previous investigations carried out by the Committee. At the same time, we find that several shortcomings remain in how interviews are prepared and conducted.
- In one complaint case, the Committee concluded that the complainant's rights had been violated when the person was denied security clearance on invalid grounds. NSM had failed to ensure that the case was sufficiently elucidated.

Other intelligence, surveillance or security services:

- The Norwegian Special Operation Forces (FSK) and PST have been criticised for giving incorrect information to the Committee about technical equipment being lent to PST by FSK. It is also unfortunate that neither PST nor the Special Operation Forces appear to have documentation or traceability concerning lending of technical equipment.

2.2 Oversight activities carried out

In 2019, the Committee conducted 19 inspections and visited all entities required by the Oversight Act. The Police Security Service (PST) was inspected six times, the Norwegian Intelligence Service (NIS) six times, the National Security Authority (NSM) twice and the Norwegian Defence Security Department (FSA) twice. The Army Intelligence Battalion, the MJK (the Norwegian Naval Special Operations Commando) and the Norwegian Civil Security Clearance Authority were all inspected once.

The Committee raised 24 cases on its own initiative in 2019, compared with 22 in 2018. The cases raised by the Committee on its own initiative are mostly follow-ups of findings made during our inspections. We concluded 17 cases raised on the Committee's own initiative in 2019, compared with 22 cases in 2018.

The Committee investigates complaints from individuals and organisations. In 2019, the Committee accepted 26⁹ complaints for consideration, compared with 19 complaints in 2018. 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 committee members 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 2019, we held eleven internal full-day meetings at the Committee's office, in addition to internal working meetings on site in connection with inspections. During our internal meetings, we discuss planned and completed inspections, complaint cases and cases raised on the Committee's own initiative, reports to the Storting and administrative matters.

⁹ Some complaints concern more than one of the services. The Committee dismissed three of the complaints, and two were withdrawn before their consideration was completed.

2.3 About the Committee's inspections

The Committee's inspections consist of a briefing part and an inspection part. The services' briefings are useful in giving us insight into the services' views on their responsibilities, assessments and challenges. The topics of 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 about the service's ongoing activities, its national and international cooperation and

cases that have triggered public debate, among other things. The Committee asks verbal questions during the briefings and sends written questions afterwards.

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

Inspections by the Committee in 2019



3.

Developments, framework
conditions and international
oversight cooperation

3.1 About the resource situation in the EOS Committee's secretariat

The Committee's remit is extensive, and expectations of us seem to be increasing. As we pointed out in our consultation submission concerning the Ministry of Defence's draft bill for a new Act relating to the Norwegian Intelligence Service, the EOS Committee is generally referred to as a security mechanism.

Over the past five years, the budgets of the three major services (The NIS, PST and NSM) have increased by approximately NOK 1.5 billion, while our budget has increased by NOK 12.5 million.

The significant growth in the services' budgets means an increase in activity within our oversight area. Our oversight is based on spot checks. It is not possible for us to review all of the EOS services' activities, nor would it be desirable to do so. The Committee nevertheless feel an expectation and a responsibility to maintain its intensity of oversight. When the services are growing as fast as they are at present, it becomes difficult to maintain the same intensity without further strengthening the Secretariat.

Moreover, the Committee finds that the intelligence, surveillance and security field is becoming more complex in terms of technological as well as legal and societal aspects. It is a precondition that the secretariat employees have a high level of expertise within all fields within the Committee's oversight area. Our oversight activities and our Secretariat must be capable of dealing with ever more specialised expertise in the services.

The Committee Secretariat used to consist of legal and administrative advisers, but now also comprises three technological advisers, with two more to be recruited in 2020. The Secretariat will then comprise 16 members of staff. In 2019, we have started to consider what would be the best way to organise the Secretariat, as it still needs more resources to be able to continue to provide the same level of support for the Committee's oversight work. This applies in particular to the Secretariat's legal adviser capacity and the need for a deputy head.

The Secretariat's technology unit will grow to comprise

five members of staff in the course of 2020. The unit has already proven highly useful to the Committee's oversight work.

In 2019, the technology unit started systematic efforts to map the EOS services' IT systems in order to improve the Committee's oversight. The unit has also focused on developing the Committee's expertise in such areas as IT security, artificial intelligence, 5G and other forms of communication technology.

In 2019, the technology unit has also familiarised itself with the proposal to allow the Norwegian Intelligence Service to use the method [facilitated bulk collection](#). The purpose of this work has mainly been to assess the technological aspects of this method.

The communication between the Committee and the services is currently non-digital. Work to digitalise parts of this communication was initiated in 2019. Digital communication would rationalise and simplify communication between the services and the Committee.

3.2 International oversight cooperation

Since 2015, the EOS Committee has taken part in a collaboration group with the oversight bodies of Denmark, Switzerland, Belgium and the Netherlands. In 2019, the UK oversight body, the Investigatory Powers Commissioner's Office (IPCO), joined the group. The Swedish and German oversight bodies were also present as observers at one meeting. The meetings are at an unclassified level, and they were also mentioned in the annual reports for the years 2015–2018.

The Committee finds this cooperation very important in relation to oversight of the increasing cooperation between the Norwegian EOS services and foreign services. This includes disclosure of sensitive personal data about Norwegians. We therefore need contact with foreign oversight colleagues in order to share experience that may become useful in our oversight of the Norwegian services.

A name for this group was adopted at a chair meeting held

Facilitated bulk collection

The gist of the proposal to introduce facilitated bulk collection is to allow the Norwegian Intelligence Service to collect transboundary electronic communication between Norway and other countries. The proposal is part of the draft bill for a new Act relating to the Norwegian Intelligence Service, which was distributed for consultation in 2018 and is expected to be presented to the Storting in 2020.

Sensitive personal data

The Personal Data Act, which is based on the EU General Data Protection Regulation (GDPR), 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, information about a person's sexual orientation or sex life, and personal data relating to criminal convictions and offences.

in The Hague in December 2019 – *the Intelligence Oversight Working Group*. On the same occasion, the chairs of the oversight bodies signed a charter for the group's work. The charter is enclosed as Appendix 5 to this report. Among other things, it states that the six oversight bodies aim to strengthen cooperation, exchange experience, provide a platform for developing effective oversight methods and increase transparency between oversight bodies within the boundaries set by national laws and regulations.

The group started a project on system-based oversight in 2019. The purpose of the project is to develop good oversight methods, particularly when it comes to overseeing large quantities of data. The work will continue in 2020.

In follow-up to a joint statement made by the oversight bodies of the group's five original member countries in autumn 2018,¹⁰ the EOS Committee raised the question of whether some classified information could be shared between the oversight bodies with the Minister of Defence and the Minister of Justice and Public Security. The ministers have so far been somewhat sceptical to our request, but we hope to continue this dialogue in 2020.

See Appendix 6 for the letters sent to and received from the ministries in connection with this matter.

You can also read more about the Nordic oversight cooperation in section 11.3.

3.3 Cooperation with the Communications Surveillance Control Committee

In recent years, the EOS Committee has been in dialogue and has had several meetings with the Communications Surveillance Control Committee. While the EOS Committee oversees the secret services, the Communications Surveillance Control Committee oversees the ordinary police service's use of lawful interception of communication, covert audio surveillance and equipment interference.

There are many details that the two committees cannot discuss because the information is classified, but the dialogue has nevertheless been useful. Among other things, technological advisers from both committees attended a joint workshop on equipment interference last year.

We see that closer cooperation between the EOS Committee and the Communications Surveillance Control Committee, including on legal issues, could be useful in our oversight of the secret services. It could also help to improve oversight of the use of coercive measures by the ordinary police.

¹⁰ The Committee's annual report for 2018 section 3.3 and Appendix 6.

Lawful interception of communication

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

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.

The Committee's consultation submissions

4.1 Introduction

The EOS Committee submitted three consultation statements in 2019. Two of them were mentioned in the annual report for 2018 – the consultation on the draft bill for a new Act relating to the Norwegian Intelligence Service¹¹ and the consultation concerning the application of the Security Act for the Storting's external bodies.¹²

We also submitted a consultation statement on lawful interception of communication in emergencies.

4.2 Consultation submission on lawful interception of communication in emergencies

The EOS Committee primarily submits consultations statements in cases where proposals will have direct consequences for the Committee's oversight and/or if there are circumstances that the Committee feels should be known before the Storting considers a bill.

On 2 September, the Committee submitted a statement to the Ministry of Justice and Public Security concerning a report by Professor Asbjørn Strandbakken on statutory regulation of the use of lawful interception of communication in emergencies.

The consultation paper consistently dealt with the need for a legal authority for using lawful interception of communication in emergencies and rescue situations where the *ordinary police* has a defined role. The EOS Committee could not see that the consultation paper considered any situation where such legal authority could be relevant for the Norwegian Police Security Service (PST). We also referred to the fact that the consultation paper did not mention the EOS Committee's role as an oversight body for PST's use of coercive measures.

In our consultation submission, we pointed out that one of PST's tasks is to prevent and investigate threats against dignitaries. If a dignitary is reported missing, the case would most likely be followed up by PST. If there are any indications that the dignitary in question has been abducted, it may be relevant for PST to make use of the necessity provision in Section 17 of the Penal Code to track the person via his/her phone or similar.

The EOS Committee concludes that the proposed legal authority for lawful interception of communication in emergencies needs clarification, including as regards whether it is relevant to PST, and the EOS Committee's subsequent oversight of lawful interception carried out by PST in emergencies.

The consultation submission is enclosed as Appendix 4 to this report.

11 The Committee's annual report for 2018 section 4.1 and Appendix 3

12 The Committee's annual report for 2018 section 4.3 and Appendix 5

5.

The EOS Committee is investigating the Frode Berg case

Based on information about Frode Berg that has come to public attention, the EOS Committee has initiated an investigation within the Committee's remit. It is unclear when this investigation will be completed.

6.

The Norwegian Police Security Service (PST)

6.1 General information about the oversight

In 2019, the Committee conducted four inspections of the PST Headquarters (DSE). The Committee also inspected the PST entities in Møre og Romsdal and Finnmark police districts.

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

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

6.2 PST's registration of members of the Storting

6.2.1 Introduction

It is one of the purposes of the EOS Committee's oversight to ensure that the activities do not unduly harm the interests of society. In light of the purpose of the Oversight Act and the historical context that formed the backdrop to the Committee's creation,¹³ we consider it one of our core functions to ascertain whether the EOS services are registering and monitoring citizens' political affiliations and activities.

PST's registration of politicians does not only represent an infringement on individuals' due process protection, but can have consequences for society as a whole. Democracy is based on the free formation of opinion and citizens' possibility to be politically active. Registration by the service could have a chilling effect on the citizens' possibility to be politically active.

For this reason, the Committee focuses on PST's intelligence registrations of members of the Storting. We have noted in particular that some members were registered because of their membership of a parliamentary friendship group. The representatives belonged to parties representing the entire political scale. They were not registered based on which party they belonged to. PST has not used any covert coercive measures such as covert audio surveillance, video surveillance or similar against any of the persons registered.

It appears to the Committee that the group membership was what triggered PST's intelligence registrations. We therefore decided to investigate the basis for these registrations.

6.2.2 PST's explanation to the Committee

PST was asked to explain whether the membership in itself necessitated the registration of individual members of the Storting.

PST denied that the registration was based on the political beliefs of the persons registered. PST referred to the fact that the service's experience shows that foreign intelligence services are particularly interested in and active in relation to the Storting's friendship groups. PST also stated that the preventive work involves informing the members of the Storting about the threats that foreign intelligence activities represent in order to enable the individual members to protect themselves. The service considers it one of its core functions to 'ensure that the full lawful range of political beliefs can be freely expressed'.

Therefore, PST considered it 'strictly necessary' to register information about each of the representatives as part of its preventive work. The service cited the Police Databases Act Section 64, cf. Section 7, cf. the Police Databases Regulations Section 21-2 first paragraph (5), as the legal basis for the registration. The Committee will review these provisions below.

6.2.3 Legal basis

PST is charged with preventing certain types of serious criminal offences. Among other things, this means that PST can register information about people before a criminal offence has taken place. PST may record what is known as intelligence registrations as part of its preventive work in cases where it is 'deemed necessary for preventive purposes'. The Police Databases Regulations Section 21-2 states about whom information can be processed. The provision's first paragraph (5) authorises registration of persons 'who are or who there is reason to believe will be targeted by foreign intelligence activities', among others.

This means that it is not a requirement that the persons have done or are suspected of having done anything improper, but that they can be registered on the basis of their exposed position. The Committee has previously pointed out to PST that registration of persons who are targeted by foreign intelligence activities must be based on a specific assessment of the nature of the contact, the assets

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 case

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

Investigation case

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

Intelligence registration

Processing of information that is deemed necessary and relevant for PST in the performance of its duties, and that does not warrant opening a prevention case.

the person in question manages and the probability that the contact may manifest as unlawful intelligence activities. It is also a fundamental condition that the data processed by PST are 'necessary' to the service's performance of its duties, cf. the Police Databases Act Section 64. The Police Databases Act Section 7 stipulates a *stricter necessity condition* for certain categories of personal data:

'The processing of personal data which reveal racial or ethnic origin, political, religious or philosophical beliefs, or trade union membership, or data concerning health, sex life or sexual orientation shall only take place if strictly necessary for the purpose of the processing.'

This requirement is elaborated on in the Police Databases Regulations Section 4-3, where it is specified that the 'strictly necessary' requirement means that the 'processing of data can only take place if it is the only way to achieve the purpose of the processing...'.¹⁴

6.2.4 The Committee's assessment

It follows from the Oversight Act Section 14 that if the Committee finds 'a decision (...) clearly unreasonable', it 'may express this opinion'. It is stated in the preparatory works to the Oversight Act¹⁵ that the oversight body must 'have the opportunity to oversee the exercise of discretion'. It is also pointed out that 'this will require caution, and it is hardly conceivable that discretionary judgment exercised within the limits of what is reasonable would be criticised'.

The Committee has considered the discretionary judgement exercised by the service in connection with the registration of the members of the Storting. We have also considered the registrations in light of the purposes of our oversight, which charge us with ensuring 'that the activities do not unduly harm the interests of society'. According to the preparatory works, this includes protecting the 'general freedom of opinion and expression'. The preparatory works go on to say that 'crimes against national security will often target politicians, and the surveillance service will therefore often operate in close proximity to political circles'.¹⁶ In connection with the 2017 amendment of the Oversight Act, it was stated that the change in the wording from 'civic life' to 'interests of society'

was not intended to entail any change in the legal realities, but to 'help to clarify that the EOS Committee can criticise activities that do not violate the rights of individuals as mentioned in Section 2 first paragraph subsection 1, but are nevertheless detrimental to collective societal interests such as freedom of expression, assembly and religion'.¹⁷

The Committee found that membership of the group could in itself signal a political position. We therefore believe that the registration of the members of the Storting's membership of the friendship group must be considered in light of the strict necessity requirement ('strictly necessary').

In the Committee's opinion, PST can achieve the purpose of registering and informing the friendship group without registering the group's individual members. *Membership of a friendship group cannot in itself constitute grounds for registration by PST.* We could not see that the registrations were strictly necessary to PST's performance of its duties.

The EOS Committee concluded that PST's registrations solely based on membership of the friendship group were clearly unreasonable and that the discretionary judgement exercised by the service in connection with the registration of the group's members was blameworthy. We are of the opinion that PST's registration of members of the Storting unduly harms the interests of society, cf. the Oversight Act Section 2 first paragraph (2).

6.2.5 Follow-up of the Committee's criticism

The Committee assumed that PST deleted the intelligence registrations of the members of the Storting. PST wrote in its reply to the Committee that the registrations were strictly necessary for the service to be able to consider relevant preventive measures. For this reason, PST wanted to keep the registrations.

The service later contacted the Committee again to express that it had taken the Committee's criticism very seriously and that it is a 'fundamental principle that special caution is exercised in connection with registrations that can be deemed to concern the registered persons' political affiliation and activities'.

13 Described as follows in section 17.1 of the Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee), Document 16 (2015–2016): 'The background to the Storting's decision to establish a special parliamentary grounded oversight committee was that, over time, considerable distrust of the EOS services and the government's oversight of its own services had developed. An important reason for this distrust was allegations that the Norwegian Police Surveillance Service (POT) was engaged in unlawful surveillance of individuals based on, among other things, political surveillance.'

14 The Police Databases Regulations Section 5-3 state that the 'strictly necessary' requirement will be met, for example, (i) when it is of significant importance to why or how a criminal offence was committed or is assumed to be committed, or (ii) when the purpose of the processing cannot be achieved without processing such data. A Royal Decree of 20 September 2013 concerning the Police Databases Act Section 4-3 states that 'the data in question can only be processed if that is the only possible way to achieve the purpose'. About the Police Databases Regulations Section 5-3 it states that 'the provision does not express anything new, but is intended to exemplify when the strict necessity requirement will be met' and that 'exemplification can provide clarification and is intended as an aid to interpreting this provision'.

