



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



ANNUAL REPORT 2017

DOCUMENT 7:1 (2017-2018)




To the Storting

In accordance with Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act) Section 17 third paragraph, the Committee hereby submits its report about its activities in 2017 to the Storting.

The annual report is unclassified, cf. the Oversight Act Section 17 third paragraph. Pursuant to the Act relating to Protective Security Service (the Security Act), the issuer decides whether or not information is classified. Before the report is submitted to the Storting, the Committee sends the relevant sections of the report text 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 errors or misunderstandings in the factual descriptions.

Oslo, 22 February 2018


Eldbjørg Løwer


Svein Grønner


Theo Koritzinsky


Øyvind Vaksdal


Håkon Haugli


Inger Marie Sunde


Eldfrid Øfsti Øvstedal


Henrik Maghusson



The Norwegian Parliamentary Intelligence Oversight Committee in 2017. Left to right: Theo Koritzinsky, Eldfrid Øfsti Øvstedal, Svein Grønner (deputy chair), Eldbjørg Løwer (chair), Øyvind Vaksdal, Inger Marie Sunde and Håkon Haugli.

Contents

1.	The EOS Committee's mandate and composition	6
2.	Overview of the Committee's activities in 2017	8
2.1	Summary – main issues in the oversight of the services	9
2.2	Oversight activities carried out	9
2.3	Amendments to the Oversight Act	10
3.	Trends and challenges	11
4.	Consultation concerning processing of surplus information from monitoring of communications etc.	14
5.	The Norwegian Police Security Service (PST)	16
5.1	General information about the oversight	17
5.2	Non-conformity reports – PST's use of coercive measures	17
5.3	Oversight of PST's source handling	17
5.4	Requirements regarding the quality of information – the necessity requirement for PST	18
5.5	PST's deletion challenges	19
5.6	Processing of information about persons who are targeted by foreign intelligence activities	20
5.7	Follow-up of investigation cases and prevention cases in PST	21
5.7.1	Introduction	21
5.7.2	Cooperation between PST and the ordinary police	21
5.7.3	Discontinuation of monitoring of communications	21
5.7.4	Question about the legal basis for storing surplus information obtained from tapped calls between closely related persons in prevention cases	21
5.8	PST's storage of context information from open sources	24
5.9	PST's notification to Nkom when mobile-restricted zones are established and facilitation of the Committee's oversight of notifications	25
5.10	Challenges in cooperation project with other oversight bodies caused by changes in PST's transparency	25
5.11	Follow-up of findings in file areas in PST's network	26
5.12	PST's processing of information about deceased persons	26
5.13	Norwegian persons registered in the FBI Terrorist Screening Center's (TSC) database	26
5.14	Complaint cases considered by the Committee	26
6.	The National Security Authority (NSM)	28
6.1	General information about the oversight	29
6.2	Case processing procedures in security clearance cases	29
6.3	Case processing times in security clearance cases	29
6.4	Revocation of security clearance – the line between disciplinary matters and security clearance cases	30
6.5	Downloading and storage of sensitive personal data by NSM NorCERT	31
6.6	Statement on processing of personal data for the purpose of investigating incidents that pose a threat to security	32

6.7	NSM's use of mobile-restricted zones	33
6.8	Complaint cases considered by the Committee	34
6.8.1	Introduction	34
6.8.2	Complaint case 1 – No need for security clearance – criticism of the security clearance authority and NSM	34
6.8.3	Complaint case 2 – Long case processing time in an access to information case	35
6.8.4	Complaint case 3 – Failure to facilitate a complainant's access to information	35
6.8.5	Complaint case 4 – Long case processing time and recording of a complainant and a lawyer during a break in a security interview	35
7.	The Norwegian Defence Security Department (FSA)	36
7.1	General information about the oversight	37
7.2	FSA's photography and filming of persons in non-military areas during an exercise	37
7.3	Processing of personal data in FSA's computer network	38
8.	The Norwegian Intelligence Service (NIS)	40
8.1	General information about the oversight	41
8.2	Norwegian citizenship and connection to Norway	41
8.3	Non-conformities in NIS's technical information collection	43
8.4	Processing of information about Norwegian persons in Norway	44
8.5	Complaint cases considered by the Committee	44
9.	Oversight of other EOS services	45
9.1	General information about the oversight	46
9.2	The Army intelligence battalion	47
9.3	The Norwegian Special Operation Forces	47
9.4	The personnel security service of the Office of the Auditor General	47
9.5	Inspection of the personnel security service at the Office of the Prime Minister (OPM)	47
9.6	Follow-up of the inspection of Haakonsværn in 2016	48
10.	External relations and administrative matters	49
10.1	The Committee's external relations	50
10.2	The EOS Committee in the media	50
10.3	Administrative matters	51
11.	Appendices	52
	Appendix 1 – Definitions	53
	Appendix 2 – Meetings, visits and participation in conferences etc.	55
	Appendix 3 – Act relating to oversight of intelligence, surveillance and security services	56
	Appendix 4 – Consultation statement – processing of surplus information from monitoring of communications etc.	61

A satellite-style map of the Earth, showing continents and oceans, overlaid with a semi-transparent blue filter. The map is centered on the Atlantic Ocean, with North and South America visible on the left and Europe and Africa on the right. The blue overlay is darker in some areas, creating a gradient effect.

1.

The EOS Committee's mandate and composition

The EOS Committee is a permanent, Storting-appointed oversight body. The EOS Committee's task is to oversee all Norwegian entities that engage in intelligence, surveillance and security activities (EOS service). The Committee's mandate follows from the Oversight Act.¹ Only EOS service carried out by, under the control of or on the authority of the public administration are subject to oversight by the EOS Committee.²

Pursuant to the Oversight Act 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 show consideration for national security and relations with foreign powers in its oversight activities.³ The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes, and shall insofar as possible show consideration for the protection of sources and safeguarding of information received from abroad.⁴ Subsequent oversight is practised in relation to individual cases and operations, but the Committee is 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. The Committee's oversight shall cause as little inconvenience as possible to the services' day-to-day operational activities.⁵

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.⁶ No deputy members are appointed. Following a statutory amendment in 2017, the members may be re-appointed once and hold office for ten years.

The Committee is independent of both the Storting and the Government. This means that the Government cannot issue instructions to the Committee, and members of the Storting cannot be members of the Committee. The Committee has a broad composition so that both different political backgrounds and experience from other areas of society are represented. The committee members and secretariat employees must have top-level security clearance and authorisation, both nationally and pursuant to treaties to which Norway is a signatory.⁷ This means security clearance and authorisation for TOP SECRET and COSMIC TOP SECRET, respectively. Below is a list of the committee members and their respective terms of office:

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 2021

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

Of the seven committee members, five have political backgrounds from different parties. The other two have professional backgrounds from the fields of law and technology. The broad composition helps to strengthen the Committee's expertise and legitimacy.

The Committee is supported by a secretariat. At yearend 2017, the Committee Secretariat consisted of eleven employees – the head of the secretariat, who has a law degree, six legal advisers, one communications adviser, one technological adviser and two administrative advisers.

1 Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act). The Act was most recently amended in June 2017.

2 References to the Oversight Act are found in Act No 10 of 20 March 1998 relating to Protective Security Service (the Security Act) Section 30, Act No 11 of 20 March 1998 relating to the Norwegian Intelligence Service (the Intelligence Service Act) Section 6, Instructions No 695 of 29 April 2010 for Defence Security Department Section 14, and Act No 16 of 28 May 2010 regarding Processing of Information by the Police and Prosecuting Authority (the Police Register Act) Section 68.

3 Cf. the Oversight Act Section 2 second paragraph.

4 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 for disputes about access to National Intelligence Service documents.

5 Cf. the Oversight Act Section 2.

6 Cf. the Oversight Act Section 3.

7 Cf. the Oversight Act Section 11 second paragraph.



2.

Overview of the Committee's activities in 2017

2.1 Summary – main issues in the oversight of the services

The EOS Committee's most important task is 'to ascertain whether the rights of any person are violated and to prevent such violations'. The Committee performs this task by checking whether The Police Security Service's registration of persons is in accordance with the law, ensuring that the Intelligence Service does not violate the prohibition against monitoring Norwegians in Norway, and checking whether security clearance cases have been processed properly, among other things.

The Norwegian Police Security Service (PST):

- PST informed the Committee about one non-conformity where covert video surveillance had continued for almost a month longer than approved by the court.
- PST is experiencing challenges when it comes to deleting personal data from some parts of its computer system.
- The Committee has investigated PST's registration of persons who are targeted by foreign intelligence activities.
- In one case, PST discontinued monitoring of communications two days after the person whose phone was tapped had been prevented from using the phone. Twelve phone calls were tapped after this time without a justifiable reason.
- Despite the fact that the Committee has been sending letters for several years, the Ministry of Justice has not yet answered questions about what the Ministry does to follow up the matter of quite a large number of Norwegians being registered in a database belonging to the FBI's Terrorist Screening Center.

The National Security Authority (NSM):

- In one of the complaint cases, the Committee concluded that the security clearance authority and NSM had 'clearly violated the complainant's rights in a manner that warrants strong criticism'. The Committee's investigation showed that there was no legal basis for requesting a security clearance for the complainant. The unlawful security clearance progress and the subsequent clearing denial led to considerable consequences for the complainant.
- The Committee is of the opinion that case processing time in the complaint cases concerning security clearance still is too long. NSM's case processing time for requests for access to information should also be reduced.

The Norwegian Defence Security Department (FSA):

- The Committee raised a case concerning photography and filming during an exercise in a public place where civilians were photographed and filmed without their consent.

The National Intelligence Service (NIS):

- NIS has been of the opinion that, in certain cases, persons who are Norwegian citizens can be considered 'non-Norwegian'. In both NIS' and the Committee's opinion, it is necessary to clarify the legal definition of 'Norwegian' in the new Act relating to the Norwegian Intelligence Service.
- Three non-conformities relating to NIS's technical information collection were reported to the Committee. One of these non-conformities concerned the collection of three calls from a person resident in Norway. According to NIS, this was due to a case processing error – the selector from which information was collected did no longer belong to the person it was registered to in the service's systems.

Other intelligence, surveillance or security services

- Following an inspection of the personnel security service at the Office of the Prime Minister (OPM), the Committee criticised the OPM for case processing errors and inadequate written documentation with the processing of a security clearance case.

2.2 Oversight activities carried out

The Committee's oversight activities mostly take the form of inspections of the EOS services.

The Directive relating to Oversight of the Intelligence, Surveillance and Security Service required the Committee to carry out at least 23 inspections per year.⁸ As of 21 June 2017, the Directive relating to Oversight of the Intelligence, Surveillance and Security Service was repealed and integrated into the Act relating to the Oversight of Intelligence, Surveillance and Security Service (the Oversight Act).⁹ After the legislative amendment, the Oversight Act Section 7 second paragraph requires the Committee to carry out at least 13 inspections per year. The reduced number of required inspections allows for greater flexibility in the Committee's oversight activities. The Committee fulfilled the new requirements concerning inspection locations and number of inspections in 2017.

In 2017, the Committee conducted 21 inspections. The Police Security Service (PST) was inspected seven times, the National Intelligence Service (NIS) five times, the National Security Authority (NSM) three times and the Norwegian Defence Security Department (FSA) twice. The personnel security service at the Office of the Prime Minister, the personnel security service at the Office of the Auditor General of Norway, intelligence and security functions at The Army

⁸ Directive No 4295 relating to Oversight of the Intelligence, Surveillance and Security Service Section 11 subsection 2 (repealed).

⁹ Act No 95 of 21 June 2017 amending the Act relating to the Oversight of Intelligence, Surveillance and Security Services.

intelligence battalion and the Norwegian Special Operation Command were also inspected.

In order to ensure that the Committee's oversight is targeted and effective, the Secretariat conducts thorough preparations in the services. The preparations have been continuously strengthened over the past ten years. Inspections are first prepared in meetings between the Committee Secretariat and contact persons in the services, and then confirmed in an inspection letter sent before the inspection takes place. Preparation for inspections is a resource-intensive part of the Secretariat's activities.

The Committee can carry out most of its inspections without assistance *directly in the services' electronic systems*. This means that the inspections contain considerable unannounced elements. Until the Committee asks verbal questions during an inspection or later follows up its findings in writing, the services are not aware which information is being subject to oversight in an inspection. No completely unannounced inspections were carried out in 2017.

The Committee raised 31 cases on its own initiative in 2017, compared with 51 cases in 2016. The cases raised by the Committee on its own initiative are mostly follow-up of findings made during its inspections. The Committee concluded 30 cases raised on its own initiative in 2017, compared with 27 cases in 2016.

The Committee investigates complaints from individuals and organisations. In 2017, the Committee received 26 complaints against the EOS services, compared with 32 complaints in 2016.¹⁰ The Committee prioritises the processing of complaints and spends more resources on this than before. Some complaints were dismissed on formal grounds, among other things because they did not fall within the Committee's area of oversight. Complaints and enquiries that fall within the Committee's area of oversight are investigated in the service or services that the complaint concerns. The Committee has a low threshold for considering complaints.

The committee members meet several days every month, except in July. The workload of the chair of the committee corresponds to approximately 30% of a full-time position, while the office of committee member is equivalent to approximately 20% of a full-time position. In 2017, the

Committee had 16 internal meetings at its office, in addition to internal meetings on site in connection with inspections. At these meetings, the Committee discusses planned and completed inspections. It also considers complaints and cases raised on the Committee's own initiative, reports to the Storting and administrative matters relating to the Committee's activities.

The EOS services have generally demonstrated understanding of the Committee's oversight. However, the Committee sometimes experience too long response time from some of the services in connection with case processing, and some shortcomings in the technical facilitation for the Committee's oversight. Experience shows that the oversight helps to safeguard individuals' due process protection and to create public confidence that the services operate within their statutory framework.

2.3 Amendments to the Oversight Act

As described in the annual report for 2016, the EOS Committee's activities and framework conditions have been evaluated by a committee appointed by the Presidium of the Storting. The Evaluation Committee submitted its report to the Storting on 29 February 2016.¹¹ This formed part of the background to the amendments to the Oversight Act adopted by the Storting on 13 and 16 June 2017. The amendments entered into force on 21 June 2017.