15 Official Norwegian Report NOU 1994:4, *Kontrollen med "de hemmelige tjenester"* ('Oversight of the 'secret services' – in Norwegian only), section 4.2.1.

16 Proposition No 83 to the Odelsting (1993–1994) *Om lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste* ('About the Act relating to the Oversight of Intelligence, Surveillance and Security Services' – in Norwegian only), p. 21.

17 Private Member's Bill 63 (2016–2017), comments to Section 2.

PST went on to say that the service will 'organise its future registration practice in accordance with the EOS Committee's assessment of the basis for registration', and also stated that the registrations based solely on membership of the group in question will be deleted.

The case has been very important to the Committee as a matter of principle. We are pleased that PST has decided to base its registration practice on the Committee's assessment and that the intelligence registrations of the members of the Storting will be deleted.

6.3 Registration of a journalist

The Committee has concluded one case concerning PST's processing of information about persons who are or may be 'targeted by foreign intelligence activities'.¹⁸ It was a key questions in this case when and for how long a person can be considered to be 'targeted by foreign intelligence activities'. A journalist was registered because he was invited to dinner by a person with links to foreign intelligence.

The journalist had been registered in PST's intelligence register Smart for five years without any new information in the case.¹⁹ PST reviewed the registration and decided that it was necessary to keep the information, as foreign intelligence services' attempts at establishing contact with potential sources can go on for years.

The Committee, on the other hand, was of the opinion that PST no longer had any basis for keeping the registered information, as there had been no development in the case for several years. We therefore urged PST to delete the information.²⁰

PST stated that the service disagreed with the Committee and believed that there were still grounds for having the journalist registered. Therefore, PST did not initially delete the information from Smart.

The service has subsequently reported that it has reconsidered and that the registered information has now been deleted based on the Committee's criticism.

6.4 Storage of documents at PST's premises in Møre og Romsdal

During an inspection of the PST office in Møre og Romsdal,

the Committee inspected the office's vault, where it found a binder containing information about an old case.

The Committee asked about the background to PST gaining access to the information and storing it in the binder. PST replied that the police district had investigated the case as a criminal case concerning threats. The case was also evaluated to determine whether it involved threats against a dignitary. Threats against dignitaries fall within the scope of PST's duties. The documents in the case were therefore handed over to PST, which stored the binder.

The case was stored as documents in a criminal case, and the provisions on deletion set out in the Police Databases Regulations Section 25-5 and the Police Databases Act Sections 50 and 51 do not apply to such documents.

Since the case had been dropped several years ago, further storage of the binder was not necessary, and it was consequently shredded following the Committee's inspection.

The Committee expressed satisfaction with this solution. No further follow-up in relation to PST was required.

6.5 Follow-up of PST's disclosure of information for use in security clearance cases

In the EOS Committee's annual report for 2018,²¹ we criticised PST because the service had in a high proportion of cases communicated information to the security clearance authorities verbally without documenting this in writing. This was in violation of the law.²²

The Committee was informed during an inspection of NSM in 2019 that NSM and PST have prepared a remit and that a working group will be appointed to draw up an agreement²³ on sharing of information in security clearance cases. The agreement will regulate the procedure for PST's disclosure of information obtained from the intelligence register for use in security clearance cases.

The Committee is satisfied with this development.

6.6 About the special report on PST and information about airline passengers

On 5 December, the Committee submitted a special report to the Storting on PST's unlawful collection and storage of

information about airline passengers. The matter is under consideration by the Storting. The main conclusion was as follows:

'The EOS Committee strongly criticises the Norwegian Police Security Service (PST) for having collected a large quantity of information about Norwegian citizens' air travel. It is our opinion that the collection has been – and is – unlawful because PST has not had legal basis for it.

The EOS Committee wishes to bring the following four circumstances to the Storting's attention:

- PST has continued its practice of collecting information about Norwegian airline passengers' travel abroad, also after being criticised by the Committee in a specific case in 2014 for not having legal authority for such collection.
- PST has unlawfully obtained access to large quantities of information about both Norwegian and foreign passengers on domestic and international flights through access to the booking system of the airline Norwegian Air Shuttle ASA. PST has not had legal authority for such access. This is information that PST would otherwise have required court authorisation to obtain in each case.
- Eight airlines have routinely submitted their passenger lists to PST. This routine submission concerned information about approximately one million passengers a year, several hundred thousand of whom were Norwegians. This routine collection of information is unlawful. The information has been stored for several months and has been available for searches.
- PST has not had sufficient internal control and documentation of its own collection activities.

In 2017, PST wrote to the Committee that the regulatory framework 'probably does not' authorise either access to the booking system or the routine submission of passenger lists. Instead of discontinuing the practice, the service adopted an internal procedure (submitted to the Committee in February 2019) in which it is stated that the service will continue to collect such information. In September 2019, PST stated to the Committee that the legal authority for the collection is unclear.

It is the Committee's clear expectation that PST will discontinue a practice that the service itself believes does not comply with the regulatory framework.

The way in which PST has handled the matter has prompted stronger criticism from the Committee.'

6.7 Non-conformity report from PST

PST has in recent years informed the Committee about non-conformities at its own initiative. We take a positive view of the fact that PST reports non-conformities that the service itself has identified. In 2019, PST has informed the Committee about one non-conformity. The service has described a trial project where personal data from two registers were checked against each other without it being necessary in each individual case. The trial project was discontinued following an internal legal evaluation. The Committee will keep informed about PST's follow-up of this non-conformity.

6.8 Complaint cases against PST

The Committee has accepted 13 complaints against PST for consideration in 2019, compared with 6 complaints in 2018. Some of these complaints were against more than one of the EOS services.

The Committee's statements to complainants shall be unclassified. Information concerning whether or not a person has been subjected to surveillance shall be regarded as classified unless otherwise decided. 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 ten complaint cases against PST in 2019, none of which resulted in criticism of PST.

18 Cf. the Police Register Regulations Section 21-2 (5).

19 There is a requirement for PST's intelligence registrations to be re-evaluated if no new information has been added during the past five years.

20 The Committee can request that PST delete information pursuant to the Oversight Act Section 14 sixth paragraph. Cf. Section 17 fourth paragraph (5), where it is stated that the annual report should include 'a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 14, sixth subsection'.

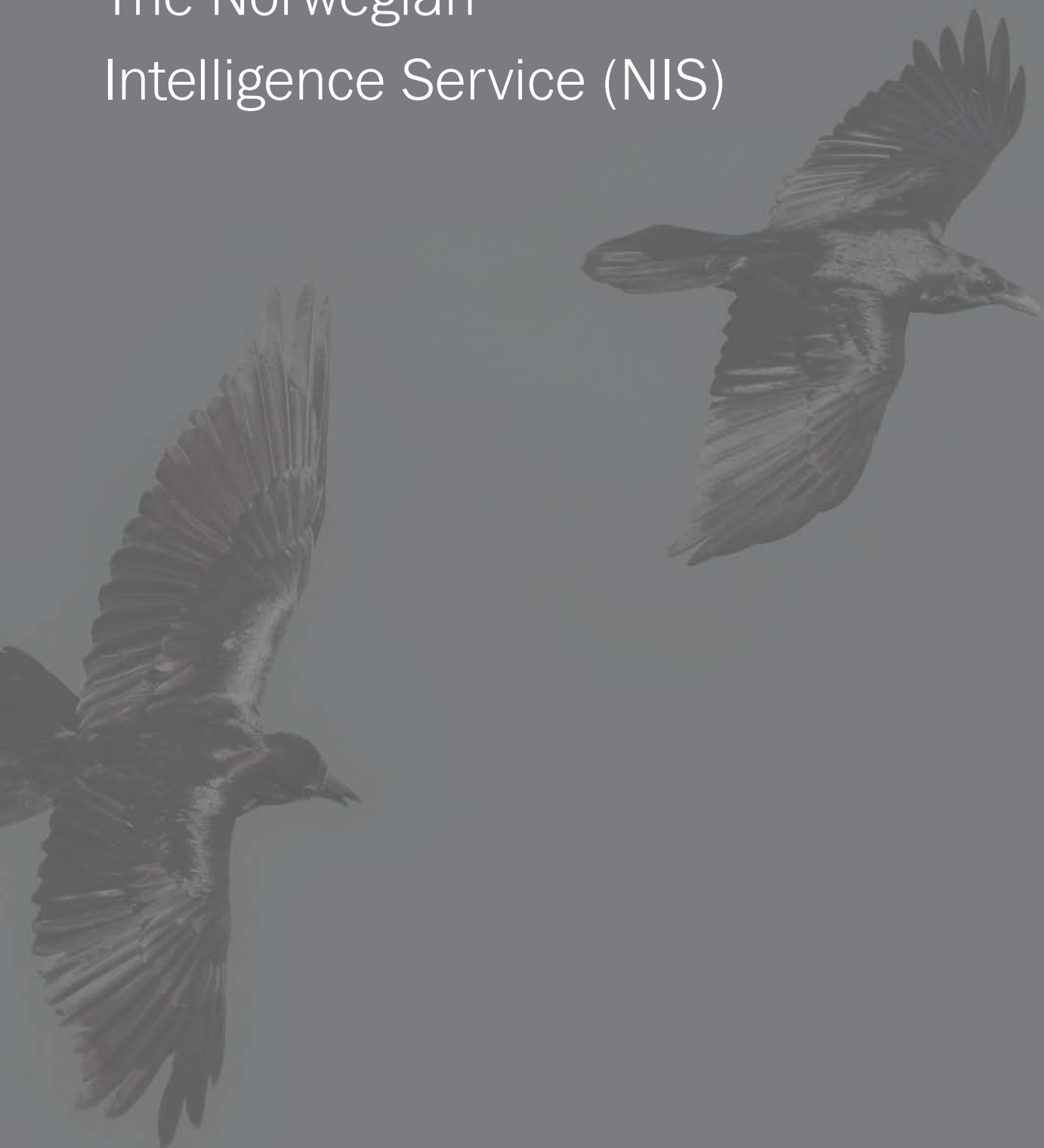
21 Section 5.2 of the Committee's annual report for 2018

22 The requirement for information to be disclosed in writing followed from the Security Act 1998 Section 20 fourth paragraph and the Police Databases Regulations Section 11-3 first paragraph, cf. the Police Databases Act Section 30 and the Police Databases Regulations Section 9-6 first paragraph (11).

23 This follows from the Clearance Regulations Section 12.

7.

The Norwegian Intelligence Service (NIS)



7.1 General information about the oversight

The Committee has conducted three inspections of the NIS headquarters in 2019, in addition to inspections of the NIS stations in Vadsø and Vardø. The inspection of the Army Intelligence Battalion based at Setermoen military base (see section 10.2) also included an inspection of the NIS.

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

- That the service does not violate the statutory prohibition against monitoring or in any other covert manner procuring information concerning persons on Norwegian territory²⁴
- The service's technical information collection
- The service's processing of information in its computer systems
- The service's exchange of information with cooperating domestic and foreign services
- Matters of particular importance or that raise questions of principle that have been submitted to the Ministry of Defence²⁵ and internal approval cases²⁶
- National control of the NIS's stations, equipment and methods

We also request that the NIS report any non-conformities it uncovers in the service's technical information collection to the Committee. The NIS has not reported any non-conformities in 2019.

The Committee's full right of inspection of 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.

7.2 The NIS omitted to inform the Committee about a counterterrorism tool

The NIS has developed a tool for systematising information in its work to combat international terrorism. The EOS Committee did not have access to this tool, nor had we received any information about it.

In response to a question from the Committee, the NIS stated that it introduced the tool in 2016 to gather notifications concerning international terrorism. The service wrote that there is no tradition for accounting for every new tool the service acquires, nor any need to do so. The service also wrote that it was not its 'intention to withhold one of the service's tools from oversight. It has simply not been considered a significant matter of principle, as the information processed using the tool is also found elsewhere in the service, including in incoming notifications, reports written, own collection etc.'

The Committee has extensive right of access to the NIS's archives and registers, and the service is obliged to provide anything that may have significance for the Committee's inspection, cf. the Oversight Act Section 8. We have previously stated to the Storting that this duty to facilitate 'must be understood to mean that the services are under an obligation to provide information about new forms of activity within the Committee's oversight area, and actively facilitate oversight within the area'.²⁷

The Committee regularly asks the services about their systems and registers. This is done to obtain an overview and the ability to organise the Committee's oversight in the best possible manner. We cannot exercise real oversight of the service's processing of information about Norwegians if we

24 Cf. the Intelligence Service Act Section 4 first paragraph. Exemptions are regulated in the Instructions for the Norwegian Intelligence Service Section 5 third paragraph.

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

26 Internal approval cases can be permission to share information about Norwegian persons with cooperating foreign services or to monitor Norwegian persons' communication when the persons are abroad. As the Committee has previously pointed out, the NIS is not required to obtain court permission to monitor 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.

27 See the Committee's annual report to the Storting for 2014 section 2. The Standing Committee on Scrutiny and Constitutional Affairs drew attention to the Committee's statement in its recommendation to the Storting regarding the annual report for 2014.

Particularly sensitive information

The EOS Committee has limited access to data held by the NIS that is deemed to be particularly sensitive information.

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

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

*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.

are not aware of all the systems, registers and tools where such information is being processed. The fact that most of the information can also be found in the NIS's other systems does not justify omitting to provide information about this specific tool.

This tool collates information about the service's counter-terrorism work, including information about Norwegian foreign fighters. This tool gives the Committee a simpler way to access information that is crucial to the oversight of the NIS. It is also possible that information that has been deleted from other registers in accordance with the service's procedures are still processed in this tool.

In its oversight of the NIS, the Committee focuses in particular on ensuring that the service complies with the statutory prohibition against monitoring Norwegians in Norway as set out in the Intelligence Service Act Section 4 first paragraph. The service's efforts to combat international terrorism is the area where the NIS's targeted collection deals with the most information about and from Norwegians. This increases the risk of the prohibition being violated, and we therefore make this a key area in our oversight of the NIS.

The Committee has made it clear to the NIS on a general basis that the Committee's right of inspection does not relieve the service of the obligation to inform the Committee about relevant systems and tools. The threshold for reporting new tools to the Committee should be a low one, particularly in key areas for the Committee's oversight of the service.

The Committee stated that the NIS should have informed it about the tool's existence on its own initiative and at a

far earlier time. We found that the service's failure to do so warranted criticism.

The NIS has subsequently acknowledged that its procedures for informing the Committee have been unsatisfactory. The service has stated that, in future, it will intensify its efforts to inform the Committee of new such tools and applications at the earliest possible opportunity.

7.3 National control over Norwegian intelligence information

National control is an important oversight point in the EOS Committee's continuous oversight of the activities of the NIS. Section 4 of the Instructions for the Norwegian Intelligence Service reads as follows:

'The Norwegian Intelligence Service shall be under Norwegian control. This includes ensuring national control over what information is disclosed to foreign collaborative partners.'

In 2019, the Committee requested verbal and written briefings from the NIS about how the service ensures national control of what intelligence information is disclosed to foreign collaborative partners.

The Committee has found the service's answers satisfactory. We have noted the NIS's assurances that the service has full national control over the disclosure of intelligence information.



Foreign fighter

A person who fights in an armed conflict outside his or her own country for ideological or idealistic reasons, and who is not a paid mercenary.

Our local inspections of the NIS stations in Vardø and Vadsø in Finnmark county in 2019, and regular inspections of the NIS headquarters, have not given us any indications of shortcomings in the NIS's efforts to ensure national control over its intelligence information.

In 2019, the Committee initiated work to review several of the NIS's important cooperation agreements with foreign partners. Among other things, the Committee focuses on checking whether the agreements are capable of ensuring that national control over what information is disclosed to foreign partners is safeguarded.

The expansion of the technology unit in the Committee's secretariat will enable the Committee to be even more thorough and specific in its oversight in relation to this issue in the time ahead.

We will also look into the possibility of being physically present at selected NIS stations for longer periods. The purpose of this will be to gain even better insight into and knowledge of the technological aspects of exchange of data with foreign partners. One important aspect of this will be to gain a better understanding of how the data exchange takes place at the technical level. The Committee will come back to this.

7.4 Intelligence cooperation with states with human rights challenges

The NIS may establish and maintain intelligence cooperation with other countries, cf. the Intelligence Service Act Section 3 second paragraph. Pursuant to the Intelligence Service Instructions Section 17, unclassified supplementary provisions were adopted concerning the NIS's collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services.²⁸ Section 4 of these supplementary provisions stipulate that personal data concerning Norwegian persons shall not be disclosed to cooperating foreign services unless certain conditions are met. We oversee that the NIS's disclosure of personal data to cooperating foreign services complies with these conditions.

The Committee has asked the NIS about the use of the service's internal instructions on intelligence cooperation with states where there is a risk of torture and other cruel, inhuman or degrading treatment or punishment (*Instruks om etterretningssamarbeid med stater hvor det foreligger risiko for tortur eller annen grusom, umenneskelig eller nedverdiggende behandling eller straff* – in Norwegian only). Among other things, we have asked the NIS how it evaluates the human rights situation in a country before disclosing

information to cooperating services.

In the Committee's opinion, the service's reply showed that it has an awareness of human rights issues when disclosing personal data to cooperating foreign services. In its concluding letter to the NIS, the Committee remarked that it considers it a positive thing that the service endeavours to raise awareness of human rights considerations and issues within the service. We also wrote that it is important that the service communicates the principles set out in the instructions to external parties in its dialogue with partners and in bilateral cooperation agreements.

The NIS stated that it has considered obtaining assurances of cooperating services' willingness and ability to observe human rights in a 'limited number of cases'. The service stated that 'however, to date such assurances have not been used, as the service has not deemed it necessary based on, e.g., the scope and type of data disclosed, the whereabouts of the person the information concerns and the dialogue with the service to which information is disclosed'. The service also wrote that 'provisos and conditions imposed in connection with the disclosure also address the NIS's limitations on subsequent use of the information'.

The Committee notes that it could be unfortunate if Norwegian services do not make it their practice to obtain assurances from cooperating services of their ability and willingness to observe human rights before sharing information. The Committee urged the NIS to obtain such assurances if there is a real risk of human rights violations.

The Committee pointed out that it is an important principle in itself to obtain assurances from cooperating services of their ability and willingness to observe human rights. Such assurances demonstrate an expectation that the recipient will respect human rights.

We also assume that Norwegian services must exercise caution when it comes to exchanging information about individuals with states that are not known to respect human rights and/or do not have satisfactory data protection legislation.

At the same time, the Committee expects the NIS to incorporate human rights conditions and principles in new cooperation agreements and to take necessary steps to reduce the risk of human rights violations. The Committee also expects the NIS to keep up to date on any changes in the human rights situation in relevant countries.

The Committee is considering a case involving similar issues related to PST's exchange of information. The consideration of this case has not yet been concluded.

28 Adopted by the Ministry of Defence on 24 June 2013 pursuant to the Instructions for the Norwegian Intelligence Service Section 17.

7.5 Differences between how PST and the NIS process information about deceased persons

In 2019, we raised the question of whether the personal data protection in the new Act relating to the Norwegian Intelligence Service *should also apply* to deceased persons.

Today, different conditions govern the processing of personal data about deceased persons by the NIS and PST. The topic has become more relevant in recent years, particularly considering the fact that PST and the NIS process information about Norwegian foreign fighters.

PST's processing of personal data about deceased persons must meet the conditions for processing set out in the Police Databases Act in terms of relevance, necessity and specification of purpose. The Police Databases Act does not distinguish between the living and the dead. PST must make a specific assessment of whether there is a basis for processing personal data about a deceased person. The Ministry of Justice and Public Security stated the following in the preparatory works to the Police Databases Act:

'[t]he data that the police possesses will usually be of such a sensitive nature that the person's death should not have any bearing on their protection. Consideration for the reputation of the registered person after death suggests the same. This will also apply in cases where the processing takes place in its entirety after the death of the person in question'.²⁹

However, no such limitations apply to the processing of personal data about deceased persons by the NIS. The reason

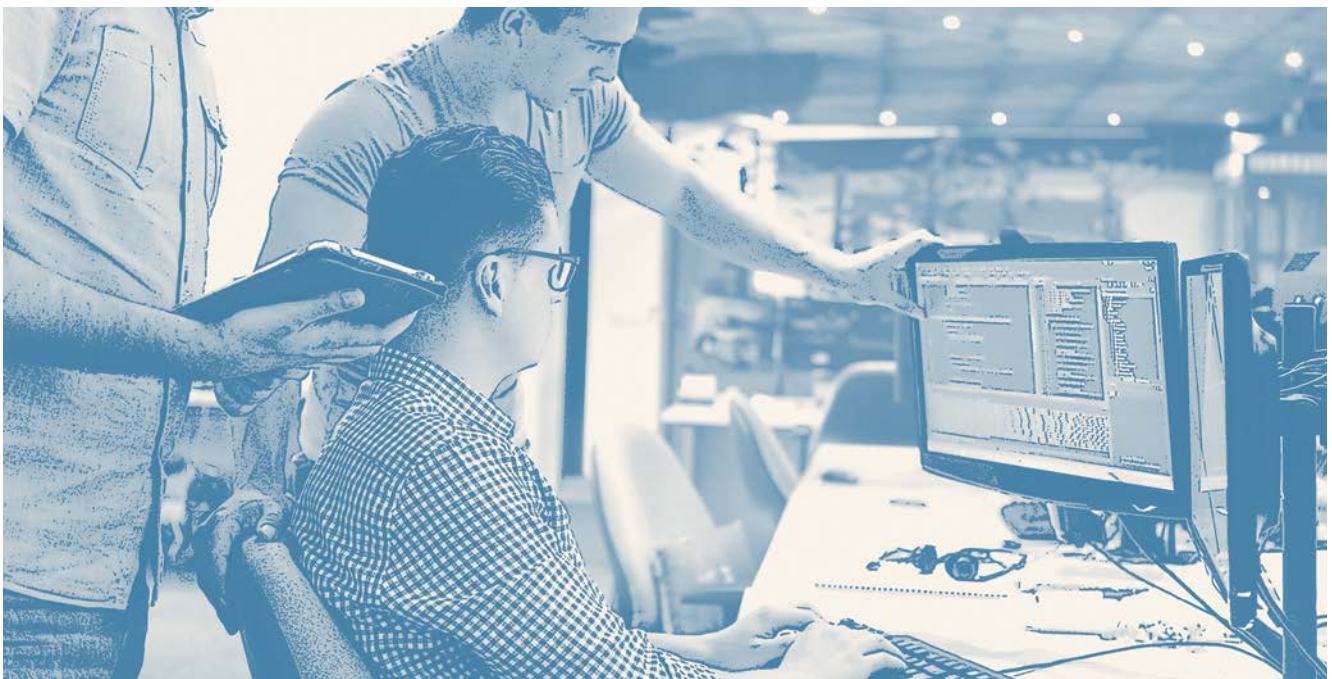
for this is that processing by the NIS falls under the scope of the provisions of the Personal Data Act, under which protection of privacy does not apply to deceased persons.³⁰

In the Committee's opinion, the NIS's processing of personal data is more comparable with PST's processing of personal data (the Police Databases Act) than with e.g. a private company's processing of personal data about its clients (the Personal Data Act). The NIS also processes personal data about Norwegian persons. In many cases, the NIS processes personal data about *the same individuals* as PST does, sometimes based on the same facts. That is the background to the Committee's statement that the different conditions for processing of data concerning deceased person by the NIS and PST appears unwarranted.

Strong reasons suggest that personal data stored by the NIS about a person that has been under surveillance must be considered just as sensitive as PST's processing of personal data – even when the person in question is dead.

The Committee has asked the Ministry of Defence to consider whether information about deceased persons should be afforded the same protection as living persons in the new Intelligence Service Act. The NIS later raised the question of whether the EOS Committee is engaging in development of the law, and whether it is 'consistent with the EOS Committee's primary role as an oversight body' to send such a request to the ministry.

In a concluding letter to the Ministry, we commented on the differences in the current regulatory framework for the processing of information about deceased persons by PST and



the NIS. The Committee referred to the Oversight Act Section 5 third paragraph, which states that the Committee shall on its own initiative deal with all matters and factors that it finds appropriate to its purpose. Factors shall here be understood to include regulations, cf. Section 5 third paragraph final sentence. We also referred to the Oversight Act Section 14 third paragraph:

‘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.’

The Committee also remarked that in autumn 2019 it was appropriate to ask the ministry to consider whether deceased persons should be afforded the same protection as the living, as the ministry has been working on a new Intelligence Service Act and special regulations for processing of personal data by the NIS. In our opinion, this is part of the consultation process.

Considering the present differences between PST’s and the NIS’s legal basis for processing personal data about deceased persons, we are hereby notifying the Storting of a potential need to amend the Norwegian Intelligence Service’s regulatory framework.³¹

7.6 Obligation to keep a list of Norwegian persons about whom the NIS is collecting information abroad

The NIS is obliged to keep a list of cases where intelligence collection targeting Norwegian persons abroad has been initiated.³² The Committee asked the NIS to explain why a Norwegian person who was presumed dead had been removed from this list despite the fact that the service was still collecting intelligence concerning the person’s selectors.

The Committee took note of the service’s account of its assessments. Nevertheless, we noted that the NIS did not directly answer the question about whether the obligation to keep a Norwegian intelligence target registered in the list lapses when the service assumes that the person may be dead. In this case, the person’s selectors were still being monitored, and it was uncertain whether the person was actually dead and, if so, who was then using the selectors.

The Committee referred to the NIS’s obligation to keep a list of cases where the services are keeping Norwegians abroad under surveillance. We referred to the fact that it is an important part of the parliamentary oversight of the NIS to oversee the service’s collection activities in relation to the means of communication used by Norwegian citizens abroad. We commented that if persons who are presumed dead and removed from this list turn out not to be dead after all, or if it turns out that other *Norwegian* persons (such as closely related persons) are using the persons’ selectors after their presumed death, the Committee could lose an important part of the overview of collection activities in relation to Norwegian citizens abroad. This could weaken our oversight.

Consideration for our oversight indicates that Norwegian persons who may be dead should remain on the list for as long as collection in relation to their selectors continue and as long as it is uncertain if any other Norwegian person could be using the selectors.

Since the number of such persons will be small, the Committee could not see that this would impose any significant additional work on the NIS.

7.7 Cooperation between PST and the NIS and information collection from open sources

Together, PST and the NIS shall help to prevent and combat threats against national security through exchange of information, cooperation and division of tasks.³³ Cooperation between the two services shall take place within the scope of their respective legal bases.

29 See Proposition No 108 to the Odelsting (2008–2009), section 7.2.1.4.

30 In its consideration and adoption of the new Personal Data Act in 2018, the Storting assumed that the new Personal Data Act would not apply to the Norwegian Intelligence Service. Until the new Intelligence Service Act enters into force, the main pieces of legislation that regulate the service’s processing of personal data will continue to be the Intelligence Service Act of 1998 and the Personal Data Act of 2000.

31 Cf. the Oversight Act Section 17 fourth paragraph (8).

32 Cf. Supplementary provisions concerning the Norwegian Intelligence Service’s collection of information concerning Norwegian persons abroad and the disclosure of personal data to cooperating foreign services Section 5 second paragraph.

33 Instructions for the Collaboration between the Norwegian Intelligence Service and the Norwegian Police Security Service Section 1.

Selector

In an intelligence context, a selector is a target from which information is collected, for example a telephone number or an e-mail address.

The Committee concluded two cases concerning cooperation between PST and the NIS in 2019. Both cases concerned the collection of information about persons resident in Norway.

In one case, PST requested information about the network of a social media profile from the NIS. The profile belonged to a person resident in Norway.

The other case concerned information about a person resident in Norway disclosed to PST by the NIS. In connection with this, the NIS had also sent the names of a number of other Norwegian persons who were living in the same building. The information had been obtained from open sources.

PST and the NIS were asked to explain their procedures for cooperation on the collection and sharing of information about Norwegian persons and persons resident in Norway. The services were also asked to give an account of PST's request to the NIS and the NIS's collection of information relating to persons resident in Norway.

PST and the NIS both argued that the NIS's collection of information from open sources (known as OSINT – open-source intelligence) about persons in Norway does not fall within the scope of the prohibition in the Intelligence Service Act Section 4 against monitoring persons in Norway as long as the purpose of the collection is not to 'target' domestic circumstances or circumstances relating to the person in Norway.

In our concluding letter to the services we remarked that the question of whether or not the NIS's OSINT activities in relation to persons in Norway fall within the scope of the prohibition in the Intelligence Service Act Section 4 is discussed in the annual report for 2018:³⁴

'We are concerned with when the NIS can collect information about persons in Norway. It is not evident from the wording of the prohibition that the *intention* of the service should be the factor that determines whether or not monitoring persons in Norway is in breach of the prohibition. That the service's intention is only to monitor a person when he/she is outside Norway, but not when the person in question is in Norway, is an artificial distinction that it is difficult for us to oversee.'

The Committee has stated that, under the present regulatory framework, there is reason to doubt whether the service's collection of information from open sources about Norwegian persons in Norway is lawful, and we have stated that the scope of the prohibition in Section 4 of the Intelligence Service Act should be clarified by the Storting. In its consideration of the annual report for 2018, the Standing Committee on Scrutiny and Constitutional Affairs expected the Storting to look into the matter in connection with the consideration of the draft bill for the new Intelligence Service Act.³⁵ Therefore, we have not gone into the details of the matter in connection with this case.

The NIS informed the Committee that the information about persons who were living in the same building as the person about whom information was exchanged, has been deleted. The Committee will follow up how this deletion has been carried out.

7.8 Complaint cases against the NIS

The Committee has accepted three complaints against the NIS for consideration in 2019, compared with four complaints in 2018. Some of these complaints were against more than one of the EOS services.

The Committee's statements to complainants shall be unclassified. Information concerning whether or not a person has been subjected to surveillance shall be regarded as classified unless otherwise decided. This means that, in principle, a complainant cannot be told whether he or she is under surveillance by the NIS or not. 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 five complaint cases against the NIS in 2019. None of these cases resulted in criticism of the NIS.

³⁴ The Committee's annual report for 2018, section 8.2.

³⁵ Recommendation No 284 to the Storting (2018–2019), the Committee's comments, page 17.

A blue-tinted background image showing a person's hands writing on a notepad. The person is wearing a light-colored shirt. The notepad is open, and the person is using a pen to write on the right page. The left page is blank. The image is overlaid with a semi-transparent blue filter.

8.

The National Security Authority (NSM)

8.1 General information about the oversight

In 2019, the Committee conducted two inspections of NSM. The authority's processing of security clearance cases was the focus of one of these inspections. The other inspection focused on NSM's technical capabilities in terms of technical security inspections, penetration testing, TEMPEST and the sensor system to identify fake base stations.

NSM has directorate status and attends to the general functions in the field of 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 EOS services
- NSM's processing of personal data
- NSM's technical capabilities

The function of the security clearance authority is to assess the reliability, loyalty and judgement of a person and determine whether he or she is fit to process classified information.³⁶ A security clearance decision can be decisive for a person's career, and strict requirements must therefore apply to the processing of such cases. The Committee maintains a particular focus on such cases for this reason – and because the processing of security clearance cases is a more closed process than other administrative decisions.

8.2 Investigation into security interviews in NSM and FSA

How security interviews are conducted has been a topic of interest to the EOS Committee for several years.

A security interview is an interview of a person for whom security clearance has been requested, conducted by a security clearance authority. In the security interview, the security clearance authority can ask about anything that is pertinent to the assessment of whether the person in question can be

granted security clearance. The interview gives NSM and FSA a better basis for assessing whether the person is suitable for security clearance. At the same time, the person for whom security clearance has been applied for (the principal person) has an opportunity to comment and elaborate on the information provided in the [personal data form](#).

The information that emerges during a security interview can help to clear up any doubts as to whether the person in question can be granted security clearance. The security interview is therefore an important tool in the security clearance authority's toolbox. All security clearance authorities may conduct security interviews. As the expert authority for the Security Act, NSM has a particular responsibility for ensuring that its security interviews are of high quality.

The Committee's previous dialogue with NSM was discussed in the annual reports for the years 2013–2015. In 2018, the Committee decided to follow up our remarks by conducting a systematic review of a large number of security interviews. The purpose of the project was to ascertain whether the quality of the interviews has improved. In this project, we looked into whether the security interviews are prepared and carried out in such a way that the security clearance authority obtains the information it needs, while the person for whom security clearance is applied for has a chance to comment on relevant topics. The Committee reviewed 30 security interviews conducted in 2017, 15 of which by FSA and 15 by NSM. After the review, a report was written about the findings.

In the project, the Committee focused on the following:

- Whether the method for conducting security interviews is appropriate and ensures that the person for whom security clearance is applied for is given sufficient opportunity to state his or her view on the matter
- Whether the form of the interview is sufficiently flexible and adapted to the individual case
- Time use during interviews
- Whether the question of the principal person's suitability for security clearance is given adequate attention in the interview

The EOS Committee concluded that there has been a positive development in the quality of security interviews since 2015. At the same time, we are of the opinion that the matter of the principal person's reliability, loyalty and judgement was still not given enough attention in the interviews from 2017.

Technical security inspection (TSI)

Inspections of premises, buildings or other objects with a view to ascertaining whether unauthorized persons can gain access to sensitive information.

TEMPEST

Electromagnetic radiation is energy that has different properties depending on its wavelength or frequency. All electronic equipment emits electromagnetic radiation. The term TEMPEST is used when such emanations contain information that can be used to reconstruct classified information.

The Committee stated that the security clearance authorities must continue their efforts to ensure that the quality of security interviews becomes better and more consistent.

The report from the security interviews project is enclosed as APPENDIX 3 to this report.

8.3 Follow-up of the special report on differing practices in security clearance cases

On 12 March 2019, the EOS Committee submitted a special report to the Storting on differing practices in the security clearance of persons with connections to other states.