As mentioned in section 2.2 above, the amendment entails a reduction in the number of inspections the Committee is required to carry out each year. The requirements concerning which services and entities must be inspected, which oversight duties must be performed and the Committee's presence during inspections, have also been modified.

The Committee is satisfied that the legislative amendment has given it greater freedom to utilise its oversight resources, and is continuously considering how its work can be carried out in the most targeted and efficient way possible. The Committee is considering an assessment of which oversight duties can be delegated to the Secretariat and how inspections should be organised. This work will continue in 2018.

¹⁰ Some complaints concern more than one of the services.

¹¹ Report to the Storting from the Evaluation Committee for the Norwegian Parliamentary Intelligence Oversight Committee, Document 16 (2015–2016).



3.

Trends and challenges

The EOS Committee's most important control task is to ensure that the EOS services do not interfere with the rights of individuals to a greater extent than the legal rules permit. The Committee is charged with ensuring that the means of intervention employed do not exceed those required and that the activities do not unduly harm the interests of society.¹² The services must balance considerations for individuals' right to privacy against society's and all citizens' need for security. It is demanding for the services to strike this balance, and it represents a challenge from an oversight perspective. It is the Committee's duty to take a critical approach to the services' actions, while the services must be able to utilise the freedom of action that the legal framework provides.

The EOS services are subject to a detailed regulatory framework relating to the protection of privacy, and generally appear to focus on due process protection. Considerations of individuals' due process protection and protection of privacy shall form part of the services' basis for assessment when considering different forms of covert surveillance measures. There are good reasons why one body exercises democratic oversight of all the EOS services. In a time of increasing cooperation between services, particularly between NIS and PST in their counterterrorism efforts, this is crucial to conduct satisfactory oversight. PST's right to disclose information to NIS was extended in 2017.¹³ The Joint Cyber Coordination Centre (FCKS) was established in 2017 to

further develop the cooperation between PST, NSM and NIS, and to strengthen the ability to counteract digital threats.

The EOS services are also increasingly taking part in international cooperation, particularly concerning counterterrorism. In the annual report for 2015, the Committee stated that a fundamental challenge is that services cooperate across borders, while oversight is limited to the national level. The Committee remains interested in transboundary oversight cooperation, and this topic has been discussed in meetings with other countries' oversight authorities, both bilaterally and at several international seminars and conferences. In section 5.10, the Committee comments on an international project it is participating in, the topic being democratic oversight of the services' exchange of information across national borders about foreign terrorist fighters. This discussion shows that it is challenging for the oversight bodies to conduct coordinated investigations that can provide relevant experience of e.g. oversight methodology, without coming into conflict with the services' need to protect information.

The rapid technological development means that both the threat situation and the EOS services' methods are changing. New forms of communication provide new opportunities, both for government organisations and for parties not associated with any state, to carry out intelligence activities, attacks against Norwegian interests and acts of terrorism. The EOS services must counteract the cyber threat and the



President of the Storting, Olemic Thommessen, received the Annual report for 2016 from Eldbjørg Løwer, Chair of the EOS Committee, on the 5th of April 2017. Photo: Stortinget

changes in communication methods by continuously developing new tools and methods. The amounts of data that the services hold and the complexity of their computer systems and surveillance measures are considerable and growing. The Committee has to adapt its oversight activities to this technological development.

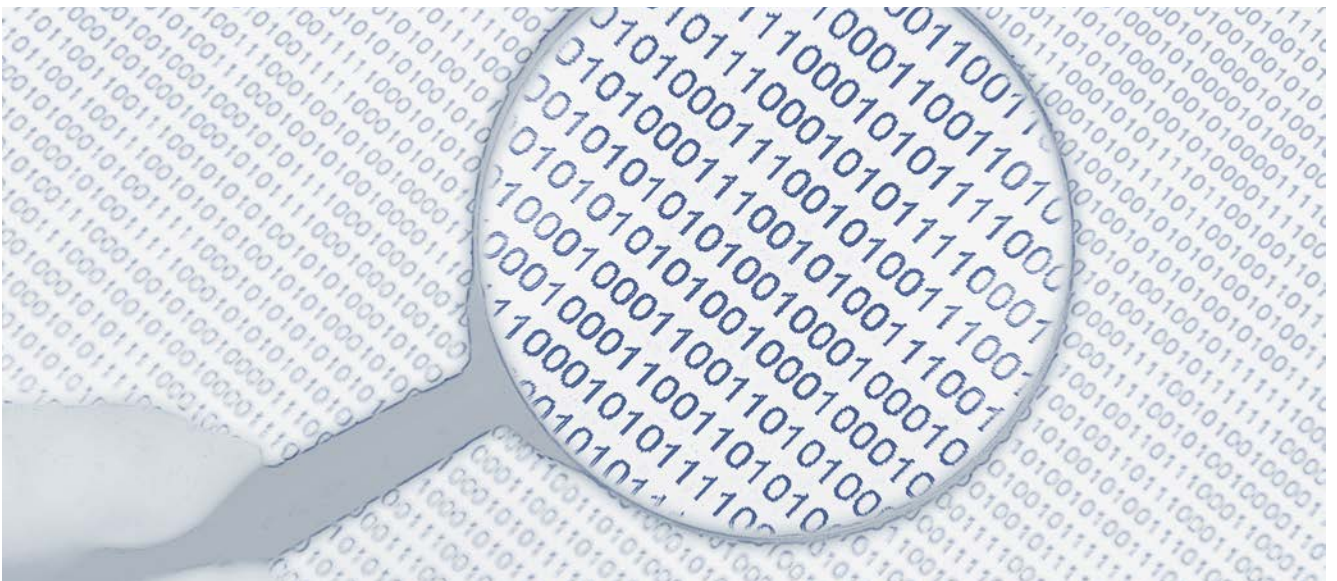
Following the Evaluation Committee's report¹⁴ and the Storting's consideration of the report,¹⁵ the Committee decided in 2017 to establish a technology unit in the Secretariat in order to strengthen the Committee's technological expertise and capacity. The EOS Committee is of the opinion that this unit should consist of at least five employees. The goal is for the unit to give the Committee better insight into the EOS services' systems and contribute further to develop oversight methods, including automated checks of the services' systems and tools. If digital border defence is adopted, this will further increase the need for technical expertise in the Committee and Secretariat, regardless of what role is assigned to the EOS Committee in the oversight.

The Committee has stated in several annual reports that it is challenging that the Committee is legally prevented from providing further information about the basis for criticism in complaint cases. Whether or not the services have information about a person is in itself classified information.

In its recommendation to the Committee's annual report for 2015,¹⁶ the Standing Committee on Scrutiny and Constitutional Affairs of the Storting requested that the Ministry of Justice and Public Security consider the practice of giving complainants grounds for the Committee's criticism of PST. In two complaint cases in 2017, the Ministry decided, at the Committee's request that a more detailed explanation can be given in both cases.¹⁷ The Committee is satisfied that the Ministry seems to have complied with the Storting's request to consider this practice in cases where a complaint has given grounds for criticism.

However, the Committee realises that a more detailed explanation is not always enough to put the complainant's mind at ease. Reference is also made to the fact that the Police Register Act's provisions on access to information in police registers does not apply in relation to PST, so that complainants have no right of access to the information on which the criticism is based. The Committee's possibility to give complainants satisfactory answers has a bearing on public confidence in the services and in the Committee's oversight.

The Committee is continuously looking into how it can, within the framework of the legislation, develop its answers to complainants regarding the results of the Committee's investigations, in order to address the complainants' needs in the best possible way.



12 Cf. the Oversight Act Section 2.

13 *Endringer i straffeprosessloven og politiloven (utlevering av informasjon fra PST til E-tjenesten)* ('Amendment of the Criminal Procedure Act and the Police Act (disclosure of information from PST to the Intelligence Service)' – in Norwegian only) Proposition No 61 to the Storting (Bill) (2016–2017).

14 Document 16 (2015–2016).

15 Recommendation No 146 to the Storting (2016–2017).

16 Proposition No 145 to the Storting (Resolution) (2016–2017), page 31.

17 See section 5.14

4.

Consultation concerning processing of surplus information from monitoring of communications etc.

The EOS Committee received the Ministry of Justice and Public Security's consultation letter on processing of surplus information from monitoring of communications etc. in criminal cases. Among other things, the Ministry proposes amending the Criminal Procedure Act¹⁸ Sections 216g and 216i concerning the deletion and further use of material obtained through monitoring of communications, and transferring provisions for this to the police register legislation.

It has been the EOS Committee's practice to have a high threshold for submitting consultation statements. The Committee nevertheless feels that it is important to submit a statement in cases where such proposals will have direct consequences for the EOS Committee's oversight and/or if there are circumstances that the Committee feels should be known before the Storting considers a bill.

The Committee submitted its consultation statement on 18 December 2017. The background to this statement was that the processing of surplus information from coercive measures *for preventive purposes* was not mentioned in the Ministry's proposal to transfer parts of Section 216g to the police register legislation. The Committee's consultation statement was submitted before the Committee received the Ministry of Justice and Public Security's reply regarding the Ministry's assessment of the application of the Criminal Procedure Act Section 216g in PST's prevention cases see section 5.7.4.

In its consultation statement, the Committee remarked that the conditions for PST's use of coercive measures *for preventive purposes* have their legal basis in the Police Act¹⁹ Section 17d. The Committee pointed out that, regardless of whether coercive measures are used in preventive activities

or as part of an investigation, the nature of the information and of the coercive measures remains the same and that the methods used entail a corresponding infringement on the right to privacy of the individuals directly or indirectly affected. Therefore, the Committee expressed the view that the rules on the processing of surplus information from coercive measures used for preventive purposes should be clarified in connection with the Ministry's work to transfer the provisions on such processing of information from the Criminal Procedure Act to the police register legislation.

Regarding future consideration of limitations on the use of *surplus information from equipment interference* in criminal cases, the Committee remarked that such limitations should also be considered for the use of surplus information from equipment interference *for preventive purposes*, cf. the Police Act Section 17d and the Criminal Procedure Act Section 216o.

Regarding *restriction of access to information*, the EOS Committee referred to the fact that it has remarked on several occasions that no satisfactory solution has been established for restricting access to information that shall no longer be available for intelligence purposes or operational activities in PST, most recently in section 4.5 of the Committee's annual report for 2015. In January 2018, PST informed the Committee that the service has a project under way to solve the problem, but that it does not yet have a technical regime that ensures 'compliance with both the Police Register Act and the Archives Act' as regards deletion and restriction of access.

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

18 Act No 25 of 22 May 1981 relating to Legal Procedure in Criminal Cases (the Criminal Procedure Act).

19 Act No 53 of 4 August 1995 relating to the Police (the Police Act).

5.

The Norwegian Police Security Service (PST)



5.1 General information about the oversight

In 2017, the Committee conducted five inspections of the PST Headquarters (DSE). The Committee also inspected the PST entities in East and Finnmark police districts.

The number of inspections decreased in 2017 as a result of amendments to the Oversight Act adopted by the Storting in June 2017, see section 2.3 for more information.

In its inspections of the service, the Committee focuses on the following:

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

The Committee's inspections consist of an orientation part and an inspection part. The service's orientations are useful in giving the Committee insight into the service's view on its responsibilities, assessments and challenges. Broad insight into the service's activities enables the Committee to conduct more targeted inspections. The Committee shall adhere to the principle of subsequent oversight, but may nevertheless demand access to and make statements about ongoing cases.²⁰ During the inspections, the Committee is briefed about PST's ongoing activities, the service's national and international cooperation and cases that have triggered public debate, among other things. The Committee asks questions to the service's orientations.

During the inspection part, the Committee conducts searches directly in the service's electronic systems. PST is not informed about what the Committee searches for. This means that the inspections contain considerable unannounced elements. The Committee's inspections are prepared by the Secretariat. These preparations enable the Committee to conduct more targeted inspections.

5.2 Non-conformity reports – PST's use of coercive measures²¹

In 2017, on its own initiative, PST informed the Committee of a non-conformity relating to the service's use of covert video surveillance. The error resulted in the video surveillance continuing for almost a month longer than approved by the court. PST has informed the Committee that it will review its internal procedures. The Committee will keep informed about the measures that PST implements to prevent such non-conformities from occurring in the future. The Committee will intensify its oversight of PST's technical information collection in 2018 as a consequence of the establishment of the Secretariat's technology unit, see section 3.

The Committee takes a positive view of the fact that the service itself detects non-conformities and reports them to the Committee during inspections of the service. The Committee expects the service to take such errors and non-conformities seriously and to focus on quality-assurance and procedures to minimise the possibility of such errors occurring again. The error must be deemed serious, and the Committee will keep informed of PST's follow-up of the non-conformity.

5.3 Oversight of PST's source handling

In the annual report for 2016, the Committee gave an account of its work to establish oversight of PST's source handling. With reference to the disagreement between the Committee and PST regarding the scope of the Committee's right to demand access to the source material, the Committee was of the opinion that this was 'a matter which should be put before the Storting'.²² The Committee's right to demand access to PST's source material was also considered during the Storting's consideration of the private member's bill²³ for amendment of the Oversight Act.

The following is quoted from the Standing Committee on Scrutiny and Constitutional Affairs' comments²⁴ of 6 June 2017 to amendments to the Oversight Act:

'The Committee refers to the fact that it is the ministers' responsibility to enable the services to carry out their duties in a way that makes them available for oversight, and at the same time observe the concern for protection of sources. The Committee therefore requests that this work be given priority and that PST's register be

20 Cf. the Oversight Act Section 2 third paragraph.

21 See also section 8.3 on non-conformity reports from NIS.

22 Cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Services in force at the time, Section 13(3) letter g).

23 Private Member's Bill 63 (2016–2017).

24 Recommendation No 431 to the Storting (Bill) (2016–2017).

organised in such a way that oversight of methods is possible without disclosing identities.’

The following is quoted from the Standing Committee on Scrutiny and Constitutional Affairs’ comments²⁵ of 6 June 2017 to the Committee’s annual report for 2016:

‘It is the Committee’s opinion that, in order to fulfil the purpose and intention of the Oversight Act, it must be possible for the EOS Committee to search in the systems where PST processes its source material without the name or personal identity number of sources being exposed.’

On 21 June 2017, the Storting decided to keep the wording in the Act that entitles the Committee to demand access to PST’s ‘archives and registers, premises, installations and facilities of all kinds’.²⁶ The Committee’s decisions concerning access are binding on PST, but PST is entitled to have any objections against such decisions included in the Committee’s annual report and thereby made known to the Storting.

With reference to the Storting’s consideration, the Committee sent requests for partial access to PST’s source material on 21 June 2017. The Committee presumed that only the names and national identity numbers of the sources would be exempt from oversight. In a letter to the Committee dated 14 September 2017, PST refused to facilitate oversight as requested. After the Committee had pointed out its right to inspect again on 21 December 2017, PST stated in a letter dated 4 January 2018 that the service acknowledges the Committee’s full right of inspection and will facilitate the Committee’s access to the source material as requested.

The right to demand access is the EOS Committee’s most important means of fulfilling its statutory function. This matter has therefore been very important to the Committee. It has been the Committee’s clear view that the Oversight Act cannot be understood to mean that it is up to the body subject to oversight to decide how far the oversight authority’s right of access extends. The importance of the right of access is twofold: Firstly, it probably has a strong disciplinary and thus preventive effect. The services know that the Committee can check every drawer, and every register. Secondly, the right of access allows the Committee to familiarise itself with and assess all aspects of a case, thereby enabling it to report to the Storting without reservations. The Committee’s oversight also strengthens the service’s legitimacy.

While the Committee has been given the right of access, the Storting has also imposed some precautions on the EOS Committee. The EOS Committee emphasises that the Storting’s instructions to exercise caution as regards sources will be taken into consideration during its oversight work. PST’s facilitation means that the names and national

identity numbers of the sources will not be exposed in the course of the oversight activities.

The Committee conducted its first inspection of the source material in February 2018, and was granted access in accordance with the intentions of the law and the Storting. The EOS Committee is satisfied with PST’s facilitation of the Committee’s oversight.

5.4 Requirements regarding the quality of information – the necessity requirement for PST

Information processed by the police and PST shall not be stored for longer than ‘necessary for the purpose of the processing’.²⁷ In 2017, the Committee has concluded several cases where, on this basis, it has questioned the necessity of continuing to process information about persons in the intelligence register Smart.

PST’s clarification of the basis for continued registration

In 2017, the Committee has followed up individual registrations in the intelligence register where the Committee has previously assumed that the service is making active efforts to clarify whether there is a basis for continuing to process information. As part of the follow-up of a case from 2015, the Committee noted that PST has now deleted or will delete information about several persons in cases where the information is no longer necessary for the processing. The Committee took note of the fact that PST deemed it necessary to uphold registrations for some persons.

In the case mentioned in section 5.7.2 below, PST was asked to explain whether the service has any concerns relating to the person in question at present. The background to this question was that the offence in the investigation case was time-barred. The service replied that it had no concerns relating to the person in question at present, and that the case had therefore been concluded. In response to questions from the Committee about the basis for processing new information about the person in question, PST informed the Committee that the service is still concerned that the person is ‘trying to improve his/her financial capacity in order to provide support to a terrorist organisation, cf. the Police Act Section 17b(1)’, and that the new information is therefore necessary for purposes of prevention.

The Committee did not find it to be evident that the new information formed a basis for a current concern that the person can be linked to financing terrorism. Seen in light of the relatively wide margin of discretion that PST is allowed in the assessment of whether a matter is considered ‘necessary for police purposes’ pursuant to the Police Register Act Section 64 first paragraph, cf. third paragraph (1) letter b, the Committee nevertheless decided, after receiving PST’s explanation, not to pursue the matter further.

Time of assessment of necessity versus the five-year rule

The service has in several cases, with reference to the five-year rule stipulated in the Police Register Regulations Section 22-3 third paragraph, argued on a general basis that information registered in the intelligence register can be processed for a period of five years before PST has to conduct an assessment of whether the intelligence registrations are still relevant and necessary to the service. At the same time, the service has pointed out that the necessity and relevance of an intelligence registration is to be reassessed when new information about a registered person is entered in Smart.

As an argument in support of the possibility of processing information in the intelligence register for five years before PST has to conduct an assessment of whether the intelligence registrations are still relevant and necessary to the service, PST referred to the Ministry's statement in the preparatory works. There it is stated that the necessity criterion 'is a principle that cannot be fully adhered to, and that practicable rules must be put in place, for example by setting time-limited deadlines for deletion or instructions to subject information to assessments of necessity at specified time intervals'.²⁸

The Committee was of the opinion that the Ministry's statement is a qualified expression that the necessity criterion is to be complied with in practice *insofar as it is possible*. The Committee also commented that the necessity criterion is a key principle of protection of privacy, which applies to all pro-

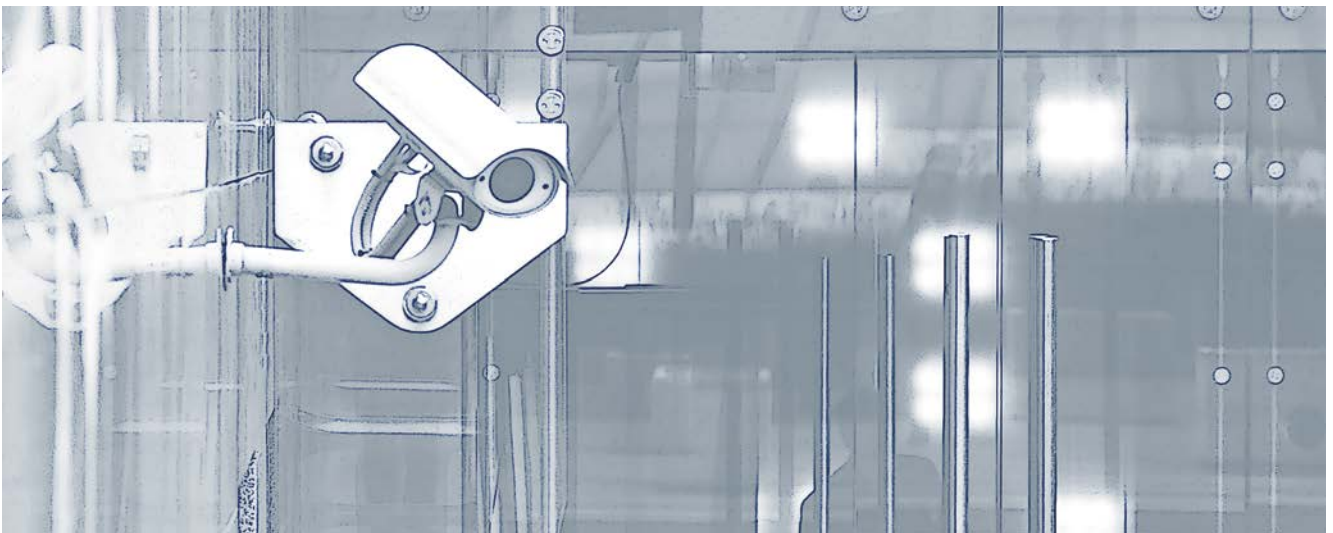
cessing of personal data. Necessity as a criterion represents a limitation on processing, in that information can only be processed when necessary for the purpose.²⁹ This criterion is a legal standard that will vary depending on time and situation. How long it will be 'necessary' to store a specific intelligence registration must be determined after a specific assessment in each individual case. The purpose of processing the information, the nature of the interference and the scope of processing will be important elements in this assessment.

In the Committee's opinion, intelligence registrations should be reviewed periodically by the person or persons responsible for registering the information in order to ensure that the intelligence register contains up-to-date, correct, necessary and relevant information.

Since the Committee made its concluding statement to PST, the service has expressed disagreement with the Committee's opinion that intelligence registrations should be reviewed more often than every five years. On this basis, the Committee has raised the issue with the Ministry of Justice and Public Security.

5.5 PST's deletion challenges

According to the Police Register Act Section 50, personal data that are no longer to be stored should be deleted or access to it restricted.³⁰



25 Recommendation No 418 to the Storting (2016–2017).

26 Cf. the Oversight Act Section 8.

27 Cf. Regulations No 1097 of 20 September 2013 regarding Processing of Information by the Police and Prosecuting Authority (the Police Register Regulations) Section 22-3 first paragraph first sentence; cf. the Police Register Act Section 6 first paragraph (3).

28 Proposition No 108 to the Odelsting (2008–2009), section 14.5.2, page 225.

29 Proposition No 108 to the Odelsting (2008–2009), section 9.3.1, page 77.

30 Restriction of access to information means to restrict access to process the information in future, cf. the Police Register Act Section 2(10).

In 2017, the Committee has noted that PST is experiencing challenges when it comes to meeting the statutory requirements, and that PST is working to resolve this situation.

The Committee has asked PST to keep it informed about the service's work to resolve the challenges relating to deletion, and has expressed its expectation for the service to shortly find a solution to prevent the processing of information when the basis for processing it has ceased to exist. The Committee will follow up the PST's deletion-related challenges in 2018.

5.6 Processing of information about persons who are targeted by foreign intelligence activities

In 2017, the Committee concluded two cases concerning PST's processing of information about persons who are or may be 'targeted by foreign intelligence activities'.³¹ The Committee has made the following general statement:

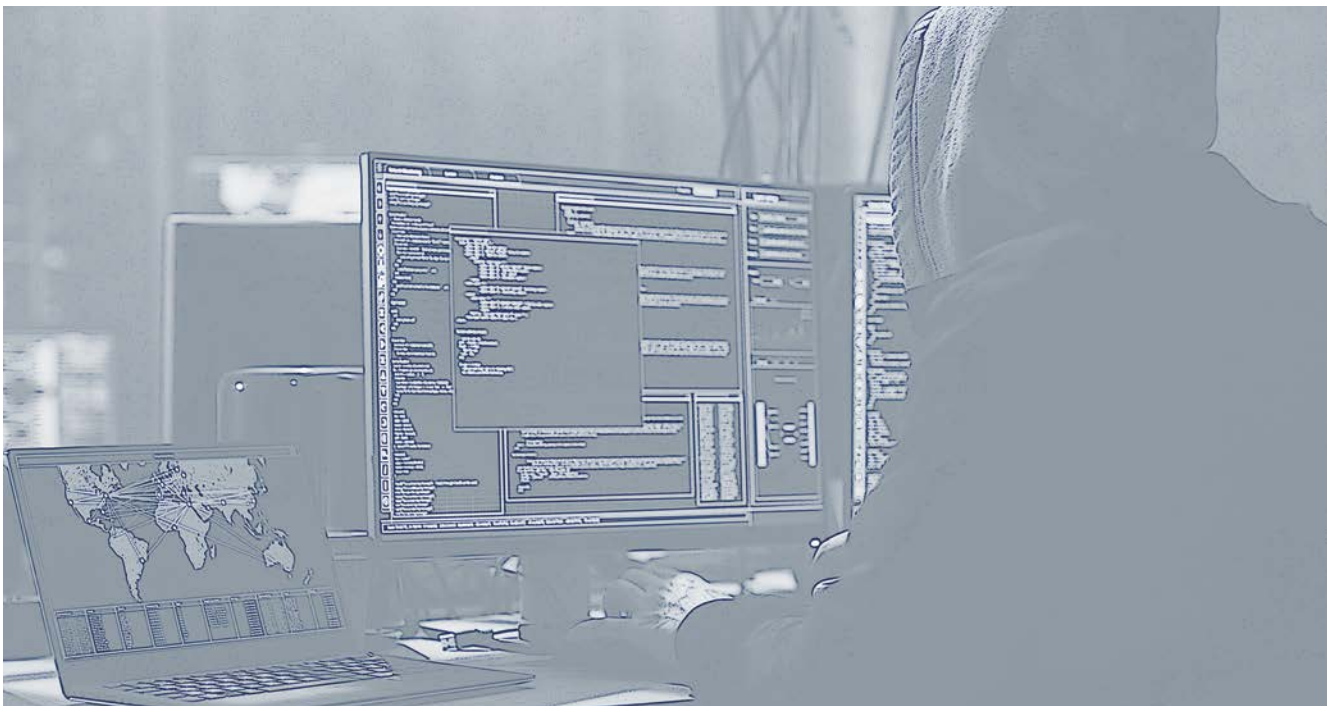
'Whether the conditions for processing information about [such] persons are met must, in the Committee's opinion, be determined on the basis of a concrete assessment of whether the person can be deemed to be 'targeted by' foreign intelligence activities. In the Committee's view, such an assessment must take into consideration e.g. the nature of the contact relationship with [foreign intelligence] (how qualified the contact is considering the circumstances and scope of contact etc.), what potential

assets the person manages/has access to that could be of importance to the security of individuals, Norway or other countries, and whether it is probable that the contact relationship could manifest itself in concrete criminal offences if the person can be exploited by a foreign state.'

The Committee has noted that PST is of the opinion that the foreign state's activities must constitute a criminal offence in Norway in order to be defined as 'unlawful intelligence activities'.

One of the cases concerned the registration of persons in professional groups that could be at particular risk of being targeted by unlawful foreign intelligence activities and where there is a considerable potential to cause harm if foreign intelligence activities are successful. PST gave an account of its views on when attempts by foreign intelligence services to influence the professional groups in question will be considered as unlawful intelligence activities. Among other things, the Committee investigated whether it was strictly necessary to register information about the political convictions of individuals, cf. the Police Register Act Section 7. The case was concluded without criticism of PST.

In the other case, the Committee commented that it understands PST's concern that foreign intelligence services are approaching Norwegian citizens. However, the Committee remarked that the grounds for PST's concern could have been made clearer, in light of the service's duty to prevent *unlawful intelligence activities*.



If it remains unclear whether the contact can be related to concerns regarding unlawful intelligence activities in Norway, it is the Committee's opinion that PST should consider whether a basis for processing information still exists.

The Committee also commented that, out of consideration for persons targeted by foreign intelligence activities, the registrations should show that nothing negative is registered about the persons themselves.

PST has informed the Committee that the service has taken note of the Committee's concluding remarks. The Committee assumed that this is now reflected in the registrations of the persons in question.

The EOS Committee takes a positive view of the service updating its registration practice to ensure that its processing of information complies with the requirements set out in the police register legislation.

5.7 Follow-up of investigation cases and prevention cases in PST

5.7.1 Introduction

The Committee regularly reviews new and concluded prevention cases and investigation cases during its inspections of PST. The Committee also keeps informed about and oversees ongoing cases in the service, including the service's use of statutory covert coercive measures and non-statutory methods, as well as cooperation and exchange of information with domestic and foreign collaborative partners. In 2017, the Committee has concluded several cases in which topics including cooperation, exchange of information and use of methods were raised with the service.