The investigation identified unjustified differential treatment by different security clearance authorities in two areas. The Committee emphasised to NSM, which is the expert

authority for security clearance cases, how important it was to put in place an experience archive and other tools to ensure uniform treatment. NSM had not yet implemented the announced measures to ensure uniform treatment when the Committee submitted its report to the Storting in March 2019. It emerged during the Storting's consideration of the Committee's special report on 17 June 2019 that NSM was in the process of developing an experience archive, and the archive was established in late 2019.

The authority has also, in cooperation with the major security clearance authorities, initiated work to develop a system to ensure uniform treatment of the cases. The experience archive and various forums for discussing security clearance-related issues and uniform treatment are important elements of this system, which also includes cooperation with the security clearance authorities on how practice notes can be used in case processing.



36 Cf. the Security Act 2018 Section 8-4.

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 and listen to calls, read text messages and see mobile data traffic.

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.

Personal data form

A form that the person for whom a security clearance is applied for has to fill in and that forms part of the basis for the security clearance authority's decision.

In its special report to the Storting, the Committee assumed that NSM would give high priority to work on the measures announced and that the work would be completed shortly. In 2019, we have kept informed about the status of the tools for ensuring uniform treatment in security clearance cases. In our opinion, it is unfortunate that it has taken so long to implement the measures. It is important that NSM as the expert authority establish solutions that ensure uniform practice, so that persons for whom security clearance is applied for can have their cases processed in a fair manner that safeguards due process protection.

8.4 Complaint cases

8.4.1 Introduction

The Committee has accepted 9 complaints against NSM for consideration in 2019, compared with 11 complaints in 2018. All the cases concerned security clearance issues or access to information about a security clearance case.

A security clearance decision can be of vital importance to a person's life situation and future career. It is therefore essential that these cases are considered by the security clearance authorities in a fair manner that safeguards due process protection. In cases where the Committee expresses criticism, the complainant is given grounds for the Committee's decision.

We concluded six complaint cases in 2019, and one complaint case has been partially concluded. We criticised NSM in two of these cases:

8.4.2 Complaint case 1 – Invalid decision to refuse security clearance on grounds of inadequate elucidation of the case

In a complaint case concerning a decision to refuse security clearance, the Committee questioned the assessment carried out by the appellate body (NSM) and the body that made the initial decision (FSA) of the available information about the personal history of the complainant's spouse. The complainant's spouse is a foreign national from a country outside Europe that does not constitute a serious intelligence threat to Norway.

In order to carry out vetting, it must be possible for the security clearance authority to obtain security-relevant information covering the past ten years about the persons covered by the vetting process.³⁷ If the person in question has stayed in

another country, such information can be disclosed to Norway if the country in question is one with which Norway cooperates on security-related matters. Exceptions may be granted from the ten-year history requirement based on a specific assessment of the case. Both information about which countries disclose vetting information to Norway and information about the specific minimum limits for what constitutes sufficient personal history is considered classified information.

In this case, the Committee has been particularly interested in two factors:

- the security clearance authority's obligation to elucidate the case, and
- that the complainant cannot be blamed for not having provided information that is relevant based on criteria that are classified, and thus not known to the complainant.

It followed from the Security Act 1998 Section 21 third paragraph that 'the security clearance authorities shall seek to ensure that security clearance cases are as well elucidated as possible before a decision is made'. In the case in question, the security clearance authority had not looked into the complainant's information about a long stay in a country with which Norway cooperates on security-related matters.

A more detailed investigation of the information about the spouse's stay could have been decisive to the outcome of the security clearance case. The Committee pointed out that the decision to deny security clearance had not been sufficiently elucidated and was therefore invalid, and requested NSM to consider the case again.

When the case was concluded, we stated that the vague grounds given made it more difficult for the complainant to respond to the decision and weakened the complainant's due process protection.³⁸

NSM considered the case again, but concluded that the personal history information available was not sufficient to indicate that security clearance should have been granted.³⁹

8.4.3 Complaint case 2 – Inadequate grounds to the principal person in a security clearance case

The case concerns a person who 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. The person for whom security clearance was requested filed a complaint with the

Personal history

Vetting in connection with security clearance requires security-relevant information about the person's background covering the past ten years.

Vetting

Obtaining information of relevance to the security clearance assessment.

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.

Committee. Among other things, the complainant argued that the grounds that NSM gave for its decision were inadequate.

The Committee asked NSM whether the grounds given to the person for whom security clearance was requested (the principal person) met the requirements for grounds and information set out in Section 25 of the Security Act 1998. The complainant's case was considered in accordance with the old Security Act.

The Committee stated that, generally speaking, the grounds provided in security clearance cases should be as comprehensive as possible. This is crucial in order to enable individuals for whom security clearance is applied for to safeguard their own interests. The fact that the decision was altered to the detriment of the complainant further strengthens the requirement for independent grounds to be provided, as NSM could not refer to the grounds given by the body that made the initial decision.

The Committee concluded that the grounds given to the complainant were inadequate, and we also criticised NSM for not having informed the complainant that some pieces of information that formed part of the grounds for the decision had been omitted from the information provided to the complainant.

The Committee urged NSM to provide the complainant with more comprehensive grounds for NSM's decision. NSM complied with the request and provided new and more detailed grounds to the complainant.

8.5 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 for security clearance was received by the security clearance authority. Below is a table of case processing times for 2019 as provided by NSM.

On average, case processing times have been longer in 2019 than they were in 2018. The Committee is concerned about the long case processing times, particularly for requests for access (102 days).

The Committee will continue to keep informed about the case processing times in security clearance cases in 2020.

CASE PROCESSING TIME NSM 2019	Average case processing time overall	Average case processing time, positive decisions	Average case processing time, negative decisions
Requests for access to information	102 days ⁴⁰ (5 cases)		
Requests for security clearance	100 days	87 days (117 cases)	266 days (9 cases)
First-tier appeals	164 days	N/A	164 days (6 cases) ⁴¹
Second-tier appeals	84 days ⁴²	104 days (1 case)	87 days (65 cases) ⁴³

37 Regulations concerning Personnel Security Section 3-7 (repealed). The provision is retained in the Clearance Regulations Section 13.

38 In Chapter 6 of the Special report to the Storting on differing practices in the security clearance of persons with connections to other states, the Committee raised the question of what information the security clearance authority can give personnel who hold a security clearance to allow them to assess their situation.

39 After the quarantine period, another application for security clearance of the complainant was submitted, and this time security clearance was granted.

40 NSM also considered appeals concerning requests for access received by NSM itself and for which it was the appellate body. The case processing times for these cases were 80 and 83 days, respectively.

41 In two of these cases, the appeal was granted in part.

42 This number includes appeals that were dismissed by NSM or annulled, for example by cases being returned to the security clearance authorities to be considered in accordance with new regulations. The average case processing time for these cases was 75 days.

43 In seven of these cases, the appeal was granted in part.



9.

The Norwegian Defence Security Department (FSA)

9.1 General information about the oversight

The Committee conducted two inspections of FSA in 2019. In our inspections of the department, we focus on the following:

- FSA's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authority
- FSA's operational security activities
- FSA's processing of personal data as part of its protective security services
- FSA's cooperation with other EOS services

FSA's processing of security clearance cases is particularly important in the Committee's oversight of the department. FSA is Norway's largest security clearance authority by far, and it processes requests for security clearance from the entire defence sector. The Committee reviews many of the negative security clearance decisions made by FSA, as well as appealed security clearance cases where the department has granted the appeal in part or in full.

9.2 Follow-up of the special report on differing practices in security clearance cases

On 12 March 2019, the EOS Committee submitted a special report to the Storting on differing practices in the security clearance of persons with connections to other states.

One of the things our investigation found, was that FSA had denied six persons clearance without their cases having been sufficiently elucidated. Since the report was made public, FSA has considered these cases again, as well as another case pointed out by the Committee.

After reconsidering the seven cases, FSA agreed that they had not been sufficiently elucidated. The decisions were thus deemed to be invalid and consequently annulled, cf. the Public Administration Act Section 41. FSA informed the Committee that the persons who had been denied security clearance had been informed that the previous decision had been annulled.

The Committee was pleased that FSA has concluded that the invalid previous decision will no longer be seen as a black mark against the persons in question.

9.3 The use of written statements from persons for whom security clearance is applied for to elucidate security clearance cases

9.3.1 General information

As part of its follow-up of the special report mentioned in section 9.2 of this report, FSA informed the Committee that the department had changed its practice. In cases involving connections to other states, the department now requests the person for whom security clearance is applied for to provide a comprehensive written account of the person's own and his/her closely related persons' connections to the state in question and to Norway.

The security clearance authority shall ensure that security clearance cases are as well elucidated as possible, cf. the Security Act Section 8-4 third paragraph. In case of doubt about whether the person is suitable for security clearance, the security clearance authority shall conduct a security interview.⁴⁴

The Committee has repeatedly raised the matter of FSA's practice when it comes to elucidating security clearance cases. A central question has been whether the security clearance cases have been elucidated in such a way that a decision can be made without conducting a security interview. Among other things, the Committee has criticised FSA for obtaining supplementary information on financial matters in phone calls with the person for whom security clearance is requested,⁴⁵ and we have raised FSA's practice for elucidating financial matters with NSM.⁴⁶

The security interview is an important guarantee of due process protection in that it safeguards the individual's right to an adversarial process. In the preparatory works to the Security Act 2018, the ministry emphasised that in 2006 there was placed a stricter obligation on the security clearance authorities to conduct security interviews.⁴⁷

44 This provision continues the one set out in the Security Act 1998 Section 21 third paragraph (repealed), of which the final sentence read as follows: 'Security interviews shall be conducted in cases where such an interview is not deemed to be obviously unnecessary'.

45 The Committee's annual report for 2009, chapter V section 6.1.

46 The Committee's annual report for 2012, chapter VI section 2, FSA's practice in financial matters.

47 Official Norwegian Report NOU 2016:19 *Samhandling for sikkerhet*. ('Cooperation for security' – in Norwegian only), section 10.2.5.

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.

Closely related person

A person who is a close family member or has some other close connection with the person for whom security clearance is applied for, for example a spouse/partner or child.

The Committee's impression is that the use of written statements to obtain information in security clearance cases has increased in recent years. In addition to financial matters and connections with other countries, we have also noted that FSA has requested written statements on matters relating to health, use of intoxicating substances and criminal records, among other things. We requested an account of FSA's practice in order to determine whether written statements are used instead of the security interviews that is the general principle laid down in the Act.

FSA informed us that if it requires further elucidation of a case after receiving the personal data form, one of the options available to the department is to contact the person for whom security clearance is applied for in writing or by phone. The choice of method is based on what the case officer deems to be the most beneficial way of elucidating the case while also fulfilling the other requirements made of FSA, such as protecting its sources and safeguarding the due process protection of individuals.

If the case has then still not been sufficiently elucidated, the case officer shall schedule a security interview. FSA stated that written statements are most suited in matters of simple clarification of facts and where it would be unreasonable to demand that the person in question attend an interview. It is also useful in cases where the person for whom security clearance is requested will have to obtain a lot of supplementary information, for example in relation to certain

financial and health-related matters. On the other hand, it is useful to conduct security interviews without a previous statement in cases involving complex matters where the use of a written statement could cause important nuances to be lost or result in a longer case processing time. FSA stated that the department has in several cases conducted a security interview after receiving a written statement.

The Committee agreed with FSA that, generally speaking, obtaining information in writing to elucidate a case is not in violation of the provisions of the Security Act. Written statements will not be a suitable tool in the elucidation of cases where important nuances of the statement could be lost or where it must be assumed that there will be a need for follow-up questions.

The Committee also noted that in the forms used in cases concerning connections to a foreign state, the person for whom security clearance is requested is asked to describe his/her connection to Norway and to the foreign state in his/her own words. We stated that the security clearance authority must exercise caution when using methods other than security interviews to obtain information from persons for whom security clearance is requested, particularly when what needs to be clarified are comprehensive topics where judgement must be exercised. This is to ensure that the rule that a security interview shall be conducted in cases where there are doubts about the person's suitability for security clearance is not undermined or circumvented.



9.3.2 Criticism in a specific case

During an inspection, the Committee noted a case where FSA asked the person for whom security clearance was being applied for to provide a written statement on a number of matters.

The Committee asked FSA about the department's use of a written statement rather than a security interview in the case in question. FSA stated that the department was going to use the information obtained in writing as a basis for considering whether to conduct a security interview. FSA found it difficult to see why the security clearance authority should not be able to request further information from the person for whom security clearance was requested about a matter of importance to the case. FSA did not receive a statement from the person, and the case was later dropped because the security clearance was no longer needed.

The Committee stated that the department should have endeavoured to clarify the questions in a security interview rather than through a written statement. This was a complex matter where a written statement would entail a risk of important nuances being lost and where FSA would have had to ask follow-up questions.

FSA's questions were based on an assumption that turned out to be incorrect. A security interview would quickly have brought to light that the assumption was incorrect, and FSA's interviewers could have omitted questions that were based on this assumption. Nor could the Committee see that the answers that the person for whom security clearance was requested gave, would have been necessary to prepare for a security interview.

9.4 Complaint cases against FSA

9.4.1 Introduction

The Committee received no complaints against FSA in 2019, compared with three in 2018. We concluded one complaint case against FSA in 2019. The complaint case in question concerned more than one of the EOS services, and it did not result in criticism against any of the services.

FSA is the body that made the initial decision in many of the complaints against the National Security Authority (NSM). In two of the cases involving complaints against NSM where the Committee found that the superior body had not done anything that warranted criticism, it nevertheless criticised FSA, which had made the initial decision in the cases in question.

9.4.2 Long case processing time

In a complaint case concerning loss of security clearance, the Committee found no reason to question NSM's decision made based on the merits of the case or the processing of the appeal. However, we concluded that the total case processing time had been unreasonably long. This applied in particular to the excessively long time FSA took to make the initial decision.

The Committee stated that this was unfortunate.

FSA took *one year and four months* to make the initial decision in the case. Since, during this time, the personal data form had become too old to be used as a basis for a security clearance case, the person for whom security clearance was applied for also had to fill in a new form. FSA's internal case documents also show that the case processing time had been too long. The Committee noted that FSA apologised to the complainant.

9.4.3 FSA's handling of a request for access to documents in a complaint case concerning security clearance

In one complaint case, the Committee reviewed FSA's handling of a request for access to documents in a security clearance case. The Committee concluded that FSA had made several mistakes in its handling of this request.

The matters that warranted criticism in this case did not affect the final decision that NSM made in the appeal case based on the merits of the case, and the EOS Committee's consideration of the complaint against the decision to deny security clearance was concluded without criticism of NSM.

When the complainant received FSA's response to the request for access, the person got neither a list of the documents in the security clearance case nor information about the deadline for appealing the decision.

With reference to NSM's guide to access to information in security clearance cases, the Committee pointed out that FSA should also have referred to relevant exemption provisions for denying access. It is positive that FSA informed the Committee that, in future, the department's practice will be 'to include in the access letter a specific reference to which document has been exempt and pursuant to which provision it has been exempt'. This should also have been done in the case in question.

FSA also failed to comply with the recommendation in the NSM's guide to prepare internal grounds when considering requests for access to information. The Committee is of the

Internal grounds

An internal document that security clearance authorities are obliged to prepare in connection with security clearance decisions. This document must deal with all the material factors in the case, including the provisions on which the decision is based, the matters to which importance has been attached pursuant to Section 8-4 of the Security Act, and which facts the decision is based on.

opinion that the department should have done this.

FSA admitted that there was room for improvement when it comes to highlighting the internal assessment of access.

We also commented to FSA that we found it difficult to see why the complainant was not granted access to the 'summary of the case' in FSA's internal grounds prepared while the security clearance case was being considered for the initial decision. The summary mostly consists of a description of the facts.

The Committee stated that it is blameworthy that FSA did not give the complainant access to information obtained as part of the vetting process that the complainant was entitled to access to. We also pointed out that it is unfortunate that FSA refused to grant the complainant access to documents that had previously been sent to and received from the complainant.

As regards FSA's practice of anonymising/redacting information that the person in question had filled in and was entitled to access, FSA argued, among other things, that the department complies with the Personal Data Act Section 1, cf. EU's General Data Protection Regulation Article 5, 1 (f), 'pursuant to which FSA is obliged to refrain from disclosing personal data unnecessarily'.

The Committee found it difficult to see how granting the

complainant full access to the information filled in by the complainant would constitute unnecessary disclosure of personal data. The redaction was problematic because the person for whom security clearance is requested has a right to access this information.

Correspondence with FSA has uncovered shortcomings in several aspects of its processing of the complainant's access case. The Committee expects FSA to consider future access cases in a manner that inspires more confidence in its case processing.

9.5 Case processing times in security clearance cases

The Committee has been concerned about the security clearance authorities' case processing times in security clearance cases for several years. 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 2019⁴⁸ as provided by FSA.

The Committee is somewhat concerned about the long case processing times for negative initial decisions (222 days).