5.7.2 Cooperation between PST and the ordinary police

In 2017, the Committee made critical remarks concerning a local PST unit's wish to 'use a potential opportunity that might present itself in an ordinary criminal case to take part in a search of the object's home' in an investigation case where the offence was time-barred pursuant to Norwegian law. The Committee asked PST to give an account of whether PST took part in such a search of the person's home under the auspices of the ordinary police, the contact with the ordinary police, and whether the service is of the view that such contact can create an unfortunate situation in relation to the ordinary police as regards the possibility

of provoking a search that might not otherwise have been carried out.³²

PST replied that no search had been conducted with PST present, nor has the service received any surplus information from a search. The Committee commented that PST's exchange of information with and requests to the ordinary police should be better documented than they were in the case in question.

5.7.3 Discontinuation of monitoring of communications

As part of monitoring of communications in a prevention case, PST asked the telecommunications providers to disconnect the monitoring two days after it had been determined that the person in question was prevented from using the means of communication. The Committee's investigation showed that twelve calls between other persons had been tapped during this period.

In response to a question from the Committee about the legal basis for continuing monitoring of communications, PST stated that the disconnection of the monitoring had been delayed in this case, and that the monitoring should have been disconnected at the time when it could be determined with certainty that the person in question could no longer use the means of communication in question.

The Committee remarked that it was unfortunate that the monitoring of communications was not disconnected immediately. The Committee assumed that PST will delete the material for the period after the monitoring should have been discontinued, and noted that 'PST will delete the event in question [from Smart] because there is no longer any basis for processing the information'.

5.7.4 Question about the legal basis for storing surplus information obtained from tapped calls between closely related persons in prevention cases

The Committee asked PST to give an account of the legal basis for recording the content of conversations between closely related persons to an individual subject to monitoring of communications.

In criminal cases, the person charged's closely related persons are exempted from the duty to testify.³³ Recordings or notes made during monitoring of communications shall as soon as possible be destroyed if they relate to statements, intercepted through monitoring of communications,

31 PST may process information about 'persons who are targeted by, or who there is reason to believe will be targeted by, foreign intelligence activities' if necessary for the purpose of the processing and indicated by a concrete assessment, cf. the Police Register Regulations Section 21-2 second paragraph (4).

32 In its annual report for 2015, section 4.3, the Committee made critical remarks concerning the link between the ordinary police's use of methods in the investigation case, PST's presence during the ordinary police's search of the home of a person involved in a PST prevention case, and the subsequent transfer of information about seizures in the case from the police to PST. The Committee criticised the lack of documentation of the requests from the ordinary police to PST for assistance in the search or the transfer of material seized to PST, among other things.

33 Cf. the Criminal Procedure Act Section 122, cf. Section 216g first paragraph letter b).

which the court may not require witnesses to testify.³⁴ The Committee has previously raised the matter of the application of the provisions of the Criminal Procedure Act Section 216g concerning the processing of surplus information in PST's preventive activities. PST has previously informed the Committee of the following:

'The Criminal Procedure Act Section 216g has not via the Police Act been made applicable to PST's prevention cases. **PST nonetheless finds grounds, also in prevention cases, for complying with the principles set out in the provision and the important considerations it safeguards.**' (Committee's boldface)

In the case in question, however, the service replied that '[c]onsiderations underlying the Criminal Procedure Act Section 119 [concerning professional secrecy] indicate that the principles of the provision should apply directly in PST's preventive activities', but not as regards the rules concerning the exemption of closely related persons from the duty to testify pursuant to the Criminal Procedure Act Section 122:

'The considerations underlying this provision are not relevant for PST's preventive activities, as the provision is intended to protect the next of kin of persons charged from having to choose between lying in court or contributing to the conviction of the person charged in a criminal case.'

In its concluding letter to PST, the Committee questioned if the decisive factor must be whether the considerations underlying the provisions on protection of confidential communication and of closely related persons' right not to incriminate the other person (protection of the witness) pursuant to Section 122 are also relevant to monitoring of communications in prevention cases, rather than whether the considerations underlying Section 216g are relevant to PST's preventive activities.

The Committee asked the Ministry of Justice and Public Security to clarify the legal understanding of the application of the Criminal Procedure Act Section 216g in PST's prevention cases.

Among other things, the Committee referred to the Police Methods Commission's³⁵ comments that a right for PST to use coercive measures for preventive purposes, would require the simultaneous adoption of case processing rules that address fundamental due process protection requirements. And that case processing rules for the use of coercive measures in investigations shall apply correspondingly when coercive measures are used for preventive purposes.³⁶ The Committee also referred to the Ministry's own statements, including that considerations of due process protection and protection of privacy becomes applicable to an even greater extent with the use of coercive measures in

prevention cases, than when coercive measures are used in the investigation of a criminal act, 'where circumstances that give grounds to investigate whether a criminal act has been committed must be identified'.³⁷

The Committee asked whether the considerations underlying the protection under the witness exemption provisions indicate that other rules should apply to PST's use of corresponding information from cases for preventive purposes. The Committee also asked which considerations indicate that considerations for due process protection and protection of privacy should be less important in connection with PST's monitoring of communications in prevention cases than in investigation cases, and whether this was intended.

In its response of December 2017, the Ministry expressed its understanding of the Committee's points of view, but argued that Section 216g does not apply to PST's preventive use of coercive measures.

In a concluding letter to the Ministry, the Committee commented that it has understood the preparatory works to mean that the regulation of the use of information obtained through the use of coercive measures for preventive purposes pursuant to the Police Act Section IIIa was intended to be stricter than the regulation of the use of coercive measures in investigation cases pursuant to the Criminal Procedure Act. The Committee concluded that the Ministry's reply must be understood to mean that the opposite is in fact the case, which the Committee found difficult to comprehend.

For criminal cases, the provisions in Section 216g will limit the processing of surplus information from monitoring of communications, with specific rules on the deletion of information that is not to be stored. The Committee's view was that, if these case processing rules are not applied correspondingly when coercive measures are used for preventive purposes, the regulatory framework will provide a weaker protection of privacy for people indirectly affected by monitoring of communications for preventive purposes. The Committee found this to give cause for concern.

The Committee pointed out that it should not be left up to PST's discretionary judgement to decide whether surplus information from monitoring of communications for preventive purposes meets the necessity criterion in prevention cases³⁸ in the sense of whether or not the material should be stored. In the Committee's opinion, this should also be specifically regulated in law in a corresponding manner as for criminal cases.

The Committee commented that the implication of the Ministry's conclusion will be that in preventive cases, PST can process surplus information from monitoring of communications that it would have had to destroy as soon as possible

in criminal cases, cf. Section 216g.³⁹ This would be the case even though one is further removed from the criminal offence in that there is no requirement for suspicion that a criminal act has been committed or is being planned.

The Ministry wrote that a corresponding application of Section 216g in prevention cases ‘could have very unfortunate consequences’ and stated, among other things, that ‘if the person subject to control were to express in a telephone conversation with a closely related person or with his doctor that he is planning a terrorist attack, PST must be allowed to make use of this information to avert the attack’. The Committee commented that confidential communication between doctors and patients enjoys special protection under Norwegian procedural rules, in the same way as conversations between lawyers and clients.⁴⁰ Confidential conversations between the subject of monitoring of communications and persons subject to a professional duty of secrecy

are covered by the prohibition on submission in evidence set out in the Criminal Procedure Act Section 119. Nor can such communication be listened through as part of a criminal case if it is clear in advance that it is confidential and protected communication. This type of surplus information must be destroyed as soon as possible. In the Committee’s opinion, the same must apply in prevention cases, a view that PST itself has also expressed on several occasions.

The Committee remarked that the Ministry seems to assume that PST can listen through confidential doctor-patient communication that enjoys particular protection in connection with monitoring of communications for preventive purposes. This understanding does not agree with the special protection of information subject to professional secrecy. This would mean that PST will not be prevented from engaging in surveillance of doctor-patient communication in preventive cases, while PST will be prevented from



34 The Criminal Procedure Act Section 216g letter b) reads as follows: ‘The prosecuting authority shall ensure that recordings or notes made during communication control shall as soon as possible be destroyed in so far as they (...) relate to statements concerning which the court may not pursuant to the provisions of sections 117 to 120 and 122 require the person concerned to testify, unless the said person is suspected of a criminal act that might have provided independent grounds for control.’

35 Official Norwegian Report NOU 2004:6 *Mellom effektivitet og personvern* (‘Between efficiency and protection of privacy’ – in Norwegian only). See also Proposition No 60 to the Odelsting (2004–2005), *om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)* (On the Act amending the Criminal Procedure Act and the Police Act (covert audio surveillance and use of coercive measures to prevent serious crime) – in Norwegian only).

36 Chapter 9.4.3.1 page 132.

37 Chapter 9.4.2.1 page 128 and 9.4.3.2 on page 133.

38 Cf. the Police Register Act Section 64 and Chapters 20 and 21 of the Police Register Regulations.

39 Or deleted, cf. the Ministry’s proposal for a new Section 25-4 third paragraph in the Ministry’s consultation letter concerning the processing of surplus information from monitoring of communications etc.

40 As regards lawyer-client communication, it is clear from the European Court of Human Rights (ECtHR) case law that correspondence between lawyer and client enjoys particular protection under the European Convention on Human Rights Article 8, see, *inter alia*, ECtHR’s judgment in the case *Michaud versus France* of 6 December 2012 (ECHR-2011-12323). This special protection is also expressed in the case law of the Norwegian Supreme Court, see for example the Norwegian Supreme Court Reports Rt. 2015 page 81.

listening through such material from monitoring of communications in a terrorism investigation case or averting terrorism investigation case – where there is suspicion that the principal object is planning to carry out an act of terrorism.

The Committee finds it difficult to see that the right to process surplus information from monitoring of communications obtained through the same type of invasive coercive measures should differ depending on whether the coercive measures are used as part of an investigation or for preventive purposes.⁴¹

The Committee considers that it is up to the Storting to determine which rules should apply to the processing of surplus information from monitoring of communications in prevention cases.

5.8 PST's storage of context information from open sources

The Committee has noted that PST sometimes store newspaper articles as attachments to intelligence information in Smart. These articles may contain information about other people in addition to persons whom PST finds it necessary to process information about. The Committee raised with the service the question of whether information about other persons in articles linked to intelligence information is deemed to be 'processed' in the sense of the Police Register Act,⁴²

and whether a requirement that the information must be necessary and relevant to the service's performance of its duties applies. The Committee also asked whether the service redacts personal data from attached articles when the information is not considered necessary and relevant to PST's performance of its duties.

PST replied that, in theory, newspaper articles in Smart are covered by the law's concept of processing, but argued that it was unnecessary to redact any personal data from the articles even though they did not meet the requirements for processing under the Police Register Act. Reference was made to the fact that the articles are publicly available and were stored to ensure documentation of the intelligence information. PST stated that such storage of newspaper articles was not a widespread practice.

With reference to the fact that the information can be retrieved by searching the register, the Committee assumed that information in newspaper articles stored in Smart must also meet the requirements set out in the Police Register Act regarding specification of purpose, necessity and relevance.⁴³ The Committee urged PST to change its practice. PST's response was that, based on the purpose of the Act and material considerations, the service did not find it correct or appropriate to change its practice.

Based on the above, the Committee requested the Ministry of Justice and Public Security to assess PST's interpretation



of the law. The Ministry also stated that the processing of personal data from published newspaper articles must meet the requirements regarding specification of purpose, necessity and relevance when registered in PST's intelligence register.

In its response to the Committee concerning the Ministry's view, PST stated that the current law does not take sufficient account of PST's need to process information that may be deemed contextual or describing sources. PST stated that the service is working on a proposal for regulatory amendment to highlight this need and a possible legal solution. Until a clear legal basis has been established, the service will change its practice.

The Committee notes that PST will redact personal data that are not relevant and necessary to the service in cases where PST finds it necessary to store newspaper articles in Smart. The Committee will monitor the development in PST's work to have the regulations amended.

5.9 PST's notification to Nkom when mobile-restricted zones are established and facilitation of the Committee's oversight of notifications

In an inspection of PST, the Committee checked whether the service had fulfilled its statutory duty to notify⁴⁴ the Norwegian Communications Authority (Nkom) when using mobile-restricted zones.⁴⁵ The Committee's investigation did not uncover any breaches of this duty. The service has facilitated the Committee's oversight based on questions from the Committee so that it can find information about and gain an overview of all use of mobile-restricted zones and notification to Nkom.

When concluding the case, the Committee stated that the service's solution is satisfactory for the purposes of the Committee's oversight.

5.10 Challenges in cooperation project with other oversight bodies caused by changes in PST's transparency

The Committee, represented by the Secretariat, has since 2016 taken part in an international project relating to

democratic oversight of the services' exchange of personal data across national borders. The project is still ongoing.

In connection with the Committee's project work on PST and NIS's exchange of information about foreign terrorist fighters with cooperating foreign services, classified draft contributions to a common project report have been sent to PST and NIS to be checked for factual errors and classified information.

In its response on the draft report, PST stated that the Committee's description of most of the service's international cooperation relationships was *classified information*, and the service requested that 'the cooperation be described in more general terms and that the examples be left out'.

After the Committee referred to the fact that the information about the cooperation relationships was taken from PST's own website, PST stated, among other things, that '[i]nformation that is subject to confidentiality, but not necessarily classified under the provisions of the Security Act, applies in particular to PST's participation in various international forums and cooperation with specific services or organisations'. PST stated that the service had removed the information about specific cooperation relationships from its own website.

The report's text on cooperation relationships was modified based on the response from PST. In its response to PST, the Committee noted that the service claimed that it is customary in international forums that information about cooperation between the services is not made public.

In its concluding letter to the service, the Committee concluded that PST does not practice the same transparency as its colleagues in other countries. The Committee again referred to the fact that PST's participation in the international forums in question has already been made public, and confirmed, including by the service itself, cooperating services and PST's superior authority.