The Committee will continue to keep informed about the case processing times in security clearance cases in 2020.

CASE PROCESSING TIME FSA 2019	Average case processing time overall	Average case processing time, positive decisions	Average case processing time, negative decisions
Requests for access to information	20 days (32 cases)		
Requests for security clearance	27 days	23 days (17,418 cases)	222 days (323 cases)
First-tier appeals	168 days	190 days (10 cases)	163 days (46 cases)

⁴⁸ The figures that FSA reported for 2018 and the EOS Committee reproduced in its annual report for 2018 have since been found to be incorrect. Therefore, the figures for 2019 cannot be compared with them.

10.

Oversight of other EOS services

10.1 General information about the oversight

The Committee oversees EOS services regardless of which part of the public administration the services are carried out by.⁴⁹ The oversight area is defined by function rather than being limited to certain organisations.

Following the 2017 amendment of the Oversight Act, 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 did not receive any complaints against other intelligence, surveillance or security services in 2019.

10.2 Inspection of the Army Intelligence Battalion

During the Committee's inspection of the Army Intelligence Battalion (Ebn) at Setermoen in Troms county, we were briefed about the battalion's ongoing activities since the previous inspection in 2018. Deployment of personnel, exercises and the new cooperation agreement between the Army and the Norwegian Intelligence Service (NIS) were also among the topics dealt with.

The main topic of the inspection was cooperation between Ebn and the NIS. When Ebn assists the NIS, the Ebn personnel in question are placed under the command of the NIS. This means that the head of Ebn is not formally responsible for the intelligence production that takes place under the command of the head of the NIS.

For this reason, the 2019 inspection of Ebn was partly considered an inspection of the NIS. The NIS management was represented during the inspection at Setermoen.

The Committee inspected Ebn's computer systems and selected paper documents. The inspection did not give grounds for follow-up.

10.3 Inspection of the Norwegian Naval Special Operations Commando - MJK

Pursuant to the Oversight Act Section 7, the EOS Committee shall conduct one inspection per year of the Norwegian Special Operation Forces. The need for oversight relates in particular to the risk of the special operation forces' capacity being used to engage in intelligence activities in Norway in peacetime or of personal data being processed without a legal basis.

In 2019, we inspected the Norwegian Naval Special Operations Commando at Haakonsvern in Bergen. The Committee was briefed about the unit's organisation, tasks and capabilities. A more detailed briefing about the regulatory framework for the MJK was provided after the inspection. The inspection did not give grounds for further follow-up.

10.4 Technical equipment on loan from the Norwegian Special Operation Forces to PST

During the EOS Committee's inspection of the Norwegian Police Security Service (PST) in December 2017, we requested an account of any technical equipment borrowed from the Norwegian Special Operation Forces. The head of PST gave a short general briefing about borrowing of equipment from the Norwegian Armed Forces without specifically referring to equipment borrowed from the Norwegian Special Operation Forces. During a subsequent inspection of the Norwegian Special Operations Commando - FSK at Rena military base in February 2018, we asked about FSK's logging of technical sensors lent to the EOS services or others. The reply was that FSK's sensors are never lent to parties outside the special operation forces.

It emerged in subsequent correspondence with Norwegian Special Operation Command in Oslo, which FSK is subordinate to, that FSK had lent a technical sensor to PST in 2013. Seen in conjunction with information received from the Norwegian Special Operation Command, it turned out that the special operation forces had lent technical equip-



Photo: Mats Heimland/Forsvaret

ment to PST on two occasions, once in 2013 (FSK) and once in 2016 (MJK). This technical equipment had capabilities that could interfere with protection of privacy. The Committee was not informed about these loans during its inspection of PST in December 2017.

The Committee criticised FSK for having provided incorrect information during the inspection in February 2018.

We remarked to PST that, in relation to the Committee's oversight of cooperation between the EOS services, it is in principle problematic that the Committee was not informed in connection with its inspection in December 2017 that PST had borrowed technical sensors from the Norwegian Special Operation Forces.

In 2019, the Committee stated in its concluding letters to the Norwegian Special Operation Forces and PST, respectively, that documentation and traceability should be ensured when the police borrows technical sensors from the Norwegian Special Operation Forces, among other things to facilitate our subsequent oversight.

We also emphasised to PST that it is important for us to be aware of the methods and technical equipment at the service's disposal at all times. We therefore expect to be informed in future when PST acquires new technical sensors, equipment, methods or similar that could interfere with protection of privacy.

10.5 The Norwegian Civil Security Clearance Authority (SKM)

10.5.1 Inspection

In the summer of 2016, the Storting decided to reduce the number of security clearance authorities and establish a

single security clearance authority for the civil sector. The Norwegian Civil Security Clearance Authority (SKM) started processing security clearance cases on 3 April 2018. In the course of 2018, SKM took over the portfolios of 25 civil-sector security clearance authorities. This reduction in the number of authorities can help to strengthen the professional quality of security clearance work, which could contribute to improving the due process protection of individuals as well as the general public's confidence in satisfactory case processing and equal treatment in an administrative process which is partly exempt from public access.⁵⁰

The Committee carried out an inspection of SKM in 2019. During the inspection, the Committee focused in particular on the authority's negative security clearance decisions and case processing practices. The Committee was also briefed about SKM's work to take over portfolios from other security clearance authorities. Among other things, SKM stated that it has identified many differences in how security clearance work has been carried out. In our opinion, this emphasises the importance of gathering security clearance authority in the civil sector in the hands of a single organisation.

10.5.2 Case processing times in security clearance cases

The Committee has been concerned about the security clearance authorities' case processing times in security clearance cases for several years. 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 2019⁵¹ as provided by SKM.

The Committee is of the opinion that the case processing times for negative initial decisions (190 days) should be shorter.

The Committee will continue to keep informed about the case processing times in security clearance cases in 2020.

CASE PROCESSING TIME SKM 2019	Average case processing time overall	Average case processing time, positive decisions	Average case processing time, negative decisions
Requests for access to information	9 days ⁵² (30 cases)		
Requests for security clearance	55 days	51 days (4430 cases)	190 days (117 cases)
First-tier appeals	95 days	172 days (2 cases)	87 days (20 cases)

49 Cf. the Oversight Act Section 1 first paragraph.

50 The Committee has expressed this view, for example in our annual report to the Storting for 2015, section 5.1.

51 a: The statistics only cover security clearance cases. SKM also processes access clearance cases, for which the case processing time in 2019 was 44 days. b: SKM uses the term 'inherited cases' to describe cases transferred from former security clearance authorities. The average case processing time for such cases is more than a year. c: SKM also has statistics showing that on average, more than a month passes in security clearance cases from the date when the person for whom security clearance is applied for signs the personal data form until the form is received by SKM.

52 The average case processing time for appeals in cases concerning access to information was 33 days.

10.6 Follow-up of inspection of the Office of the Auditor General of Norway

In its annual report for 2018, the Committee described its follow-up of an inspection of the Office of the Auditor General of Norway's personnel security service. The Committee criticised the Office of the Auditor General for not having given people who were denied security clearance grounds for the decision. The Office of the Auditor General admitted that the persons should have been given grounds for the decision and stated that such a practice would be established.

The Committee has stated that it is pleased that the Office of the Auditor General has changed its practice. Persons who receive a negative decision will now be given grounds for the decision as required by the provisions of the Security Act. The Committee has assumed that the Office of the Auditor General has remedied the error by ensuring that persons who had not previously been given grounds have now received them.

The Committee also referred to one specific case that had not been sufficiently well elucidated and documented to enable the Committee to verify the decision. We therefore requested feedback from the Office of the Auditor General on what action would be taken based on the Committee's remarks.

The Office of the Auditor General informed the Committee that the person in question had not provided adequate information and that in any case, the person no longer needed security clearance.

The Committee let the case rest after receiving the Office of the Auditor General's statement.

The Committee emphasised on a general basis that a negative security clearance decision will still be seen as a black mark against a person, even though the person in question no longer needs security clearance. It is therefore crucial that the security clearance status does not remain 'no clearance' without this being based on satisfactory processing of the case.

Personnel security

Measures, actions and assessments made to prevent persons who could constitute a security risk from gaining any access that could result in a security breach.

Communication and external relations in 2019



11.1 Introduction

The EOS Committee would like 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.

The Committee also publishes media summaries on news stories and reports of relevance to the intelligence, surveillance and security field, both on its website and via its Twitter account. External parties can also receive these summaries via email.

An overview of the meetings, visits and conferences that the Committee and the Secretariat have attended in 2019 is provided in Appendix 1.

11.2 External relations

Provided that we are able and are not prevented by our duty of secrecy, we want to be available to answer questions from the media, researchers and others. We also give talks, and in 2019 the committee chair gave talks on democratic oversight to students at the School of Intelligence, which is organised under the Norwegian Intelligence Service, and at the Norwegian Defence University College.

The committee chair and the Secretariat's senior technological adviser have also given talks about the right to complain in security clearance cases and how the EOS Committee can oversee facilitated bulk collection (digital border defence) if the Storting decides to allow the NIS to use this method.

In connection with the development of the Secretariat's technology unit, we have also prioritised resources for competence-building measures and courses/conferences in Norway and abroad, including courses on artificial intelligence. Representatives of the Committee and the Secretariat have also attended several oversight conferences, including in The Hague and in London.

The Committee has continued to cooperate with other oversight bodies in 2019. See section 3.2 for more details.

In 2019, the Secretariat contributed to a publication from the German think tank Stiftung Neue Verantwortung – *Data-driven Intelligence Oversight*.⁵³ Furthermore, we have written the article 'Bridge of trust', which deals with contact

between oversight bodies and civil society, for the think tank's 'intelligence blog' *About:intel*.⁵⁴

11.3 Nordic meeting for oversight bodies

Since 2013, the oversight bodies for secret services in the Nordic countries have met every two years. The EOS Committee hosted the conference in 2019. This was the first time the conference was attended by representatives of Finland, where dedicated oversight bodies for secret services were only established last year. The Nordic oversight systems are different, but nevertheless similar enough for it to be useful to meet and share experience and discuss oversight methods. The meetings are kept at an unclassified level.

The topics of this year's meeting included radicalisation, control of bulk collection of raw data (such as facilitated bulk collection etc.) and artificial intelligence in an oversight context. The next Nordic meeting will take place in Stockholm in 2021.



November 2019 representatives from oversight bodies in Sweden, Denmark, Finland and Norway met in Oslo. Photo: The EOS Committee

11.4 The EOS Committee's annual conference

Our third annual open conference was held in 2019. The number of participants has increased every year. The topics included oversight pursuant to a new Intelligence Service Act, security clearance, oversight cooperation across national borders, and a discussion of what it means when the EOS Committee is charged with ensuring that the services 'do not unduly harm the interests of society'.⁵⁵

The annual conference 2020 was planned in connection with publication of this report, but was cancelled due to the Coronavirus-situation.

⁵³ https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf

⁵⁴ <https://aboutintel.eu/bridge-of-trust/>

⁵⁵ Cf. the Oversight Act Section 2.



12.

Appendices

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

Talk at defence conference

The committee chair gave a talk on technology, intelligence and oversight at Oslo forsvarsforenings security conference in January.

Committee seminar on the new Intelligence Service Act

As part of the process of preparing the Committee's consultation submission on the draft bill for a new Act relating to the Norwegian Intelligence Service, the Committee held a seminar in January to which we invited Olav Lysne and representatives of the Norwegian Data Protection Authority and the Norwegian National Human Rights Institution (NIM).

Talk at the University of Oslo

The head of the Secretariat's technology unit gave a talk on oversight of facilitated bulk collection/digital border defence at the AFsecurity forum at the University of Oslo.

Meeting on new Intelligence Service Act

In January, the Secretariat attended a meeting at NIM on the draft bill for a new Act relating to the Norwegian Intelligence Service.

Meeting of the group of cooperating oversight bodies in The Hague

In January, three representatives of the Secretariat attended a meeting at secretariat level of the group now known as the Intelligence Oversight Working Group (IOWG). The group originally comprised the oversight bodies of the Netherlands, Belgium, Switzerland, Denmark and Norway. The UK oversight body joined the group in 2019. See section 3.2 for more details.

Panel on new Intelligence Service Act

In February, the head of the technology unit of the Secretariat took part in a panel on the new Intelligence Service Act at an event hosted by the Norwegian Computer Society.

Participation in Arbeidslivsdagene career information event for law students in Oslo

In February, the head of the secretariat gave a talk on what the EOS Committee does and what kind of work there is for the legal advisers. Three secretariat employees were available at a stand to talk to interested law students.

Participation at cybersecurity conference

Two employees from the Secretariat's technology unit attended the cybersecurity conference HackCon14.

Chair meeting of the Intelligence Oversight Working Group – IOWG

The committee chair and the head of the technology unit attended a chair meeting of the Intelligence Oversight Working Group in Brussels in March. See section 3.2 for more details.

IT security course

The head of the technology unit attended an IT security course in London in March.

Meeting with the Norwegian Data Protection Authority

Three secretariat employees had a meeting with the Norwegian Data Protection Authority in March at which oversight methodology experience was shared.

Annual conference

The EOS Committee hosted its third annual conference. The conference took place at the House of Literature in Oslo in March, and nearly 150 people attended. The topics included oversight pursuant to a new Intelligence Service Act, security clearance, oversight cooperation across national borders, and what it means that the EOS Committee is charged with ensuring that the services 'do not unduly harm the interests of society'.

Talk at NTL conference

The committee chair gave a talk in April at conference on security clearance hosted by the the Norwegian Civil Service Union (NTL). Two secretariat employees also attended the conference.

Meeting with the minister of defence

The Committee met with Minister of Defence Frank Bakke-Jensen in May. The topics included the Ministry of Defence's management of the Norwegian Intelligence Service, the new Intelligence Service Act and international cooperation between oversight bodies.

Oversight workshop in Berlin

In May, two secretariat employees took part in a workshop on innovation in oversight methodology under the auspices of the think tank Stiftung Neue Verantwortung. This workshop formed part of the basis for the publication *Data-driven intelligence oversight*.

Artificial intelligence conferences in London

A secretariat employee attended the O'Reilly Strata Data & AI conference in London in late April/early May. The focus of the conference was data science, machine learning and artificial intelligence.

The head of the technology unit attended the AI Summit conference in London in June.

Software developers' conference in Oslo

A secretariat employee attended the NDC conference in Oslo in June.

Seminar with the Communications Surveillance Control Committee

Three secretariat employees took part in a seminar on equipment interference hosted by the Communications Surveillance Control Committee in June. There was a follow-up meeting in September.

Meeting of the Intelligence Oversight Working Group – IOWG

In June, two secretariat employees participated in a working meeting of the Intelligence Oversight Working Group in Copenhagen. See section 3.2 for more details.

Talk at the Security Festival

In August, the head of the technology unit gave a talk on oversight of facilitated bulk collection/digital border defence at the Security Festival in Lillehammer.

Meeting with judges with security clearance

In August, the Committee met with judges working at Oslo District Court and Borgarting Court of Appeal who have been granted security clearance and consider requests from PST for permission to use covert coercive measures.

Conference on artificial intelligence

The head of the technology unit attended an AI conference in San Jose, the USA, in September.

Software developer conference

A secretariat employee attended the Javazone conference in Oslo in September.

IT security conference in the Netherlands

The head of the technology unit attended the One Conference in The Hague in October. This IT security conference was hosted by the Dutch authorities.

International oversight conference in London

In October, the committee chair and a secretariat employee attended the International Intelligence Oversight Forum in London. The forum brings together people from different continents who work in oversight of secret services. It is also attended by people who work in the services or ministries, as well as judges and politicians. The conference was held for the fourth time under the auspices of the UN Special Rapporteur on the right to privacy, Joe Cannataci.

Participation and talk at the dagen@ifi career information event in Oslo

Three secretariat employees manned a stand at the career information day for IT students at the University of Oslo in October. One of them gave a talk on oversight of facilitated bulk collection/digital border defence.

Nordic meeting for oversight bodies

In November, the Committee hosted a Nordic meeting for bodies that oversee intelligence and security services. Denmark, Sweden and Finland participated. See section 11.3 for more details.

Meeting with an expert on Russia

Senior Research Fellow Julie Wilhelmsen of the Norwegian Institute of International Affairs (NUPI) gave a lecture to the Committee on Russian foreign and security policies.

European oversight conference in the Netherlands

In December, the committee chair and three secretariat employees attended a European control conference in The Hague under the auspices of European oversight bodies. The chairs of the collaboration group Intelligence Oversight Working Group met in connection with this conference. See section 3.2 for more details.

Talk on our special report

In December, a secretariat employee gave a talk on the Committee's special report to the Storting on PST's unlawful collection and storage of information about airline passengers at a meeting with the Norwegian National Human Rights Institution (NIM).

Data conference in Oslo

In December, three secretariat employees attended the conference *Rethinking 2019: Verdien av Data* ('the value of data') under the auspices of the media group Schibsted and the Norwegian newspaper Aftenposten.