As a consequence of this, the Committee cannot discuss international cooperation that PST takes part in, even when information about it is publicly available and known to other countries' oversight bodies. Worse, the cooperation project is suffering because the project report will have to be much

41 The Committee also refers to section 4 of its consultation statement submitted in connection with the Ministry's consultation concerning the processing of surplus information from monitoring of communications etc. The consultation statement was submitted before the present case had been concluded in relation to the Ministry.

42 Cf. the Police Register Act Section 2(2).

43 Cf. the Police Register Act Section 64, cf. Sections 4, 5 and 6.

44 Act No 83 of 4 July 2003 relating to Electronic Communications (The Electronic Communications Act) Section 6-2a.

45 A mobile-restricted zone is defined as a limited geographic area in which communication in electronic communications networks used for public mobile communication is affected or obstructed using legal identity capture and/or jamming, cf. the Electronic Communications Act Section 1-5(19).

more general than desirable. This contributes to making it more challenging to achieve closer cooperation between oversight bodies on the oversight of international exchange of information. The Committee considers this unfortunate for international cooperation in the oversight area.

5.11 Follow-up of findings in file areas in PST's network

In previous annual reports, the Committee has discussed PST's processing of intelligence information and personal data in file areas⁴⁶ outside of the ordinary intelligence system. In 2017, PST has informed the Committee that the service has 'initiated work to change the internal regulations to ensure that they regulate the above-mentioned needs in a satisfactory manner within the framework of the Police Register Act. In connection with this, PST has appointed a working group to review the needs and the status in the file areas, as well as to develop good and expedient interim storage procedures.'

The Committee will keep informed about PST's ongoing work and continue its oversight of information that PST processes in its file areas.

5.12 PST's processing of information about deceased persons

In its annual report for 2016 section 4.5, the Committee criticised the service for having processed data about persons for several years after their death without this being necessary.⁴⁷ The Committee noted that the service was working on a technical solution to ensure that registrations are reviewed shortly after the service receives information about the death of a registered person. In 2017, PST informed the Committee that the service introduced a new script in the intelligence register with effect from 1 January 2017, and that this script contains a category for 'dead objects in need of review'.

The Committee assumes that the use of the new script will help to ensure that the service will review information about persons registered as dead at an earlier stage than was common under the old practice, which was not until the five-year review.

5.13 Norwegian persons registered in the FBI Terrorist Screening Center's (TSC) databas

In its annual reports for 2013 and 2014, the Committee mentioned that it had been informed that information about quite a large number of Norwegians had been processed in a database belonging to the Terrorist Screening Center

(TSC), which is an FBI unit. The purpose of the database is to identify suspected or potential terrorists. The Committee has previously emphasised that it is problematic that information about Norwegian persons and persons with connections to Norway has been processed in the FBI database TSC without the basis for their registration being known. The annual report for 2014 described how the Minister of Justice and Public Security informed the Committee that he would continue to follow up the matter in relation to the American authorities and provide a satisfactory reply to the Committee's question once such clarification had been received.

In the annual report for 2016 section 4.9.1, the EOS Committee stated that it had asked the Ministry of Justice and Public Security for information about the status of the Ministry's follow-up of the matter since the Committee's annual report for 2014, including any further dialogue with the American authorities. The Committee had contacted the Ministry in connection with this matter on three separate occasions,⁴⁸ without receiving a reply. In its recommendation⁴⁹ to the EOS Committee's annual report for 2016, the Standing Committee on Scrutiny and Constitutional Affairs stated that it 'finds it incomprehensible that an enquiry relating to a foreign state storing information about persons with connections to Norway remains unanswered'.

The Committee has, in letters of August and December 2017, asked the Ministry of Justice and Public Security for information about the status of the Ministry's follow-up of the matter. At the time of the Committee's final consideration of this annual report,⁵⁰ the EOS Committee had still not received any response from the Ministry.

5.14 Complaint cases considered by the Committee

The Committee received 12 complaints against PST in 2017, compared with 20 complaints in 2016. 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 the complaint gave grounds for criticism.⁵¹

The Committee concluded six complaint cases against PST without criticism in 2017. In one complaint case, the Committee found grounds for criticising PST. This complaint concerned PST's behaviour in relation to the complainant during an open investigation. PST conducted a search of the complainant's home without having obtained the court's permission. PST may conduct searches without the court's

approval 'if delay entails any risk', cf. the Criminal Procedure Act Section 197 second paragraph. In the Committee's opinion, PST did not substantiate that a delay would entail any risk. The service should therefore have obtained the court's permission before conducting the search. The Committee believes that the condition 'if delay entails any risk' was not met, and criticised PST for conducting a search of the complainant's home without court approval. The complainant was informed of this.

The annual report for 2016 shows that the Committee expressed criticism against PST in two complaint cases. In both cases, the Committee submitted a request to the Ministry of Justice and Public Security for more detailed explanation to be given to the complainants, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Services in force at the time, Section 8 second paragraph.⁵² The Committee had not received a reply from the Ministry at the time of the consideration of its annual report for 2016.

In 2017, the Committee was allowed to give the complainants in the two cases a more detailed explanation than just that the complaint gave grounds for criticising PST. The Committee is satisfied that the Ministry granted permission for this.

In one of the cases, which concerned a complaint regarding unlawful surveillance of telephone and e-mail communication, the Committee expressed mild criticism against PST for processing information about the complainant that the service had no grounds for processing.⁵³ The complainant was informed about this, and about the fact that the situation that warranted criticism had been brought to an end and that the Committee's investigation had not uncovered matters of the nature claimed in the complaint.

The other case concerned PST's processing of information about a person who expressed criticism of the authorities in e-mails to the Office of the Prime Minister. In its concluding letter to PST and the complainant, the Committee stated that there was no basis for processing information about the person in the first place, and that the information had been stored for longer than necessary for PST's purpose of the processing. The Committee also stated that the processing was in breach of the prohibition in Section 15 of the PST Regulations in force at the time⁵⁴ against processing information about a person based solely on, e.g., what is known about the person's political conviction. The service was criticised for this. PST subsequently disagreed that the service had breached the PST Regulations Section 15.

It took the Ministry four and six months, respectively, to reply to the Committee's requests for more detailed explanations to be given. In the latter of the two cases, it took another four months for the Ministry to provide a response capable of clarifying the basis for the criticism of PST for the complainant. The Ministry apologised for not responding to the Committee's enquiries sooner. As a consequence, complainants experience unreasonably long case processing time for their complaints to the Committee.

The Committee finds this unfortunate.

The Committee's limited possibility to give complainants grounds for its criticism of PST in complaint cases continues to represent a great challenge for the Committee, see section 3.

46 The annual report for 2016 section 4.7. The file area in question is what is called the I area (in the Windows file structure), and is thus outside PST's case processing system Smart.

47 Cf. the Police Register Regulations Section 22-3 first paragraph.

48 The Committee's letters of 1 April 2016, 26 October 2016 and 12 January 2017.

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

50 The Committee's final consideration of the annual report for 2017 took place at a meeting on 22 February 2018.

51 Cf. the Oversight Act Section 15 first paragraph: '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 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.'

52 Now regulated by the Oversight Act Section 15 first paragraph.

53 Cf. the Police Register Act Section 64.

54 Regulations No 92 of 19 August 2005 concerning the Norwegian Police Security Service (the PST Regulations). Now regulated by the Police Register Act Section 7.

6.

The National Security Authority (NSM)

6.1 General information about the oversight

The Committee carried out three inspections of NSM in 2017, including one of NSM NorCERT.⁵⁵ NSM attends to the general functions in the protective security services pursuant to the Security Act. NSM is the security clearance authority for its own personnel as well as for civil sector CTS clearance (the highest NATO security clearance level) in Norway, in addition to being the appellate body for clearance decisions made by other security clearance authorities.

During its inspections of the authority, the Committee focuses on the following:

- The authority'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 NorCERT's information processing.

During the inspections, the Committee is routinely briefed about NSM's ongoing activities, including its cooperation cases with other EOS services and processing time in security clearance cases. During the inspections, the Committee conducts searches directly in NSM's electronic systems.

When deciding whether to grant security clearance, the clearance authority shall assess whether the reliability, loyalty and sound judgement of the person concerned indicate that he or she is fit to process sensitive information.⁵⁶ A decision in a security clearance case can be crucial for a person's career, and strict requirements must therefore be applied to the processing of such cases. Based on the above, and because the processing of security clearance cases is a more closed process than case processing in relation to other administrative decisions, the Committee maintains a particular focus on such cases.

6.2 Case processing procedures in security clearance cases

Security clearance cases start with the person for whom security clearance is sought filling in information about him/herself and his/her closely related persons in the personal particulars form. The employer (requesting authority) submits the form along with a request for security clearance to the security clearance authority. The need for security clearance must be specified in this form. The security clearance

authority obtains information about the person in question from a number of registers and carries out an assessment, based on the information provided by the person him/herself and obtained from the registers, of whether the person concerned is fit to process classified information. If the requested security clearance is granted, the employer will be notified. If the requested security clearance is not granted, the person concerned will be notified and given grounds for the decision and the opportunity to appeal the decision.

In the Committee's annual report for 2013,⁵⁷ it requested that NSM review its procedures for handling access to documents. In 2017, NSM published a guide containing its recommendations on how the Security Act's provisions on access should be interpreted and practised. The purpose of this guide is to cultivate a clear and uniform practice, as well as to simplify the processing of access to information cases.

The Committee shares NSM's expectation that the guide will have an effect in terms of equal treatment, efficiency and security in connection with requests for access to information. The Committee is satisfied with the fact that the guide has been published on NSM's website so that people in a security clearance process can access detailed information about how requests for access are to be considered and processed.

6.3 Case processing times in security clearance cases

The Committee has pointed out in its last six annual reports that case processing times are far too long in many security clearance cases.

The basis for the Committee's focus on case processing times in security clearance cases is that a decision in a security clearance case is often crucial to a person's life situation and future career. The Committee has kept informed about case processing times in security clearance cases in connection with its inspections.⁵⁸ NSM has informed the Committee during the year that the number of security clearance cases under consideration has been significantly reduced, from 301 ongoing cases in December 2016 to 106 cases in December 2017.

The Committee notes that the average case processing time in complaint cases has increased compared with the case processing time given in December 2016.⁵⁹ NSM

55 NSM NorCERT (Norwegian Computer Emergency Response Team) is Norway's national centre for coordination of incident management in connection with serious ICT security incidents. NSM NorCERT is a function attended to by NSM's Department for ICT Security.

56 Cf. the Security Act Section 21 first paragraph.

57 See Chapter V section 7 in the Committee's annual report for 2013.

58 See the table of average case processing times communicated to the Committee in connection with inspections in 2017.

59 160 days in December 2017, compared with 82 days in December 2016.

has informed the Committee about several measures implemented to reduce the case processing time. The Committee expects NSM to continue its efforts to reduce case processing times in security clearance cases.

In 2017, the Committee has also kept informed about case processing times in cases concerning requests for access to information in security clearance cases. The average case processing time for requests for access was just under three months in May 2017, and just over two months in December 2017. Since requests for access of information rarely involve material questions of doubt, the Committee finds this case processing time to be much too long.

The Committee notes that the average case processing time for requests for access to information has increased somewhat since 2016. In the Committee's opinion, the case processing time still should be considerably reduced. The Committee expects NSM to continue to give priority to this case category.

6.4 Revocation of security clearance – the line between disciplinary matters and security clearance cases

As part of its review of security clearance cases, the Committee asked NSM questions in which the authority, as the appellate body, had upheld the security clearance authority's decision to revoke a security clearance because the person in question allegedly had acted in a manner that was disloyal to the employer. The decision to deny security clearance was upheld, and a three-year observation period was imposed on the person concerned. This means that another request for security clearance cannot be submitted until three years have passed since the decision to refuse.

The Committee asked NSM to explain the basis for this case being considered within the framework of the security clearance system, since the matter actually appeared to be

a conflict between an employer and an employee. NSM was also asked to explain how the person in question's breach of the employer's guidelines on work-related matters gave rise to 'reasonable doubt' about the person's ability and willingness to process classified information. Furthermore, NSM was asked to explain whether revoking the person's security clearance was a proportional reaction seen in relation to the facts of the case, cf. the Security Act Section 6, the assessment regarding the observation period, and generally how NSM ensures that the security clearance system is not abused to 'get rid of' employees the employer would not otherwise have a legal basis for dismissing.

After receiving response from NSM, the Committee agreed that 'matters of relevance in disciplinary matters can also be relevant in assessing suitability for security clearance', provided that the matters are 'relevant to evaluating the reliability, loyalty and sound judgement of the person concerned in relation to the processing of sensitive information', cf. the Security Act Section 21.

The Committee pointed out that the decision to revoke the person in question's security clearance had been considered in relation to the Security Act Section 21 first paragraph letter l) concerning 'Other matters', a provision intended as a 'safety valve'. The subject for evaluation is whether the person in question 'is capable of maintaining secrecy about sensitive information and can otherwise be deemed to be suited for security clearance' in order to, as far as possible, 'exclude any doubt that the person in question will act in accordance with the requirements that apply to dealing with sensitive information'.⁶⁰

There was little doubt that the person in question had failed to comply with the employer's instructions and guidelines, and that the person had thus demonstrated a lack of loyalty in relation to the employer's managerial prerogative. The Committee was nevertheless of the opinion that it did not necessarily follow from this that the person had or could behave disloyally in security matters. In the Committee's

Table of case processing times given in connection with inspections:

Types of cases	Inspection in May 2017		Inspection in December 2017	
	No of cases	Average case processing time	No of cases	Average case processing time
Requests for access	18	81 dager	7	65 days
Requests for security clearance	211	99	258	78
First-tier appeals	13	114	19	126
Second-tier appeals	28	140	117	160

opinion, there were no concrete circumstances in the case that gave any indication that the person in question had or could behave in an unreliable or disloyal manner in security matters, or that the person otherwise represented a security risk in relation to the processing of classified information.

The Committee also referred to the fact that NSM, in its own internal grounds, pointed precisely to several factors that indicated that the case was really about a disciplinary matter. The Committee commented to NSM that it therefore gave cause for concern for the person in question's legal rights that the matter was dealt with as an authorisation and security clearance case.

The Committee concluded that it was highly doubtful whether the person's disloyal actions in relation to the employer were relevant factors to consider in a personnel security case. The Committee therefore requested NSM to reconsider the security clearance case and conduct a security interview with the person in question in connection with this, cf. the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 7 final paragraph.