Events for which no other location is specified have taken place in Oslo. In addition to the events mentioned above, the Committee and Secretariat have attended events and smaller meetings and given talks to various smaller organisations.

APPENDIX 2 – News from foreign oversight bodies

Finland

In 2019, Finland established its first dedicated and independent oversight bodies for the intelligence services. An Intelligence Ombudsman and a parliamentary Intelligence Oversight Committee for the two Finnish intelligence services were appointed. The Ombudsman is independent, but appointed by the government. The Ombudsman has the authority to make binding decisions, for example order the discontinuation of use of coercive measures, and has full right of inspection of the services. The Ombudsman is also an appellate body.

Denmark

The Danish Intelligence Oversight Board criticised the Danish Defence Intelligence Service (DDIS) and the Danish Security and Intelligence Service (PET). The reason for the criticism was that DDIS had unlawfully shared surveillance data about Danish persons with PET. PET asked DDIS to conduct searches in raw data collected by DDIS without having obtained a court order.

It was debated in Denmark in 2019 whether the Danish Intelligence Oversight Board should be given a broader remit. At present, the Danish Intelligence Oversight Board is largely only able to oversee the services' processing of personal data, and not, for example, the services' work in relation to HUMINT and sources.

Sweden

The Swedish Commission on Security and Integrity Protection oversees the use of covert coercive measures, surveillance and processing of personal data by the police, including the Swedish Security Service, and the prosecuting authority. In 2019, it criticised the prosecuting authority of Malmö for having sought the court's permission to continue secret surveillance for longer than the law permits.

The Netherlands

Since the Netherlands introduced the new Intelligence and Security Services Act, which includes bulk collection of information from cable traffic, among other things, the oversight body CTIVD has submitted several follow-up reports in which it points out that several statutory preconditions for the introduction have still not been met. Since the new 'intelligence reform' came into force, CTIVD's Complaints

Handling Department can make binding decisions.

In 2019, CTIVD criticised the two Dutch intelligence services for several things, including how the services share raw data with foreign partners and how information is filtered when communication data are collected in bulk.

Switzerland

Like in several other countries, Switzerland has implemented an intelligence reform in recent years that means that the intelligence services are now allowed to use more methods. Another effect has been that the country has introduced a new and more independent oversight body. This oversight body, abbreviated AB-ND, issued its first public annual report in 2019. In addition to reviews of legality, the Swiss body will also oversee how effective the intelligence services are. The oversight body does not consider complaints, but writes in its annual report that tips from the public may be used as a basis for oversight activities.

The UK

The UK oversight body, the Investigatory Powers Commissioner's Office (IPCO), conducts advance and subsequent oversight of the British secret services, police and other organisations permitted to use covert coercive measures and lawful interception of communication. The annual report for 2017, published by IPCO in 2019, states, among other things, that they were not persuaded that GCHQ (the signals intelligence service) officers understood how intrusive the nature of their work can actually be the citizens.

Canada

The parliamentary oversight committee for the Canadian secret services, the National Security and Intelligence Committee of Parliamentarians, is a young organisation and submitted its first annual report (for 2018) last year. Before this committee was appointed, Canadian military intelligence was not subject to independent oversight.

The even more recently established non-parliamentary oversight body the National Security and Intelligence Review Agency (NSIRA), which was created through a merger of several previous oversight bodies, will oversee all of Canada's intelligence and security services in future. The NSIRA was established in 2019, and will probably in time become

HUMINT

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

the world's largest independent oversight body for secret services. Canada will also appoint an intelligence commissioner, whose role will be to approve certain intelligence operations in advance.

USA

The NSA's Inspector General has pointed out in a public semi-annual report that the NSA does not have adequate documentation when sharing data with cooperating foreign services. The report also questions whether the service's staff has sufficient training in how to process such data.

The Privacy and Civil Liberties Oversight Board, whose remit is to oversee all intelligence services with a role in the USA's anti-terrorism efforts, has in 2019 overseen, among other things, the use of airline passenger information, NSA's collection of telephone metadata, NSA's use of the computer program XKeyscore, and the use of facial recognition and biometrics.

France

Unlike several other oversight bodies for secret services in Western Europe (including the EOS Committee), the French oversight body CNCTR does not have access to information about what the French intelligence services share with their partners. In 2019, the French oversight body asked to be granted access to such information.

Belgium

The remit of the Belgian oversight body for the secret services has been broadened several times in recent years. In the annual report for 2017, published in 2019, the committee chair is quite clear that it is a very difficult situation to be in to be required to cut their budget at the same time as parliament is adding to their workload.

New Zealand

The Inspector-General of Intelligence and Security criticised New Zealand's services for having been too passive when they received intelligence reports based on use of torture by the CIA in Afghanistan.

APPENDIX 3 – Report on the security interviews project

1. Introduction

The security interview is an important tool in the security clearance authority's toolbox. The function of the security interview is twofold: Firstly, the security clearance authority can ask questions to map and elaborate on relevant facts relating to the principal person. Secondly, the way in which the principal person describes, reflects on and relates to these facts may provide important information about the person's reliability, loyalty and judgement.

The EOS Committee has advocated increasing the use of security interviews in security clearance cases. The Committee has previously stated that the security interview helps to safeguard the right to an adversarial process and serves as an important guarantee of due process protection.⁵⁶

Since 2013, the EOS Committee has focused on how security interviews are conducted. The Committee referred to its dialogue with the National Security Authority (NSM) about security interviews in the Committee's annual reports for 2013–2016. Matters raised by the Committee include:

- whether the method for conducting security interviews is appropriate and adequately ensures the right to an adversarial process,
- whether the form of the interview is sufficiently flexible and adapted to the individual case,
- time use during interviews, and
- whether the question of the principal person's suitability for security clearance is given adequate attention in the interview.

⁵⁶ The Committee's annual report for 2013, chapter V section 4.1.

2. The EOS Committee's review of security interviews

In the annual reports for 2014 and 2015, the Committee raised the question of whether an external evaluation was required of how security interviews are conducted. The conclusion was that, in light of the dialogue with NSM and the measures due to be implemented, there was no need for such a review in 2015.

The EOS Committee has previously reviewed some security interviews as part of its dialogue with NSM during the period 2013–2016. In 2018, the Committee decided to carry out a more comprehensive review of security interviews. The Committee obtained and reviewed 30 security interviews, 15 of which were conducted by FSA and 15 by NSM. The interviews were selected based on main topics, with six interviews on financial matters, six on mental health, six on criminal offences and twelve on connections to foreign states. All of the cases were from 2017.

The purpose of the project has been to examine whether security interviews are now prepared and carried out in such a manner that they meet the security clearance authorities' need for information about the principal person's suitability for security clearance while also ensuring that the person in question is given a chance to comment on the relevant topics. The Committee has also looked at whether the method for conducting security interviews is flexible and adapted to the individual cases. The goal of the project was not to review the processing of each individual case in its entirety, but to assess security interviews at a more general level.

3. The legal basis for security interviews

The Security Act Section 8-4 second paragraph states that when assessing whether a person is suitable for security clearance, the security clearance authority can attach importance to matters that are relevant to the person's reliability, loyalty and judgement in relation to processing of classified information and access to sensitive objects and infrastructure.

Pursuant to the Security Act Section 8-4 third paragraph second sentence, the security clearance authority shall conduct a security interview if there is doubt about whether a person is suitable for security clearance.⁵⁷ The Clearance Regulations Section 19 state that the purpose of the security interview is to obtain information for the purpose of considering whether a person is suitable for security clearance pursuant to the Security Act Section 8-4.

A number of factors that may be relevant in the assessment of a person's suitability for security clearance are listed in the Security Act Section 8-4 fourth paragraph letters a)–o).

The security clearance authority can attempt to clarify all these matters by means of a security interview.

This means that at present, a security interview should take place in all security clearance cases that involve doubt. The security interview can only be omitted in cases where it is clear that the principal person can be granted or must be denied security clearance.

4. Model for conducting security interviews

4.1 Model for security interviews

The model used for security interviews was developed on the basis of the interview/interrogation technique PEACE. The PEACE model consists of five phases:

- P – Planning and preparation
- E – Engage and explain
- A – Account clarification and challenge
- C – Closure
- E – Evaluation

Phase P is the preparation phase. Phase E (Engage & explain) begins when the service meets with the principal person, and is followed by the other three phases.

The Committee's review found that 27 of the 30 security interviews included in the project followed a very similar model.

Before the interview

- The principal person is summoned for an interview.
- A preparatory memo is written

The interview

- Introduction to the interview
- Free narrative account
- Specific questions about the topic
- Suitability for security clearance
- Conclusion
- Evaluation with the principal person

The remaining three interviews deviated somewhat from the model. Two of the three lacked a clearly defined section on suitability for security clearance, but questions relating to this topic were asked in the course of both the interviews. One was a follow-up interview and therefore contained only some of the elements from the model.⁵⁸

5. The Committee's remarks

5.1 General information

The EOS Committee believes that there has been a positive development in how security interviews are conducted. The overall quality of the interviews has, with some exceptions, improved compared to interviews previously reviewed by the Committee.

The quality of security interviews conducted by FSA is also significantly better than the quality of those conducted by NSM. This gives cause for concern, both because security interviews are an important tool for ensuring adversarial process and because NSM is both the expert authority and the appellate body in security clearance cases. The Committee is of the opinion that there is room for improvement in the security interviews of both these security clearance authorities, but that FSA has come a long way in terms of dialogue, a flexible approach and guiding the principal person.

The Committee also found that several of the problematic features of the interview model that the Committee has previously pointed out still remain. Among other things, suitability for security clearance is the topic to which the least time is devoted during the interview, time is not always used in an appropriate manner, and it takes time to get to the relevant topics.

5.2 Preparations for interviews

Good preparations are important in order to ensure that all relevant topics are covered and that resources are used in an effective manner. The security clearance authority prepares two documents for each interview. The principal person receives a summons containing practical details and some information about the interview, while the security clearance authority draws up preparatory notes for its own use.

Summons to security interviews are mostly quite uniform. They contain the practical details, information about the interview, information about what the information is used for, video recording and the principal person's duties. The Security Act's provisions on security interviews are enclosed with the summons. It does not state what topic(s) the interview will cover.

The preparatory notes for the 30 interviews in question varied greatly in both scope and content. The shortest consisted of a three-page pages of points to be covered during the interview, while the longest comprised 18 pages of detailed questions. The Committee takes a positive view

of the fact that several of the preparatory notes contain specific questions relating to the facts of the case in question. However, the majority of them were dominated by generic questions about the topic of the interview, sometimes at a very detailed level.

The Committee still believes that it should be possible for the security clearance authorities to inform the principal person of why he or she has been summoned for a security interview and what the topic(s) of the interview will be. As regards the interviews reviewed by the Committee, 10 of the 29 persons summoned stated that they had guessed the topic and came prepared to talk about it. This may have enabled them to provide better and more comprehensive answers to allay the security clearance authority's doubts. The remaining 19 did not make any explicit statements to this effect. The Committee noted that in one interview, the principal person had prepared for a different topic than the one the security clearance authority wished to discuss. The interview in question did not go well. There were also differences in terms of whether the principal person had brought documents to aid their memory. The persons who did so, found it easier to answer the most detailed questions.

5.3 Suitability for security clearance

The principal person's suitability for security clearance is the main topic of any security interview. The purpose of the interview is to shed light on the person in question's reliability, loyalty and sound judgement.⁵⁹ The principal person's understanding and awareness of matters in his or her own life that could form a basis for external pressure or conflicting loyalties will be crucial in the assessment of the person's suitability for security clearance. The Committee's view is that it warrants criticism that this topic continues to receive relatively little attention in security interviews.

The topic is rarely touched on in the introduction to the security interviews. Only in 4 out of 29 interviews did the security clearance authorities explicitly mention the concepts of reliability, loyalty and sound judgement or suitability for security clearance during the introduction.

Suitability for security clearance is not often brought up in connection with questions about the topic of the conversation (financial situation, mental health, criminal offences, connections to foreign states). In 8 out of 29 interviews, the security clearance authority brings the topic up – normally in the context of dialogue with the principal person about why the questions are asked. In some cases, the principal person him/herself brings it up in his/her answers.

57 Cf. the Security Act 1998 Section 21 third paragraph third sentence: 'Security interviews shall be conducted in cases where such an interview is not deemed to be obviously unnecessary.'

58 This interview was omitted from several of the Committee's summaries, as the way in which it was conducted is not directly comparable with the rest of the sample.

59 The Security Act 1998 Section 21 used the term 'sound judgement'. This was changed to 'judgement' in the Security Act 2018. As the security interviews reviewed by the Committee took place in 2017, we have used the term 'sound judgment' in this report.

The Committee notes that questions that gave the principal person a chance to reflect on his/her own judgement were asked during all the interviews. The quality of these questions varied, but there were attempts to trigger reflection on the part of the principal person. In many of the interviews, the principal person reflected on his/her own initiative on choices and assessments made.

27 of the 29 interviews contain a separate section on suitability for security clearance. This is introduced after questions about other topics have been asked, usually towards the end of the interview. Nonetheless, there is considerable variation in how the matter is broached during this phase. Only in 11 out of 29 interviews did the security clearance authority explicitly use the terms 'reliability, loyalty and sound judgement'. In most of the interviews, the discussion of suitability for security clearance was opened in some other manner, for example via questions about the duty to provide information, authorisation, workplace procedures, what it means to hold security clearance, or challenges and vulnerabilities. In some interviews, the security clearance authority's questions about suitability for security clearance were so vague that the principal person did not understand the question. In other interviews, good and direct questions are asked and linked to the preceding dialogue, for example:

'We are here to evaluate your reliability, loyalty and sound judgement. Based on what you have told us, how will you describe yourself in relation to these terms?'

The Committee finds this to be an opening that emphasises the purpose of the interview while also encouraging the principal person to assess and reflect on his/her own situation. During its review of the interviews, the Committee observed that in cases where there was good dialogue between the security clearance authority and the principal person, the topics of duty to provide information, reliability/loyalty and sound judgement often came up at an earlier stage. The security clearance authorities also received better and more comprehensive answers in cases where they explained the concepts or explained why the questions were asked.

In the Committee's opinion, it should be made clearer to the principal person that suitability for security clearance is at the core of the interview. Also, more time should be spent getting the person to assess and reflect on his/her own situation. It is a positive thing that this has become a fixed item on the interview agenda, but it should be a recurring topic *throughout* the interview.

5.4 Interview management and time use

As mentioned, the EOS Committee has also previously focused on the security interview being a flexible tool. Conducting a security interview with two staff members from the security clearance authority present along with the principal person is a resource-intensive task. The interview itself can also be very wide-ranging and include many questions of

a personal nature, which may be stressful for the principal person. In its previous dialogue with NSM, the Committee has expressed the opinion that one should consider whether some security interviews can be conducted in a less resource-intensive way by taking a flexible approach to the use of resources, scope etc.⁶⁰

The interviews that the Committee has reviewed varied in complexity and length. The shortest interview lasted 1 hour, while the longest one lasted for 5 hours and 44 minutes, including breaks. The average duration of the security interviews was 2 hours and 55 minutes. 9 of the 30 interviews were shorter than 2 hours, while 4 exceeded 5 hours. Most of the interview time was spent on questions and answers about specific topics. The principal person's free narrative account about him/herself also took up a lot of time. Some time was also spent reflecting on suitability for security clearance.

In the Committee's opinion, there is still reason to question whether the time is spent in an appropriate manner in these cases. As mentioned above, the Committee is of the opinion that more of the time should be given to reflection on the principal person's suitability for security clearance. The Committee also questions whether what can be gained from the principal person's free narrative account always justifies the time spent. In the ten cases where the principal person arrived prepared to discuss a specific topic, they were normally asked to wait until after the free narrative to do so. There was a 'delay' of between 17 minutes and about an hour. The Committee also observed that some principal persons found it confusing to be asked to talk about themselves instead of answering questions asked by the security clearance authority. In some of the interviews, trust was established already during the introduction when the security clearance authority gave a more detailed explanation of the purpose of the interview.

The Committee has also looked into the flexibility of the form of interview. In principle, it should be possible to adapt the number of questions and their form and scope depending on what the principal person tells the interviewers. The Committee has noted that FSA in particular tries to omit irrelevant questions and ask follow-up questions to what they are told without being too bound by their preparatory notes. This is positive. However, there are also several interviews where the preparatory notes are followed point by point with the result that the principal person ends up describing the same things two or three times.

The Committee would like the security clearance authorities to have a clearer idea of what constitutes 'enough' information about a topic. In several interviews, the principal person was asked repeatedly about the same topic. The Committee's observations show that in several cases, it was only once the security clearance authorities explained why a question was being asked that the principal person gave an

‘adequate’ answer so that the interview could progress.

It is also a positive thing that the security clearance authorities use the breaks to adjust the course of the interview. It would not be a bad idea to do so more often. The Committee has observed that despite being encouraged to do so, principal persons rarely ask for a break. Breaks normally take place at the security clearance authority’s initiative.

The dialogue between the principal person and the security clearance authority is of great importance to the quality of the interview. It made a lot of difference whether the security clearance authority managed to engage the principal person in dialogue. It was easier for the security clearance authority to get good answers to their questions in interviews where dialogue was good, and the answers yielded more information. At the same time, good dialogue demands more of the authority’s interview management to avoid repetitions and too much excessive small talk.

6. Concluding remarks

It has been very useful for the Committee to review this many security interviews together. The interviews varied in length, complexity and quality. The sample included both first-time clearance and reclearance cases, and in one case a second security interview in the same case. As mentioned, the EOS Committee believes that there has been a positive development in how security interviews are conducted. However, there are great differences between interviews. Too often, the topic of the conversation is not sufficiently clearly linked to the question of whether the person in question is suitable for security clearance, and the security clearance authority cannot test the principal person’s level of reflection.

The purpose of a security interview is to clear up doubt, and it should not be used purely as a tool for obtaining factual information. The Committee also sees a general tendency towards interviews containing more factual questions than questions intended to prompt the principal person to

understand and reflect on his or her situation. The security interview is of great importance to the case, and it therefore gives cause for concern that so many interviews today do not seem to elucidate the question of whether the principal person is fit to hold security clearance.

The Committee also sees a difference between principal persons who are familiar with the security clearance system and those without such prior knowledge. Both these categories come prepared to be asked questions. However, principal persons with prior knowledge of the system are more likely to understand what they will be asked about, bring documentation, be ready to get straight to the point or make demands of the security clearance authority. The Committee also found that in one case, the principal person was largely steering the interview.

Unlike these people, principal persons who were not familiar with the system or had received insufficient guidance, needed more guidance from the security clearance authority about what security clearance is and what it means to be suitable for security clearance before they were able to give good answers. There were several examples of principal persons who misunderstood questions or whose interpretation of ‘security’ differed from that of the security clearance authority. People in this group also tended to underestimate their own importance from a security perspective, since they did not consider themselves to be ‘important enough’ to be approached by, for example, foreign intelligence services.

The Committee is therefore of the opinion that the security clearance authorities must ensure better and more consistent quality of security interviews. The Committee believes reflection on suitability for security clearance, a good atmosphere and dialogue with the principal person, good and specific preparations and a flexible approach to the actual interview to be crucial factors in determining whether this tool functions in an optimal manner. Both the preparations and the interview should therefore be better adapted to the principal person’s security situation. It should be possible for the security clearance authorities to provide more guidance and information to principal persons about the security clearance system and the purpose of the interview in order to facilitate more targeted interviews.

APPENDIX 4 – Consultation submission on lawful interception of communication in emergencies

The Ministry of Justice and Public Security
PO. Box 8005 Dep
NO-0030 OSLO

2 September 2019

Our ref.: 2019/78-3

Your ref.: 19/427

Consultation submission from the EOS Committee – consultation on lawful interception of communication in emergencies

Part I – Introduction

The EOS Committee refers to the Ministry of Justice and Public Security's consultation letter of 17 June 2019 on the proposed legal authority for lawful interception of communication in emergencies and hereby submits our consultation statement.

The EOS Committee primarily submits consultations statements in cases where proposals will have direct consequences for the Committee's oversight and/or if there are circumstances that the Committee feels should be known before the Storting considers a bill.

Part II – Comments to the proposal

It is an unsatisfactory situation if the police intercepts communication without a clear legal authority for doing so, and the EOS Committee agrees that it is important that, as far as possible, the methods applied by the police should have a basis in law. The EOS Committee agrees with the Communications Surveillance Control Committee that lawful interception of communication in emergencies, subject to approval by the court, should be made into law.

The Committee has noted that the consultation paper consistently refers to the need for a legal authority for using lawful interception of communication in emergencies and rescue situations where the *ordinary police* has a defined role. As far as the EOS Committee can tell, the consultation paper does not discuss the possibility of situations where lawful interception of communication in an emergency may be relevant for the *Norwegian Police Security Service* (PST).

The EOS Committee would like to comment that, generally speaking, it cannot be ruled out that lawful interception of communication in an emergency may also be relevant for PST, even though it is unlikely that a PST case begins as a rescue operation. PST's duties include preventing and investigating threats against dignitaries. If a dignitary was to be reported missing, the case would most likely be followed up by PST. If such a situation arises and it is unclear whether the case concerns a rescue operation or a criminal offence, it would at present be difficult, both for PST and the ordinary police, to determine which criteria to apply in relation to the use of the necessity provision. If there are indications that a dignitary may have been abducted, PST can be faced with the same situation as the ordinary police in that PST will have to use the necessity provision in Section 17 of the Penal Code to trace the dignitary in question via his or her means of communication.

The EOS Committee cannot see that the proposal set out in the consultation paper states whether it has been considered whether lawful interception of communication in emergencies could be relevant to PST. Reference is

also made to the fact that the consultation paper does not mention the EOS Committee's role as an oversight body for PST's use of coercive measures. This is illustrated in the proposed new Section 7b sixth paragraph⁶¹ and the comments relating to reporting on the use of lawful interception of communication in emergencies.⁶²

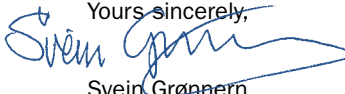
'Although the oversight model that applies to lawful interception for investigation purposes cannot be used here, there may be reason to draw on experience gained from the investigation area, see the Interception of Communications Regulations Section 10. It may therefore be natural to establish a system for reporting to the National Police Directorate, which will in turn submit quarterly reports to the Communications Surveillance Control Committee. Oversight will then be carried out by the same body that currently oversees the use of this coercive measure for investigation purposes. This would prevent uncertainty as to whether a case falls within one or the other oversight body's area of responsibility. A single oversight body would also allow the cases to be seen in a bigger picture. In addition, there is the matter of the right to bring the decision's validity before the courts, see above. If such an amendment is endorsed, the Communications Surveillance Control Committee's competence in relation to interception of communication in emergencies should be clarified.'

The EOS Committee refers to the fact that the Communications Surveillance Control Committee does not oversee cases that fall within the scope of the Oversight Act, cf. the Criminal Procedure Act Section 216 h. It is not clear to the EOS Committee why the Committee's oversight of PST's use of coercive measures is not mentioned in the consultation paper. The Committee is unsure whether the reason is:

1. that it has not been considered whether PST might need such legal authority in an emergency, or
2. that reporting should be addressed to the Communications Surveillance Control Committee also in cases when the legal authority for interception of communication in emergencies is used in PST cases, or
3. that it has been assumed when drafting the consultation paper that it already follows from the Criminal Procedure Act Section 216 h that the EOS Committee oversees the use of coercive measures in PST cases, and that oversight of any use of the proposed legal authority by PST has therefore not been mentioned in the consultation paper.

The Committee is of the opinion that the provisions of the Criminal Procedure Act Section 216 h and the Interception of Communications Regulations Section 12 mean that the Communications Surveillance Control Committee's remit must be interpreted as having limitations in relation to oversight of cases of interception of communication by PST. Any use of the proposed legal authority for interception of communication in emergencies in PST cases will, in the Committee's opinion, fall within the EOS Committee's remit pursuant to the Oversight Act.

Based on the above, the EOS Committee concludes that the proposed legal authority for lawful interception of communication in emergencies needs clarification, including as regards whether it is relevant for PST and in relation to the EOS Committee's subsequent oversight of lawful interception carried out by PST in emergencies.

Yours sincerely,

 Svein Grønner
 Chair of the EOS Committee

61 'The oversight committee mentioned in the Criminal Procedure Act Section 216 h shall oversee the way the police deal with cases pursuant to this provision.'

62 The consultation paper pages 30–31.

APPENDIX 5 – Signed charter for the Intelligence Oversight Working Group



Charter of the Intelligence Oversight Working Group

1. Members of the European Intelligence Oversight Group

This Charter establishes the Intelligence Oversight Working Group, an informal cooperation between the following oversight bodies:

- Belgian Standing Intelligence Agencies Review Committee,
Comité permanent de contrôle des services de renseignement et de sécurité /Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (Belgium);
- Danish Intelligence Oversight Board,
Tilsynet med Efterretningstjenesterne (Denmark);
- Review Committee on the Intelligence and Security Services,
Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (The Netherlands);
- EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee,
EOS-utvalget (Norway);
- Independent Oversight Authority for Intelligence Activities (OA-IA),
Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND (Switzerland);
- Investigatory Powers Commissioner's Office,
(United Kingdom).

2. Purposes of the Intelligence Oversight Working Group

The Intelligence Oversight Working Group aims to:

- strengthen cooperation between the participating oversight bodies;
- increase transparency between oversight bodies within the limits and according to the standards set by national legislators, in order to support effective oversight of international cooperation between intelligence and security services;
- exchange knowledge, experiences and best practices of oversight;
- provide a platform for developing new and/or more effective oversight methods;
- maintain contact, share information and provide each other with mutual assistance as appropriate, in accordance with the boundaries set by national laws and regulations.

3. Meetings

a) Chair meetings

The Intelligence Oversight Working Group shall annually hold at least one meeting between the chairs of the oversight bodies, or a member of the oversight body representing the chair. In principle, each chair will be supported by their head of secretariat and/or another senior staff member.



b) Staff meetings

The Intelligence Oversight Working Group shall regularly, when appropriate, hold staff meetings. The staff meetings are aimed at practically substantiating the purposes referred to in Section 2 of this Charter and carrying out the cooperation projects referred to in Section 4 of this Charter.

c) Preparation of meetings

Chair meetings shall be prepared by the oversight body hosting the meeting in cooperation with the informal secretariat referred to in Section 5 of this Charter. Staff meetings shall be prepared by the oversight body hosting the meeting. All Members voluntarily contribute to hosting meetings on a rotation basis.

4. Cooperation projects

The Intelligence Oversight Working Group may decide to enter into cooperation projects. Cooperation projects relate to a specific interest of the Group. The decision to enter into a cooperation project will be taken during a Chair meeting on the basis of a project proposal. Project proposals are prepared at staff level and shall include at a minimum:

- the intended goals for the project;
- the proposed methods to reach those goals;
- the timeframe in which the project is to be carried out.

5. Informal secretariat

The informal secretariat will be responsible for:

- reporting conclusions of the chair meetings;
- reporting conclusions of the staff meetings in cooperation with the oversight body that organised the respective meeting;
- monitoring progress on the cooperation projects;
- communication with regard to outside interest in the Group.

The secretariat will rotate every two years.

6. Information exchange

The participating oversight bodies commit to facilitating information sharing within the Group to further the purposes referred to in Section 2 of this Charter, where appropriate and in accordance with the boundaries set by national laws and regulations. The nature and extent of information sharing within the Group may also be defined by or dependent upon bilateral and/or multilateral agreements between the intelligence and security services overseen by the participating oversight bodies.

7. Membership

Extending membership of the Intelligence Oversight Working Group to other European oversight bodies on their request, shall take place on the basis of a decision by consensus taken during a Chair meeting.



8. Status, Implementation and Amendment of the Charter

This Charter reflects the intent of the participating oversight bodies within the Intelligence Oversight Working Group. Each participating oversight body commits to implementing this Charter. Amendment of this Charter shall take place on the basis of a decision by consensus taken during a Chair meeting. This Charter is not legally binding.

Signed in The Hague on 12 December 2019,

Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board

Mr. Nico van Eijk, Chair of the Dutch Review Committee on the Intelligence and Security Services

Mr. Svein Grønner, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

Mr. Thomas Fritschi, Director of the Swiss Independent Oversight Authority for Intelligence Activities

Sir Brian Leveson, Investigatory Powers Commissioner, United Kingdom

APPENDIX 6 – Letters to and from the Ministry of Justice and Public Security and the Ministry of Defence concerning sharing of information with other oversight bodies



Minister of Defence Frank Bakke-Jensen
The Ministry of Defence
P.O. Box 8126 Dep.
NO-0032 OSLO

Enclosures: 3

18 June 2019

Our ref.: 2016/68-52

Your ref.:

Query about international oversight cooperation

Dear Minister,

First of all, I would like to thank you for your visit 8 May. The Committee appreciated the meeting very much.

We refer to your request for a letter concerning the joint statement *Strengthening oversight of international data exchange between intelligence and security services*.

The background of the statement is that the oversight bodies of five countries (Norway, Denmark, Belgium, the Netherlands and Switzerland) have started to cooperate more closely in recent years than European oversight bodies have done before. We have met several times each year to discuss various issues and methods – always at an unclassified level.

We conducted a project where we looked at international data exchange between the respective countries' security and intelligence services. The project identified several challenges to oversight cooperation, primarily that while there is international cooperation between the services, oversight is only national.

A case in point: The EOS Committee oversees how the Norwegian services exchange data about Norwegian nationals with cooperating foreign services. However, we cannot oversee how the data are processed by the foreign recipient. We depend on an oversight body in the recipient country to do that. If that is not done, or if the other oversight body has a limited remit, there is a risk of an oversight gap may arise. At present, we can only discuss methods and common issues with other oversight bodies at an unclassified level.

As a result of this cooperation, we published a joint statement autumn 2018 in which we described how important it will be to strengthen the international cooperation between oversight bodies.

In this statement, the EOS Committee and the other oversight bodies also advocated minimising secrecy between cooperating oversight bodies to allow some classified information to be shared for oversight purposes.

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Nils Hansens vei 25
TEL.: (+47) 23 31 09 30
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

Our ref.: 2016/68-52

The statement did not describe how such sharing might take place. We envisage that the oversight bodies will primarily share information that has already been exchanged between the respective cooperating services. It follows from this that it will also be necessary for the oversight bodies to be able to share information that the two countries' services are cooperating. It would probably be easiest to implement this arrangement on a trial basis as part of a bilateral cooperation scheme.

One example of international oversight cooperation would be for the EOS Committee to ask a cooperating oversight body about how their service processes information about a Norwegian national received from the Norwegian Intelligence Service or PST. The foreign oversight body could investigate the matter in accordance with its own remit and provide feedback to the EOS Committee. We would be able to assist other oversight bodies in the same way if requested.

There are of course a number of challenges involved in allowing for such cooperation. Statutory amendments may be required, and guidelines must be prepared for the practical aspects of such cooperation. It will also be necessary to consider which countries to include in such cooperation arrangements.

We see a development towards increasing international data exchange between services. That is why the EOS Committee sees a need to put in place an arrangement that could reduce the risk of an oversight gap and ensure a better and more confidence-inspiring oversight regime. It is our opinion that, when data have already been exchanged between services, it should also be possible for the oversight bodies to share this information.

We would like to hear your views on the proposal to allow for limited sharing of classified information between the EOS Committee and foreign oversight bodies.

A corresponding letter has been sent to the Minister of Justice.

Please find enclosed the joint statement in English and press releases in Norwegian and English.

Yours sincerely

Eldbjørg Løwer
Chair of the EOS Committee



Enclosures: 3

Minister of Justice Jøran Kallmyr
Ministry of Justice and Public Security
P.O. Box 8005 Dep.
NO-0030 OSLO

18 June 2019

Our ref.: 2016/68-53

Your ref.:

Query about international oversight cooperation

Dear Minister,

In connection with the joint statement *Strengthening oversight of international data exchange between intelligence and security services* published by the EOS Committee and four other European oversight bodies last autumn, the Committee would like to hear the Minister's views on some of the issues pointed out in the statement.

The background of the statement is that the oversight bodies of five countries (Norway, Denmark, Belgium, the Netherlands and Switzerland) have started to cooperate more closely in recent years than European oversight bodies have done before. We have met several times each year to discuss various issues and methods – always at an unclassified level.

We conducted a project where we looked at international data exchange between the respective countries' security and intelligence services. The project identified several challenges to oversight cooperation, primarily that while there is international cooperation between the services, oversight is only national.

A case in point: The EOS Committee oversees how the Norwegian services exchange data about Norwegian nationals with cooperating foreign services. However, we cannot oversee how the data are processed by the foreign recipient. We depend on an oversight body in the recipient country to do that. If that is not done, or if the other oversight body has a limited remit, there is a risk of an oversight gap may arise. At present, we can only discuss methods and common issues with other oversight bodies at an unclassified level.

As a result of this cooperation, we published a joint statement autumn 2018 in which we described how important it will be to strengthen the international cooperation between oversight bodies.

In this statement, the EOS Committee and the other oversight bodies also advocated

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Nils Hansens vei 25, Oslo
TEL.: (+47) 23 31 09 30
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

Our ref.: 2016/68-53

minimising secrecy between cooperating oversight bodies to allow some classified information to be shared for oversight purposes.

The statement did not describe how such sharing might take place. We envisage that the oversight bodies will primarily share information that has already been exchanged between the respective cooperating services. It follows from this that it will also be necessary for the oversight bodies to be able to share information that the two countries' services are cooperating. It would probably be easiest to implement this arrangement on a trial basis as part of a bilateral cooperation scheme.

One example of international oversight cooperation would be for the EOS Committee to ask a cooperating oversight body about how their service processes information about a Norwegian national received from the Norwegian Intelligence Service or PST. The foreign oversight body could investigate the matter in accordance with its own remit and provide feedback to the EOS Committee. We would be able to assist other oversight bodies in the same way if requested.