The Committee also found reason to criticise NSM for the long case processing time, since about 14 months passed from the security clearance authority upheld its own decision to deny security clearance in the initial consideration of the appeal until the person received a letter containing NSM's decision as the appellate body.

NSM later informed the Committee that it would *not* reconsider the case.

In its concluding statement to NSM, the Committee emphasised that trust in the security clearance system depends on it being beyond doubt that the system is not abused to get rid of employees that the employer would not otherwise have a legal basis for summarily dismissing or otherwise terminating the employment relationship with.

Based on the above, and not least the personal consequences the security clearance revocation had for the person in question, the Committee remarked that NSM's unwillingness to comply with the Committee's request was in contravention of the intentions of the Storting regarding follow-up of criticism or recommendations from the EOS Committee. The Committee also remarked that NSM also had problematised whether the case primarily concerned a disciplinary matter. The Committee underlined that the slightest indication that this is the case should trigger follow-up by the superior authority.

NSM then informed the Committee that it would reconsider the case. The case was reviewed by new case officers, and another security interview was conducted with the person in question. NSM's conclusion was still that the person 'was not suited for security clearance at the present time'. The Committee is aware that the person in question will be dismissed from work because of the refusal to grant security clearance.

The Committee took note of the fact that NSM again concluded that the person in question's failure to comply with the employer's instructions and guidelines in the case in question gave rise to reasonable doubt about the person's suitability for security clearance. This conclusion was reached despite the fact that a conflict between the employer and the employee concerned plays a significant role in the case, and that there are no other circumstances in the case that give grounds for doubting the person's suitability for security clearance. The Committee has no authority to instruct the EOS services to reverse a decision, and the case is therefore finally concluded on the part of the Committee.

6.5 Downloading and storage of sensitive personal data by NSM NorCERT

NSM NorCERT's purpose is to be a 'national response function for serious cyberattacks against critical infrastructure', and to run a 'national warning system for digital infrastructure'.⁶¹ The Committee carries out regular oversight activities in relation to NSM NorCERT, including its processing of personal data.

The Green Party's list of members was leaked on the internet following a cyberattack against the party's website in June 2016. NSM NorCERT asked the party for information about the attack and offered its assistance.

During an inspection in February 2017, the Committee discovered that NSM NorCERT had downloaded the list of Green Party members from the internet. The list of members was stored in NSM NorCERT's computer systems for more than seven months, and was deleted just after the Committee's inspection.

The Committee referred to the fact that information relating to political opinions is defined as sensitive personal data under the Personal Data Act.⁶² The Committee asked NSM to explain why the sensitive personal data was downloaded and whether the authority was of the opinion that it had a legal basis for processing this information.

60 Cf. Proposition No 49 to the Odelsting (1996–1997), section 9.6.1.

61 The Security Act Section 9 first paragraph letter e).

62 Act No 31 of 14 April 2000 relating to the Processing of Personal Data (the Personal Data Act) Section 2 (8) letter a).

In addition to giving an account of the above-mentioned facts, NSM stated that the list of members was downloaded to prevent its further spread on the internet and the Green Party was kept informed. As regards the question of legal basis, the NSM replied as follows:

'After reviewing the assessment, we now see that it is doubtful whether [the Personal Data Act] Section 9e provides a sufficient legal basis, and that another legal basis for downloading the material should have been sought'.

NSM also wrote that the Security Act did not preclude NSM NorCERT from processing sensitive personal data, and that downloading the list of members was necessary for security reasons.

When concluding the case, the Committee stated that the downloading and storage of the list of members by NSM NorCERT constituted processing⁶³ of sensitive personal data in the sense of the Personal Data Act. The Committee referred to the fact that the provisions of the Security Act do not in themselves give NSM NorCERT a legal basis for processing sensitive personal data. Moreover, it is a breach of NSM's own internal instructions to obtain and store such personal data. The Committee therefore criticised NSM NorCERT for having processed sensitive personal data without a legal basis and in breach of internal instructions.

NSM apologised for downloading the list of members and stated that it has taken action in the form of a revision of their instructions and better quality assurance of the basis for processing. The purpose of this is to prevent a similar situation from occurring in cases where NorCERT is made aware that sensitive personal data may have been compromised.

The Committee recognises that situations may arise in which NSM NorCERT will have an operational need to process sensitive personal data. The Committee presupposes that NSM takes the initiative for necessary regulatory changes.

6.6 Statement on processing of personal data for the purpose of investigating incidents that pose a threat to security

The Committee has noted in the course of its oversight activities that registers and pertaining reports on incidents that pose a threat to security also contain personal data about affected persons. The Regulations concerning Information Security⁶⁴ (hereinafter referred to as the Regulations) Section 5-4 second paragraph second sentence states that '[t]he register with pertaining reports shall be stored for at least five years'.

The Personal Data Act stipulates that information processed shall not be stored for 'longer than is necessary for the

purpose of the processing'.⁶⁵ The same requirement is set out in e.g. the Instructions for Defence Security Service (hereinafter referred to as the Instructions).⁶⁶ The Personal Data Act⁶⁷ stipulates that the data is to be destroyed, unless otherwise provided for in the Archives Act⁶⁸ or other legislation.

Based on the above, the Committee raised several issues with NSM as the superior security authority, including how the storage regime for reporting of incidents that pose a threat to security pursuant to the Regulations relate to the regulatory regime for processing of personal data in the enterprises that fall within the scope of the Security Act. NSM was asked to give an account of what type of information the Regulations instruct the enterprises that fall within the scope of the Security Act to store in connection with incidents that pose a threat to security and to what extent the Regulations Section 5-4 take account of the regulatory framework for processing of personal data. The Committee also asked NSM to consider whether considerations for the protection of individuals' privacy may indicate that personal data should be deleted before five years have passed, even in cases where security considerations could give grounds for five-year processing of information about the actual incident that posed a threat to security and its follow-up.

The Committee takes a positive view of the fact that NSM stated in its reply that it is working on a policy for what kind of information can be registered in connection with investigations into incidents that pose a threat to security. The Committee noted that NSM plans for a distinction to be made between a report and a register of incidents (based on de-identified data).

When concluding the case, the Committee urged NSM to clarify in greater detail the extent to which and how enterprises that fall within the scope of the Security Act are to process personal data as part of investigations into incidents that pose a threat to security. The background for this was that the Ministry of Defence did not follow up the Security Commission's⁶⁹ proposal to include a separate provision on the processing of personal data⁷⁰ in Proposition No 153 to the Storting (Bill) (2016–2017) *om lov om nasjonal sikkerhet (sikkerhetsloven)* ('on the act relating to national security (the Security Act)' – in Norwegian only).

The Committee noted that NSM agreed that it must be possible to delete personal data that is no longer necessary for the purpose of the processing, provided that there is a formal basis in the regulatory framework for archives for doing so. The Committee urged NSM to clarify which formal conditions must be in place for personal data to be deleted.

The Committee remarked to NSM that it is important for considerations of protection of privacy to clarify the extent to which personal data can be processed as part of the reporting of incidents that pose a threat to security. And that any

processing must be relevant and necessary to the purpose of the processing – namely to investigate the circumstances surrounding an incident that posed a threat to security.

Finally, the Committee commented on the special position of processing of personal data in enterprises that engage in protective security services and that fall within the EOS Committee's oversight area. Unlike the Norwegian Data Protection Authority, the EOS Committee cannot order enterprises to delete or restrict access to personal data.⁷¹ Moreover, in order to request that processed personal data be deleted or access to them restricted, the person registered has to be aware of the processing, and this will not necessarily be the case when data is processed as part of protective security services.

The Committee emphasises the importance of the enterprises that fall within the scope of the Security Act having a high level of awareness of what investigations they can carry out as part of the investigation of incidents that pose a threat to security, what methods they can use and which types of information they can obtain and process.

The Committee will keep informed about the work on a policy

for the collection and storage of information related to incidents that pose a threat to security.

6.7 NSM's use of mobile-restricted zones

NSM may, in exceptional cases and for a short period of time, use mobile-restricted zones to secure conference rooms.⁷² A mobile-restricted zone is defined as a limited geographic area in which communication in electronic communications networks used for public mobile communication is affected or obstructed using legal identity capture and/or jamming.⁷³

In 2017, the Committee conducted oversight activities in relation to NSM's use of mobile-restricted zones in the years 2014, 2015 and 2016. The oversight took place by NSM submitting information to the Committee about when and where it has used mobile-restricted zones, the grounds, and a copy of the notifications submitted to the Norwegian Communications Authority.

The investigation did not uncover any violation of the regulatory framework in connection with NSM's use of mobile-restricted zones.



63 The term 'processing' in the Personal Data Act means any use of personal data, such as collection, registration, assembly, storage and extradition or a combination of such.

64 Regulations No 723 of 29 June 2001 concerning Information Security.

65 Cf. Section 11 first paragraph letter e) and Section 28 first paragraph.

66 Cf. Section 20 first paragraph letter c), cf. Section 24 second paragraph.

67 Cf. Section 28 first paragraph, and the Instructions Section 24 third paragraph.

68 Act No 126 of 4 December 1992 concerning Archives (the Archives Act).

69 Official Norwegian Report NOU 2016:19 Samhandling for sikkerhet ('Cooperation for security' – in Norwegian only).

70 Proposition No 153 to the Storting (Bill) chapter 9.4 page 82.

71 Cf. the Personal Data Act Section 28 fourth paragraph.

72 Cf. the Electronic Communications Act Section 6-2a.

73 Cf. the Electronic Communications Act Section 1-5(19).

6.8 Complaint cases considered by the Committee

6.8.1 Introduction

The Committee received three complaints against NSM in 2017. One of them came from a complainant who claimed to be subjected to unlawful surveillance. The other two complaints concerned security clearance cases.

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

In its annual report for 2014,⁷⁴ the Committee criticised NSM for having made a decision regarding the merits of a security clearance case before considering the appeal against the decision to deny access to the documents in the case. Six months after the Committee's statement about the case, and one year and six months after the appeal against the decision was submitted, the NSM reached a decision regarding the decision to deny access. The Committee has subsequently criticised NSM for its long case processing time in the processing of the appeal against the decision to deny access, and stated that it was unfortunate that six months passed from the Committee made its statement until the appeal concerning access was considered. The Committee emphasised in its communication with NSM how important it is that the authority demonstrate an understanding of the Committee's oversight, including by following up the Committee's statements within a reasonable period of time.

Of the cases that the Committee concluded in 2017, the following four cases gave grounds for critical remarks from the Committee:

6.8.2 Complaint case 1 – No need for security clearance – criticism of the security clearance authority and NSM

In a complaint concerning a decision to refuse security clearance, the complainant also asked the Committee to investigate whether a security clearance was even necessary for the position. The Committee asked the requesting authority (the employer) to document and give grounds for the need for security clearance for the position in question.⁷⁵ The Committee forwarded the employer's grounds to NSM for assessment. Based on the Committee's enquiry, NSM carried out supervisory activities in relation to the enterprise and concluded that there was no real need for security clearance of personnel in the position in question. NSM was also of the opinion that the grounds and documentation provided for the request for security clearance were inadequate.

The authority that made the initial decision should have dismissed the request for security clearance. Vetting information should therefore not have been obtained, and no decision should have been made. Furthermore, this error should have been identified by NSM as the appellate body.

In NSM's opinion, the negative decision to refuse security clearance was invalid. As a result, the decision could simply be disregarded with immediate effect. NSM informed both the complainant and the employer of this. The employer later informed the Committee that the complainant had been reinstated to the position.

When concluding the case, the Committee based its assessment on NSM's account of the case processing errors committed and endorsed the authority's assessment that the decision was invalid. There was no legal basis for a security clearance process in relation to the complainant. The Committee also stated:

'It warrants strong criticism that the security clearance authority implemented an intrusive measure without there being a real need for security clearance. This means that the measure lacked a legal basis. The EOS Committee notes that NSM will implement several measures to help to limit the risk of such errors occurring in future.'

The Committee's review of the security clearance case has shown that both [the body that made the initial decision] and NSM have processed a lot of detailed information about [the appellant]'s private life. The Committee is of the opinion that the security clearance case without a legal basis has resulted in a clear violation of [the complainant]'s right to privacy.

The Committee notes that NSM has anonymised [the complainant]'s security clearance case and restricted access to it in the case processing system for security clearance cases.

The security clearance case without a legal basis has had several actual negative consequences for [the complainant]. The EOS Committee would like to draw particular attention to the complainant's account of the major personal, professional and financial consequences that the negative decision had for [the complainant]. This case serves to illustrate how a decision in a security clearance case can be of vital importance to a person's life situation and future career.'

The Committee is of the opinion that the security clearance authority and NSM have clearly violated the complainant's rights in a manner that warrants strong criticism; cf. the Oversight Act Section 2 first paragraph (1) and (3).

It is important to the Committee that the need for a security clearance must be real, and the Committee has opened a case to consider general issues that this complaint case has given rise to.

6.8.3 Complaint case 2 – Long case processing time in an access to information case

In 2017, the Committee considered a complaint against NSM for failure to respond to a request for access in a security clearance case. The complainant argued that the access case, in which NSM was to make the initial decision, had taken unreasonably long, and that this constituted a breach of good administrative practice. The complainant also requested access to all correspondence between the EOS Committee and NSM in the case.

The Committee's review found that it took NSM 87 days to make the initial decision in the access to information case. This was from the date when the complainant's lawyer filed the complaint against the decision to allow partial access.

In its concluding letter to NSM, the Committee criticised the authority because the case processing time in the access case was too long, because it did not respond to enquiries from the complainant's lawyer, and because no information about the expected case processing time was sent to the complainant. The complainant was also informed of this.

Both NSM and the EOS Committee gave the complainant access to all correspondence between the two parties.

6.8.4 Complaint case 3 – Failure to facilitate a complainant's access to information

In its annual report for 2016 section 5.8.4, the Committee described a complaint case where, among other things, it criticised NSM for the long case processing time in an access case. When the case originally was concluded on 24 January 2017, the Committee expressed its expectation for NSM to contact the complainant again shortly so that access to the documents in accordance with the decision to grant access could take place as intended.

Subsequent feedback from the complainant showed that NSM had not facilitated such access. After the Committee had requested on three occasions that NSM contact the complainant for access to take place, the authority informed the Committee that it did not see any reason for NSM to make further contact with the complainant. NSM added that it would facilitate access if contacted by the complainant.