There are of course a number of challenges involved in allowing for such cooperation. Statutory amendments may be required, and guidelines must be prepared for the practical aspects of such cooperation. It will also be necessary to consider which countries to include in such cooperation arrangements.

We see a development towards increasing international data exchange between services. That is why the EOS Committee sees a need to put in place an arrangement that could reduce the risk of an oversight gap and ensure a better and more confidence-inspiring oversight regime. It is our opinion that, when data have already been exchanged between services, it should also be possible for the oversight bodies to share this information.

We would like to hear your views on the proposal to allow for limited sharing of classified information between the EOS Committee and foreign oversight bodies.

A corresponding letter has been sent to the Minister of Defence.

Please find enclosed the joint statement in English and press releases in Norwegian and English.

Yours sincerely,

Eldbjørg Løwer
Chair of the EOS Committee



THE ROYAL NORWEGIAN MINISTRY
OF JUSTICE AND PUBLIC SECURITY

The EOS Committee
P.O. Box 84 Sentrum
NO-0101 OSLO

Your ref.:

Our ref.:
19/3357-MCS

Date
5 June 2019

Query about international oversight cooperation

The Ministry of Justice and Public Security refers to the EOS Committee's letter of 18 June 2019, in which the Committee requests the Minister of Justice's views on issues relating to the wish for legal authority to share classified information with other European oversight bodies. The Ministry will obtain assessments on the matter from the Police Security Service and the National Security Authority.

As stated by the Committee in its letter, there are a number of challenges associated with allowing for the proposed cooperation, including the need for statutory amendment. The proposal could also entail challenges relating to compliance with the third party rule. This rule is enshrined in agreements between the services and therefore cannot be changed through statutory amendments in individual countries.

In order to prepare an answer, the Ministry asks the Committee to elaborate on what it means by 'a risk that an oversight gap may arise'. That would provide a better basis for a more detailed assessment of the need for and appropriateness of the Committee's proposal 'to allow for limited sharing of classified information'.

The remits of the individual oversight bodies only cover the question of whether the services they themselves oversee operate within the bounds of their legal authority. The Ministry therefore requests the Committee to clarify its wish for a way of '(...) overseeing how the data are processed by the foreign recipient'. In particular, we request that the EOS Committee elaborate on how the Committee will use any information it may be granted access to, considering that it has a national remit.

Yours sincerely,

Unni Gunnes
Director General

Maria Collett Sælør
Senior Adviser

The document has been approved and sent without signature.

Postal address

P.O. Box 8005 Dep.
Gullhaug Torg 4a
NO-0484 Oslo

Office address

Gullhaug Torg 4a
NO-0484 Oslo

Delivery address

Varemottak
Akersgata 59
NO-0180 Oslo

Phone – switchboard

(+47) 22 24 90 90
Org. no: 972 417 831

Maria Collett Sælør



The Ministry of Justice
P.O. Box 8005 Dep
NO-0030 Oslo

3 September 2019

Our ref.: 2016/68

Your ref.: 19/3357 - MCS

Reply concerning international oversight cooperation

The EOS Committee refers to the Ministry of Justice and Public Security's letter of 5 July 2019, in which the Ministry requested that the Committee elaborate on what it means by 'a risk that an oversight gap may arise'. The Ministry also requested that the Committee clarify its wish for a way of '(...) overseeing how the data are processed by the foreign recipient' and elaborate on 'how the Committee will use any information it is granted access to, considering that it has a national remit'.

The concept of 'oversight gap' and challenges to the Committee's oversight

In the EOS Committee's cooperation with four other European oversight bodies, the term 'oversight gap' has been used to describe a potential lack of oversight of the international exchange of data between cooperating services. The oversight bodies have been concerned about our ability to conduct full and effective oversight of our own services' participation in international cooperation.

In cases where services exchange data at the request of a foreign service, the EOS Committee oversees the PST's and the Norwegian Intelligence Service's exchange of data with cooperating services on the Norwegian side of the border. It is then assumed that the remit of the receiving country's oversight body will cover oversight of the receiving service's processing of the data. A typical example is cases where the Norwegian services have set conditions for how the information can be used. It is then up to the receiving country's oversight body to oversee whether the conditions are complied with. The EOS Committee cannot investigate how information has been used abroad. If the remit of the oversight body in the receiving country does *not* cover conditions for use of information imposed by other parties, an oversight gap will arise.

If conditions imposed by Norwegian services are overseen by the receiving country, the EOS Committee currently has no way of receiving information about the results of oversight in a specific case. The Committee will therefore not be informed of any breaches of law or violation of the rights of Norwegian nationals resulting from exchange of data. If it had been possible for oversight bodies to exchange such information, the EOS Committee would have a better basis for our national oversight of the services' assessments relating to sharing of Norwegian data. This is the basis for our wish to be able to share information with other

POSTAL ADDRESS: P.O. Box 84 Sentrum, NO-0101 OSLO
OFFICE ADDRESS: Nils Hansens vei 25
TEL.: (+47) 23 31 09 30
EMAIL: post@eos-utvalget.no
WEBSITE: www.eos-utvalget.no

oversight bodies about the results from our and their oversight of data exchange between services.

International cooperation between services is increasing and takes different forms. If Norwegian services wanted to take part in closer forms of cooperation, for example in a group that works in near-real time, the EOS Committee believes that it could be challenging to ensure good oversight of the Norwegian side of the cooperation without considering the cooperation as a whole. The EOS Committee's remit does not, nor should it, extend to oversight of parties other than our own services. In our opinion, good and effective oversight over time will entail the possibility to coordinate oversight and communicate about the results of our national oversight with other oversight bodies involved. This will enable national, but comprehensive, oversight of international cooperation.

Communicating with other oversight bodies about the concrete areas covered by each body's national remit and what is overseen will also help to determine whether there are areas of cooperation that nobody has the authority to oversee, and this will make it possible to identify any oversight gaps.

Challenges relating to the development of oversight methodology

The EOS Committee's oversight methods must be developed in step with the services' introduction of new methods and forms of cooperation. The Committee has benefitted greatly from discussing oversight methodology with other oversight bodies at an unclassified level.

At the same time, our inability to share information about international cooperation can sometimes make such discussions with other oversight bodies difficult. An example of such a situation was described in the Committee's annual report for 2017, section 5.10. In the situation in question, the EOS Committee was unable to discuss information that was known to all parties in the collaboration group and was only considered classified in some of the countries.

It is the EOS Committee's opinion that in order to develop good and effective oversight of such international cooperation, it is both useful and necessary to be able to discuss methodology with other involved oversight bodies. We emphasise that in such cases, the information concerned is already known to the oversight bodies.

It will also benefit the development of oversight methodology to share with other oversight bodies some information about the results from our own oversight activities and about legal assessments relating to oversight. In some cases, it is difficult to share information in a meaningful manner without providing any context and background to the assessments. In the EOS Committee's opinion, it would be beneficial to be able to exchange some classified information about concluded oversight cases in order to achieve a broader understanding of the assessments and interpretations of other oversight bodies. This could help us to improve our oversight methods. Exchange of such classified information will always require dialogue with the service in question in advance.

The Committee hopes that this letter has provided the Ministry with further information on which to base any follow-up on the matter. The EOS Committee will of course be at your disposal to answer any further questions you may have.

Yours sincerely,

Svein Grønnern
Chair of the EOS Committee



ROYAL NORWEGIAN MINISTRY
OF DEFENCE

The Minister of Defence

The EOS Committee
P.O. Box 84 Sentrum
NO-0101 OSLO

Your ref.:

Our ref.:
2019/1227-2/FD II 5/ERMO

Date:
12 November 2019

Regarding query about international oversight cooperation

First of all, I would like to take this opportunity to thank you for our very productive and useful meeting on 7 May this year.

I also refer to the Committee's letter of 18 June, in which it provides an account of the past three years' cooperation between the oversight bodies of Norway, Denmark, Belgium, the Netherlands and Switzerland. Among other things, the cooperation resulted in the joint statement *Strengthening oversight of international data exchange between intelligence and security services*. The statement describes how important it is to strengthen international cooperation between oversight bodies. It also advocates minimising secrecy between cooperating oversight bodies to allow some classified information to be shared for oversight purposes. Such information sharing is intended to remedy a challenge currently experienced by the oversight bodies – primarily that the cooperation between services is international, while oversight is national.

In its letter, the EOS Committee expresses its concern that this divergence between the services' and the oversight bodies' possibilities to share information could give rise to an oversight gap, particularly considering the development towards increasing international data exchange between the services. The EOS Committee therefore sees a need to put in place an arrangement that could reduce the risk of an oversight gap and ensure a better and more confidence-inspiring oversight regime.

The letter requests my views on the proposal to allow for limited sharing of classified information between the EOS Committee and foreign oversight bodies. The matter has been submitted to the Norwegian Intelligence Service, and the response received forms part of the basis for my assessment.

Before going into the actual assessment, I would like to underline that international cooperation is, and always has been, important to the Norwegian Intelligence Service's performance of its duties. The Intelligence Service Act Section 3 second paragraph allows the NIS to establish and maintain intelligence cooperation with other countries. In Proposition

Postal address: P.O. Box 8126 Dep., NO-0032 OSLO
Office address: Glacisgata 1, Oslo
Phone: (+47) 23 09 80 00
Org. no: 972 417 823

No 50 to the Odelsting (1996–1997), section 2 on page 4, this is described as one of the service's primary duties. The advantages of international intelligence cooperation are vital to Norway, as a small country with limited resources. The exchange of information, which can promote a shared understanding of the situation and better and more efficient intelligence production, is a key part of such cooperation. In some areas, Norway has an obligation under international law to take part in international cooperation. Among other things, the UN has adopted a number of counter-terrorism conventions and Security Council resolutions that oblige states to contribute to the fight against international terrorism. The same applies to efforts to prevent the spread of weapons of mass destruction. Data exchange can be part of or a condition for such international cooperation. The Norwegian Intelligence Service must comply with a number of principles and requirements when disclosing information to foreign partners. It has been proposed that the conditions for exchange be codified in the new Intelligence Service Act

I understand the oversight bodies' wish to be able to share more information for oversight purposes. International experience sharing and dialogue is already contributing to improving national oversight of the respective countries' intelligence, surveillance and security services. Allowing the oversight bodies to share classified information for oversight purposes may well strengthen this cooperation further. However, the question of such a right to share information raises many issues of a legal, security-related and intelligence-related nature, and the sum of these considerations means that I cannot support the proposal to allow the Committee to share classified information with other countries' oversight bodies.

The question of how international sharing of classified information between oversight bodies relates to the principle that the Norwegian Intelligence Service should be in control of the information it possesses is particularly relevant. This principle is set out in the Instructions for the Norwegian Intelligence Service Section 4 first paragraph, which states that: 'The Norwegian Intelligence Service shall be under Norwegian control. This includes ensuring national control over what information is disclosed to foreign collaborative partners.' The wording of the Norwegian Intelligence Service Instructions does not in itself preclude the EOS Committee from sharing classified information with its partners, but the purpose of the provision is clear: the constitutional and parliamentary responsibility for the Norwegian Intelligence Service and its sharing of data rests with the Minister of Defence on behalf of the Norwegian government. It can be argued that if the EOS Committee were permitted to share intelligence information with its partners, that would constitute a breach of this arrangement.

Moreover, the EOS Committee's statutory oversight responsibility does not extend to overseeing how foreign services process information, even when the information in question originates from Norwegian intelligence activities. A service's processing of information is a national concern. Each nation is responsible for how the information it receives is used – and each oversight body is responsible for exercising its oversight in accordance with the laws of its own country.

The EOS Committee is charged with overseeing that the Norwegian services comply with the applicable regulatory framework. The EOS Committee currently has every opportunity to oversee the Norwegian Intelligence Service's compliance with the applicable rules for exchange of data, including which due diligence and risk assessments are made before information is shared. The EOS Committee is entitled to access information about and review all feedback that the Norwegian Intelligence Service receives from its partners. This allows the EOS Committee to oversee and comment on the Norwegian Intelligence Service's sharing of information.

I would also like to emphasise that allowing the sharing of information would contribute to information that is often highly sensitive to national security being disclosed to more people. This would increase the risk of classified information falling into the wrong hands, which could make cooperating services less willing to share information with the Norwegian Intelligence Service. As I mentioned above, international cooperation is one of the Norwegian Intelligence Service's primary duties, and such a development could potentially have serious consequences for the service's ability to fulfil its social mission.

Yours sincerely,
Frank Bakke-Jensen



THE ROYAL NORWEGIAN MINISTRY
OF JUSTICE AND PUBLIC SECURITY

Minister of Justice and Immigration

The EOS Committee
P.O. Box 84 Sentrum
NO-0101 OSLO

Your ref.:
2106/68

Our ref.:
19/3357-

Date
21 November 2019

Query about international oversight cooperation

I refer to the EOS Committee's letter of 18 June 2019, in which the Committee requested my views on matters relating to the Committee's wish to share classified information with the oversight bodies for the intelligence and security services of certain other countries. I also refer to the Committee's reply of 3 September 2019 to follow-up questions asked by the Ministry in a letter of 11 July 2019. Statements have been obtained from the National Security Authority (NSM) and the Norwegian Police Security Service (PST) to provide a basis for my response.

The threats that the Norwegian security and intelligence services are charged with counteracting are constantly changing. The methods used by those who represent a threat develop all the time, both in terms of information collection and measures, and the methods are becoming increasingly transboundary in nature in the integrated physical and digital world. In order for our secret services to be able to fulfil their mission, they need to develop their work methods, including their exchange of information, with corresponding services in cooperating countries.

I understand that the EOS Committee has to continuously assess the appropriateness of its oversight as the services develop their cooperation with corresponding services in other countries. It is of course important that the Committee has access to sufficient information to allow it to assess whether the Norwegian services operate within the framework of the law and whether the rights of Norwegian nationals are safeguarded. Based on the above, I take a positive view of the EOS Committee broadening its cooperation with oversight bodies in countries with which Norway cooperates on

Postal address: P.O. Box 8005 Dep., NO-0030 Oslo
Office address: Gullhaug Torg 4A Phone: (+47) 22 24 51 00
Org. no: 972 417 831

security policy-related matters. International dialogue and experience sharing can help to strengthen national oversight of the intelligence, surveillance and security services.

However, based on legal, intelligence-related and security-related considerations, I cannot support the proposal to allow the Committee to share classified information with other countries' oversight bodies.

Processing of intelligence information is a national concern. The EOS Committee's area of responsibility does not extend to overseeing how foreign services process information, even when the information in question originates from Norwegian intelligence activities.

The EOS Committee is charged with overseeing that the Norwegian services comply with the applicable regulatory framework, including that the services carry out due diligence and risk assessments in each case before disclosing information to cooperating foreign services. I see how an 'oversight gap' of the kind that the Committee is concerned about may arise if the foreign service that receives information from Norway uses the information in breach of the conditions under which it was shared, and the oversight body of the receiving country is not authorised to or omits to oversee whether the information disclosed is used in a manner that is in breach of the conditions. It is also important to underline that should it come to a Norwegian service's attention that information has been misused in the receiving country, that would have a bearing on its assessments of future requests for information from that recipient. It will naturally also have consequences for the EOS Committee's oversight of the Norwegian service's disclosure of personal data.

Based on the strict assessments carried out before a Norwegian service discloses information – generally and in each individual case – I consider there to be little risk of an 'oversight gap' arising that may affect Norwegian nationals. I also refer to the fact that the proposed arrangement challenges the established principle that each service should have control over the information it possesses, including what information is disclosed to foreign parties. If the EOS Committee was permitted to share intelligence information with its partners, that could constitute a breach of this arrangement.

Allowing the sharing of information would contribute to spreading information and increasing the risk of classified information falling into the wrong hands. Concern that sensitive classified information could be shared with unauthorised parties could make cooperating services less willing to share information with Norwegian services.

I am therefore of the opinion that the problems that the Committee's proposal would bring far outweigh any benefits. It is also important to remember that the oversight bodies with which the Committee would exchange classified information are those of the countries Norway cooperates most closely with. The EOS Committee's cooperation with the oversight bodies in question also indicates that the Committee

has a good overview of what is covered by each of the relevant bodies' oversight activities within the limits of their remits.

The resources of the Norwegian security and intelligence services are limited. The services therefore depend on access to information from corresponding services in other countries to be able to fulfil their mission. This makes it very important to ensure that cooperating services do not lose confidence in the Norwegian services' ability to ensure that no unauthorised parties gain access to classified information.

Yours sincerely,

Jøran Kallmyr

APPENDIX 7 – Act relating to oversight of intelligence, surveillance and security services⁶³

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.

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 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 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 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 Presidium of the Storting is the security clearance authority for the Committee members. Background checks will be performed by the National Security Authority.

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 investi-

gated 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 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 23 31 09 30

Email: post@eos-utvalget.no

www.eos-utvalget.no