The Committee commented to NSM that it had expected the authority to take active steps in relation to the complainant. In the Committee's view, NSM's failure to follow up the Committee's requests for active facilitation demonstrated an inadequate degree of understanding for the Committee's oversight. The Committee found that it warranted criticism that NSM did not comply with the Committee's requests to take active steps in relation to the complainant, regardless of which action the complainant might have taken.

The Committee referred to the fact that it has also criticised NSM for failure to facilitate and follow up access granted on previous occasions, cf. the Committee's annual report for 2015 section 5.6.4.

In October 2017, the complainant informed the Committee that NSM had finally made contact so that access to the documents in the case could take place at NSM's premises.

6.8.5 Complaint case 4 – Long case processing time and recording of a complainant and a lawyer during a break in a security interview

In one complaint case, the Committee criticised NSM for its long case processing time as the appellate body. The Committee had previously criticised FSA, which made the initial decision, for the same thing, and requested that NSM prioritise the consideration of the appeal. In its final statement to NSM, the Committee stated that the case processing time for the appeal, nearly 15 months, was unreasonably long, and made particular reference to the fact that it took nearly ten months before the authority took any action in the case.

With reference to the annual report for 2016,⁷⁶ the Committee levied criticism at NSM in the same appeal case for continuing to record the complainant and his lawyer during a break in the security interview when the interviewers had left the room. The security interview with the complainant took place before the Committee raised this practice with NSM in connection with an inspection in 2016.⁷⁷

The Committee stated that filming the complainant and his lawyer during breaks appeared particularly invasive in light of people's reasonable expectation of being able to communicate confidentially with one's lawyer.

74 Document 7:1 (2014–2015) section 4.8, Complaint 5 – Processing of a complaint regarding access to documents of a case.

75 Cf. the Security Act Section 19 and Regulations No 722 of 29 June concerning Personnel Security (the Personnel Regulations) Section 3-1.

76 The EOS Committee's annual report for 2016, Document 7:1 (2016–2017) section 5.4.

77 The EOS Committee's annual report for 2016, Document 7:1 (2016–2017) section 5.4.

The background of the slide is a blue-tinted image. On the left side, there is a close-up of a camera lens. On the right side, there is a faint, semi-transparent image of a globe showing the continents. The overall aesthetic is professional and technical.

7.

The Norwegian Defence Security Department (FSA)

7.1 General information about the oversight

The Committee conducted two inspections of FSA in 2017.

During its inspections of the department, the Committee focuses on the following:

- FSA's processing of cases where security clearance has been denied, reduced or suspended by the security clearance authorities
- FSA's cooperation with other EOS services
- FSA's protective security activities

During the inspections, the Committee is regularly briefed about FSA's ongoing activities.

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. With effect from 1 January 2017, FSA became the security clearance authority for the defence sector,⁷⁸ and took over responsibility for security clearance cases from the Ministry of Defence and the Norwegian Defence Estates Agency. As a result of this, FSA's portfolio has grown. The Committee reviews most of the negative security clearance decisions made by FSA, as well as appealed security clearance cases where the department granted the appeal in part or in full.

The Committee also oversees FSA's protective security activities and carries out spot checks of investigations into activity that poses a threat to security targeting the Armed Forces (security investigations) and operational cases that are part of the agency's responsibility for military counterintelligence in Norway in peacetime. One of the Committee's primary duties in this connection is to oversee FSA's processing of personal data as part of its protective security activities.

The Committee received one complaint against FSA in 2017. This complaint was also against PST and the Intelligence Service. The complaint case was concluded without criticism of FSA. In 2016, the Committee received four complaints and enquiries concerning FSA.

7.2 FSA's photography and filming of persons in non-military areas during an exercise

During an inspection of FSA, the Committee found a folder

containing 532 files from an exercise that took place in a civilian area in Oslo. The files were from a military counter-intelligence exercise in autumn 2015, and contained many photos and films of people. Part of the exercise took place inside a café. The Instructions for Defence Security Service Section 15 states that 'education, training and practice in methods that entail an interference with persons' legal sphere can only take place on Norwegian territory in peacetime in relation to participants who have given informed consent in advance'.

In response to a question from the Committee, FSA replied that the course participants had consented to being photographed and filmed. The material was stored for longer than necessary before being deleted.

As regards persons who did not take part in the exercise, but who were photographed and filmed, FSA replied that '[a]s regards third parties who may have been photographed or filmed, reference is made to the fact that they were not participants in the exercise and therefore are not part of the group of persons from which consent is required'. FSA referred to the fact that the photographs and video recordings were only aimed at course participants, and assumed that any images of third parties fell outside the scope of the definition in the Personal Data Act Section 2(1).

In its concluding statement to FSA, the Committee criticised the department for having stored personal data for more than a year longer than the participants had consented to. The Committee noted that FSA had reviewed its procedures to ensure that information is processed in accordance with the regulatory framework.⁷⁹

The Committee considered whether photographing persons who did not take part in the exercise should be deemed to be processing of personal data⁸⁰ or an interference with persons' legal sphere.⁸¹ The Committee referred to the fact that the term 'interference with persons' legal sphere' is not defined, but found that collecting photographs can constitute such interference because the department asked for the participants' consent to process photographs.

In its assessment of whether photographing the third parties constitutes processing of personal data in the sense of the Act, the Committee referred to the purpose⁸² of protecting natural persons from violation of their right to privacy as a factor that could have a bearing on the interpretation.⁸³ The following is quoted from the Committee's statement:

78 Cf. the Security Act Section 23, amended by Act No 78 of 12 August 2016 in force from 1 January 2017.

79 The Personal Data Act and the Instructions for Defence Security Service.

80 Cf. the Personal Data Act Section 2(2).

81 Cf. the above-mentioned Instructions Section 15.

82 Cf. the Personal Data Act Section 1 first paragraph.

83 This is clear from the preparatory works to the Personal Data Act, see Proposition No 92 to the Odelsting (1998–1999) p. 101.

'That the third parties are not the focus of the photos/ films is an indication that the material and its storage do not constitute a violation of these parties' right to privacy, and that the processing of information is not to be considered an interference with their legal sphere.

Indications to the opposite include that several of the persons shown can be identified, either from their appearance or from the licence number of their vehicles alone. This applies to the café staff in particular, since they were photographed and filmed more than passers-by and customers in connection with the exercise. It is also easier to identify them by linking information about their appearance and place of work. No notification was given about this activity, so it was not possible for third parties not to be photographed/filmed, and they were not at any time informed that they had been photographed/filmed. The third parties had no reason to believe that a unit from the Norwegian Armed Forces were carrying out an exercise in this location, since it was in a civilian, and not a military, area. Importance has also been attached to the argument that the party that photographed/recorded the material was an authority that can, to a certain extent, conduct covert security service activities, and that the material, even if it was to be deleted, was stored in the department's systems for more than a year after it was collected.'

FSA subsequently disagreed with the Committee's conclusion.

Following an overall assessment, the Committee is of the opinion that the information about third parties, to the extent that they can be identified from the images, must be deemed to be personal data. Photographing and filming them and subsequently storing the material entail an interference with their legal sphere, even if they were not the intended targets. The Committee therefore finds that they should have given informed consent.

7.3 Processing of personal data in FSA's computer network

The Committee regularly oversees FSA's processing of personal data. This topic has been discussed e.g. in the annual reports for 2010,⁸⁴ 2011,⁸⁵ 2012,⁸⁶ 2015⁸⁷ and 2016.⁸⁸

In 2017, the Committee put several questions to FSA in two cases concerning whether the department had a basis for processing information about persons in different databases and records, and how requirements relating to the processing of information are ensured and followed up.

FSA's analysis section marks documents to indicate whether they contain personal data or not. The Committee noted that eight documents contained information about named persons or identifying information such as images and vehicle licence numbers without the documents being marked as containing personal data. Among other things, the documents contained information that the named persons had committed security breaches. In one of the documents, FSA had given the following grounds for the marking: '[t]here are names related to the case, but nothing unfavourable is stated about them. Therefore, they are not considered personal data relating to a case, and are not ticked.' Based on the above, the Committee requested an account of FSA's interpretation of the term 'personal data', how registrations are followed up, and how the department ensures that the regulatory requirements pertaining to the processing of personal data are complied with.

FSA agreed that the documents contained personal data and amended its procedures to ensure that all documents that contain personal data are marked accordingly. The department also introduced a procedure whereby case officers have to specify a legal basis in order to create a registration that



contains personal data. This would ensure that requirements relating to the processing of personal data are followed up.

The Committee took note of the department's account and was pleased that FSA had changed its procedures for processing of personal data in the archive records.

The Committee also referred to an incident where FSA had registered information about a private individual who contacted the Navy. The registration stated that it could not be deleted until October 2020 at the earliest. The department nevertheless deleted the information as a consequence of the Committee's questions.

The Committee took a positive view of the fact that the information was deleted, as it did not meet the requirements for information processing.

An FSA record contained information about 536 events registered in 2005. The events included observations, enquiries and invitations that were perceived as suspicious, and information had been registered about persons linked to many of the events. In relation to 16 of these cases, the Committee asked whether FSA had carried out an assessment of whether it was necessary to process information about the persons in question, and whether the department believed that it was still necessary to process the personal data in question. Following these questions, FSA stated that the department no longer had a basis for processing the information and that the record had been deleted.

The Committee found it to be positive that the department deleted the register in its entirety, and not only the events that the Committee had questioned. However, the Committee criticised FSA for not having considered at an earlier time whether it was still necessary to store this information. Such an assessment should have taken place after five years at the latest, i.e. in 2010.

In connection with FSA's investigation of an incident that posed a threat to security, the department processed information in two documents about a person who was then employed by the Norwegian Armed Forces, and who had an affiliation to a motorcycle club. The information was registered in 2010. With reference to the rule that personal data should not be stored for longer than is necessary for the purpose of the processing,⁸⁹ the Committee put a question

to the department in 2017 about whether a basis for processing the information still existed. FSA stated that it was no longer necessary for the purpose to process the information in question, and referred to the requirements set out in the Regulations concerning Information Security Chapter 5⁹⁰ being met. The documents were deleted.

In its concluding letter to FSA, the Committee expressed its satisfaction that FSA had deleted the documents from its computer network because of the Committee's questions in the matter.

Information that a person who served in the Armed Forces had been in contact with a group that could harm interests of national security was registered in connection with a security investigation in 2012/2013. After an interview with the person in question, FSA assessed the contact as being non-ideological in nature and found that the person did not pose a risk. In response to a question from the Committee about whether it was still necessary for FSA to process information about this person, the department referred to the Regulations concerning Information Security Section 5-4, which states that registered incidents that pose a threat to security and reports relating to these incidents must be stored for a minimum of five years.

With reference to the fact that what was registered appeared to be a concern rather than a specific incident, and that the concern had long ago been found to be unfounded, the Committee urged FSA to delete the information about the person in question. The reason for this was that the information no longer seems to be necessary for the purpose of the processing, cf. the Instructions for Defence Security Service Section 24 second paragraph.

FSA maintained that the information had to be stored for a minimum of five years, and would not comply with the Committee's request.

The Committee do not has the authority to order the department to delete or restrict access to personal data, and therefore took note of FSA's response. The Committee has raised with NSM the issue of the relationship between the duty to store reports on incidents that pose a threat to security and the requirement for information to be deleted as soon as it is no longer necessary for the purpose of the processing. The Committee's requests to NSM in this context are described in section 6.6.

84 Chapter V section 3.

85 Chapter VI section 4.

86 Chapter VI section 6.

87 Section 6.3.

88 Section 6.2.

89 Cf. the Personal Data Act Section 11 first paragraph letter e).

90 The Regulations require registers of reports on incidents that pose a threat to security to be stored for a minimum of five years, cf. Section 5-4 second paragraph.

8.

The Norwegian Intelligence Service (NIS)



8.1 General information about the oversight

The Committee conducted three inspections of the NIS headquarters in 2017, in addition to inspections of two local stations: Varanger and Vardø.

The oversight of NIS focuses in particular on ensuring that the service does not violate the statutory prohibition against monitoring or in any other covert manner collect information concerning Norwegian physical or legal persons on Norwegian territory, cf. the Intelligence Service Act Section 4 first paragraph. Another key oversight point for the Committee is to oversee that the service complies with the Ministry of Defence's provisions regarding collecting and/or sharing of information concerning Norwegian persons outside Norwegian territory.

The Committee is to ensure that NIS's activities are carried out within the framework of the service's established responsibilities, cf. the Oversight Act Section 6 third paragraph (2). The oversight is also intended to ensure that NIS activities do not violate the rights of any persons or unduly harm the interests of society, that the activities are kept within the framework of statute law, administrative or military directives and non-statutory law, and that the means of intervention employed do not exceed those required under the circumstances, and that the service respects human rights, cf. the Oversight Act Section 2.

The Committee's oversight of NIS shall cover the service's technical activities, including surveillance and collecting of information and processing of personal data. The Committee shall ensure that the cooperation and exchange of information between NIS and domestic and foreign collaborative partners are kept within the legal framework and the applicable regulations, cf. the Oversight Act Section 6 second and third paragraphs.

In its inspections of NIS, the Committee focuses on the following:

- 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
- Cases submitted to the Ministry of Defence⁹¹ and internal approval cases

During the inspections, the Committee is routinely briefed about NIS's ongoing activities, including the service's cooperation cases with other EOS services, the threat situation and cases submitted to the Ministry of Defence, as well as internal approvals. Internal approval cases can be permission to share information about Norwegian legal persons with cooperating foreign services or to monitor Norwegian legal persons' means of communication when the persons are abroad. As the Committee has previously pointed out, the legislation does not require external permission from the courts for NIS to monitor Norwegian legal persons' means of communication abroad, as it does for PST in relation to e.g. monitoring of communications of persons in Norway.

In 2017, the Committee has been kept informed of non-conformities relating to NIS's technical information collection, and it has concluded its follow-up of a non-conformity case in the service, see section 8.3.

The Committee continued in 2017 its work to improve its understanding of NIS's demanding technical systems, installations and capacities, among other things through technical meetings with the service and the Committee's technical expert. The Committee is in the process of establishing its own technology unit with more technologists in the Committee Secretariat, in order to raise its competence in this and other areas.

8.2 Norwegian citizenship and connection to Norway

The regulatory framework relating to NIS sets limits for collecting information concerning persons on Norwegian territory. As a rule, NIS is prohibited from monitoring or in any other covert manner collect information concerning Norwegian physical or legal persons on Norwegian territory, cf. the Intelligence Service Act Section 4 first paragraph. Limitations also apply to its right to collect information about foreign persons in Norway or Norwegian persons abroad.⁹² Supplementary provisions⁹³ have also been adopted for NIS's collection of information concerning Norwegian persons⁹⁴ abroad.

In 2017, the Committee asked NIS to clarify, on a general basis, whether the service under certain circumstances would not consider a Norwegian citizen abroad to be 'Norwegian',

91 Cf. the Royal Decree of 31 August 2001 No 1012 relating to instructions for the Norwegian Intelligence Service Section 13 letter d stating that 'matters of particular importance or that raise questions of principle' shall be submitted to the Ministry of Defence for consideration.

92 Proposition No 50 to the Odelsting (1996–1997) chapter 9 page 10.

93 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, adopted by the Ministry of Defence on 24 June 2013 pursuant to the Instructions for the Norwegian Intelligence Service Section 17.

94 By 'Norwegian person' is meant a physical or legal person covered by Section 4 first paragraph of the Act relating to the Norwegian Intelligence Service, cf. the Supplementary provisions concerning the Norwegian Intelligence Service's collection of information concerning Norwegian persons abroad etc. Section 2(1).

provided that the person has no particular connection to Norway other than the citizenship. One consequence of not being considered a Norwegian person will be that the person in question will not be covered by the above-mentioned provisions concerning the service's collection of information concerning Norwegian persons abroad and the pertaining internal approval regime for such collection.

The reason for this question was that the service had carried out an internal assessment of whether or not a person abroad was to be considered 'Norwegian', despite the fact that the person in question is a Norwegian citizen. In the specific case in question, the person was deemed to be 'Norwegian'.

Based on the response from NIS, the Committee stated that it could not find any strong arguments or indications for carrying out an assessment of whether a *Norwegian citizen* has a 'close connection' to Norway or not, in order to consider the person 'Norwegian'. In the Committee's assessment, Norwegian citizenship means that a person is Norwegian, regardless of what connection NIS believes the person has to Norway. The Committee also commented that, given the requirements set out in the Ministry's provisions⁹⁵ regarding monitoring of Norwegian persons abroad, it found it somewhat difficult to see what NIS hopes to achieve by under certain circumstances not considering a Norwegian citizen to be Norwegian.

If a Norwegian citizen can be deemed to be 'non-Norwegian' in the eyes of NIS, the Committee believes that this could be in breach of the applicable provisions. Such a practice could

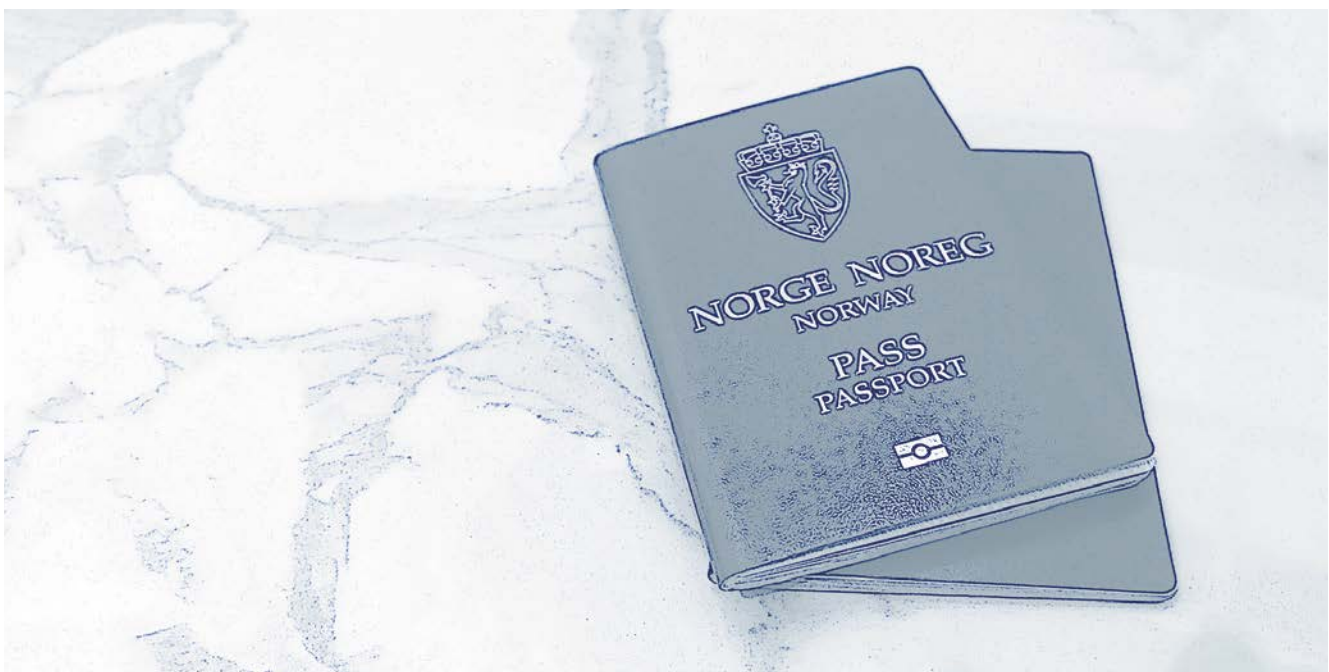
potentially have unforeseeable negative consequences for the legal position of Norwegian persons, particularly when it comes to disclosing information to cooperating foreign services.

The Committee noted that NIS considers that 'legal persons that hold Norwegian citizenship shall, as a rule, be considered "Norwegian person[s]" under Section 2(1) of the Ministry of Defence's provisions'.

However, NIS stated that 'special situations can be envisaged where, in exceptional cases, a Norwegian citizen is nevertheless not to be considered a "Norwegian person" under the internal approval regime', as illustrated by the service with a hypothetical example where a person holding both Norwegian and a foreign citizenship emigrates from Norway.

The Committee nevertheless expressed the opinion that it seems unnatural not to consider Norwegian citizens 'Norwegian'.

Considerations for parliamentary oversight of NIS's monitoring of Norwegian citizens is another reason why the Committee believed that persons who hold Norwegian citizenship should be considered 'Norwegian', regardless of any assessments of their connection to Norway or to abroad/a foreign state. They will then fall within the scope of the supplementary provisions concerning the the Norwegian Intelligence Service's collection of information concerning Norwegian persons abroad and the pertaining internal approval regime, which is subject to oversight by the Committee.



Both The NIS' and the Committee are of the opinion that it is necessary to clarify the territorial limitations of The NIS's collection activities in the new Act relating to the Norwegian Intelligence Service. This concerns the term 'covert', the term 'Norwegian' and issues relating to whom the collection activities target.

8.3 Non-conformities in NIS's technical information collection

Follow-up of non-conformity reported in 2016

In its annual report for 2016 section 7.1, the Committee stated that it would inform the Storting about the outcome of the Committee's follow-up of a non-conformity in the service's technical information collection that resulted in the unintentional collection of information from means of communication (hereinafter referred to as selectors) that were in reality Norwegian.

The service itself detected the non-conformities and informed the Committee. According to the service, the reason for this non-conformity was an error in the technical collection.

In response to the Committee's questions, the service gave detailed accounts, capable of clarifying how the error occurred and how the unintentional collection of information from selectors that were in fact Norwegian could take place. The Committee commented to the service that such errors could have consequences for the due process protection of Norwegian legal persons, and assumed that the service will focus on the challenges related to the error that caused the non-conformity, which the service itself has expressed that it will. This is positive. The Committee asked to be kept continually informed about NIS's procedures for detecting such errors.

When concluding the case, the Committee remarked that information appeared to have been collected from one of the selectors in violation of the prohibition stipulated in the Intelligence Service Act Section 4 first paragraph against covert monitoring of Norwegian citizens in Norway, despite the fact that the service cannot be blamed for the circumstances that resulted in information being wrongfully collected. As regards the other selector, the user of which remains unknown, the Committee noted that it was unclear whether the collection was in breach of the Intelligence Service Act Section 4. Considering the service's thorough accounts of the matter, the Committee did not find reason for further follow-up, other than to remark that information

was collected about the Norwegian selector outside the internal approval regime, even if the service could not be blamed for the underlying cause.

The Committee also noted that NIS would not review the wrongfully collected material, as it had previously stated, and that the service now wanted to delete the material immediately. Based on the above, the Committee found that it was no longer necessary for the Committee's oversight purpose to review the material before deleting it.

Finally, the Committee commented that the way in which the service has handled the non-conformities inspires trust and shows that NIS takes the matter seriously. The Committee also noted that such errors might occur again, but that the service has a strong awareness about minimising the possibility of such errors arising.

Non-conformities in 2017

The service has uncovered and informed the Committee about three non-conformity cases in 2017.

Non-conformity case 1

NIS reported a non-conformity, which, according to NIS, was due to a mistake on the part of a case officer. When it came to the service's attention that the selector from which information was collected did not belong to the person it was registered to in the service's systems, the service discontinued its collection activities. An error resulted in information about a person resident in Norway nevertheless being collected for a period of just under a year. The collection consisted of three calls during this period.

NIS has subsequently corrected the error and improved its procedures. NIS has itself deemed the collection to be in breach of the Intelligence Service Act Section 4, since objectively speaking, unlawful collection of information did take place during the period in question. The Committee agreed with this assessment.

The Committee will follow up aspects of the non-conformity case in relation to the service in 2018. The Committee will provide information about its follow-up in next year's annual report.

Non-conformity case 2

NIS reported a non-conformity where information had been collected about a Norwegian person abroad and probably also in Norway. The basis was an initial assessment that the likely user of the selector was abroad. NIS collected three calls in 2017. The first two contained no speech or other

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

content. The third sound recording contained a conversation. Based on an analysis and collation of information from this call as well as a dialogue with PST, NIS found that the person abroad was not the user of the selector, but that the user was probably in Norway. The selector was then deleted from NIS's systems.

The Committee has taken note of NSM's account of the non-conformity.

Non-conformity case 3

NIS reported a non-conformity related to a person who was initially assumed to be abroad. The service was later notified by FKTS⁹⁶ that the person had returned to Norway, without this resulting in the collection from the selectors being discontinued. Therefore, collection activities targeting the person's selectors were carried out for nine days before the error was detected. No information was collected from the selectors during this period, however. An internal review conducted by NIS found that the service's personnel was notified by FKTS on time, but that the NIS personnel did not discontinue the collection activities. NIS stated that a review with FKTS had been held to ensure that notification procedures are complied with. The service also reports that it has held an internal review on the importance of ensuring that information collection is discontinued in such cases.

The Committee has taken note of NIS's account and is satisfied that the service has reviewed its procedures.

The Committee takes a positive view of the fact that the service itself identifies non-conformities and reports them to the Committee during inspections of the service. The Committee is of the impression that the service takes such errors and non-conformities seriously and focuses on quality-assurance and procedures to minimise the possibility of such errors occurring again.

8.4 Processing of information about Norwegian persons in Norway

In connection with the Committee's oversight of the service's information systems, the Committee asked about the legal basis for processing personal data in a document that appears to have been prepared for training purposes for NIS and PST personnel. The document concerned Norwegian persons in Norway, among other things.

Based on the response from NIS, the Committee agreed with NIS's assessment that the basis for processing personal data for training purposes cannot be the same as the basis for the service's processing of personal data for intelligence purposes. The Committee nevertheless noted that the processing of personal information *on this concrete occasion exceeded what could be considered purely training purposes*, since the personal data of the persons in question were of intelligence relevance in the cooperation between NIS and PST.

8.5 Complaint cases considered by the Committee

The Committee received six complaints against NIS in 2017. Four of the complaints were also against PST, and one was against FSA.

One of the complaints concerned an appeal against an NIS decision to deny access to information. The case was concluded without criticism of NIS.

Five of the complaints concerned suspicion of unlawful surveillance. One of the complaints was dismissed because it gave no basis for initiating an investigation on the part of the Committee. The other four complaint cases were concluded without criticism of NIS.

9.

Oversight of other EOS services

9.1 General information about the oversight

The Committee regularly oversees the intelligence, surveillance and security services carried out by, under the control of or on the authority of the public administration.⁹⁷ In other words, the area of oversight is defined by function rather than being limited to certain entities.

Pursuant to the Directive relating to Oversight of the Intelligence, Surveillance and Security Service Section 11 subsection 2 letter e, the Committee should carry out annual inspections of at least two Intelligence Service units and/or intelligence/security services at military units, and of the personnel security service of at least two ministries/government agencies. This provision was repealed with effect from 21 June 2017 and replaced by the Oversight Act Section 7.

In its evaluation of the EOS Committee, the Evaluation Committee considered whether there are intelligence units in the Norwegian Armed Forces that should to a greater extent be subject to ordinary oversight⁹⁸ by the EOS Committee.⁹⁹ The Evaluation Committee proposed that the Army Intelligence Battalion and the Norwegian Special Operation Forces should be subject to ordinary oversight by the EOS Committee. The Standing Committee on Scrutiny and Constitutional Affairs endorsed the Evaluation

Committee's proposal,¹⁰⁰ and the private member's bill for amendments to the Oversight Act¹⁰¹ was adopted by the Storting.

The Oversight Act Section 7 second paragraph now in force requires the Committee to conduct at least one inspection per year of The Army intelligence battalion and the Norwegian Special Operation Forces, and 'at least one Intelligence Service unit or the intelligence/security services at a military staff/unit'.

In 2017, the Committee inspected the intelligence and security services of The Army intelligence battalion and the Norwegian Special Operation Command. The Committee has also inspected the personnel security services of the Office of the Prime Minister and the Office of the Auditor General of Norway.

The Committee's inspection of the Office of the Prime Minister gave grounds for follow-up, and is described in more detail in section 9.5.

In 2017, the Committee received three complaints against security clearance decisions made by the Ministry of Defence. In the course of the year, one complaint case against the Ministry of Defence was concluded without criticism. The Ministry of Defence is no longer a security

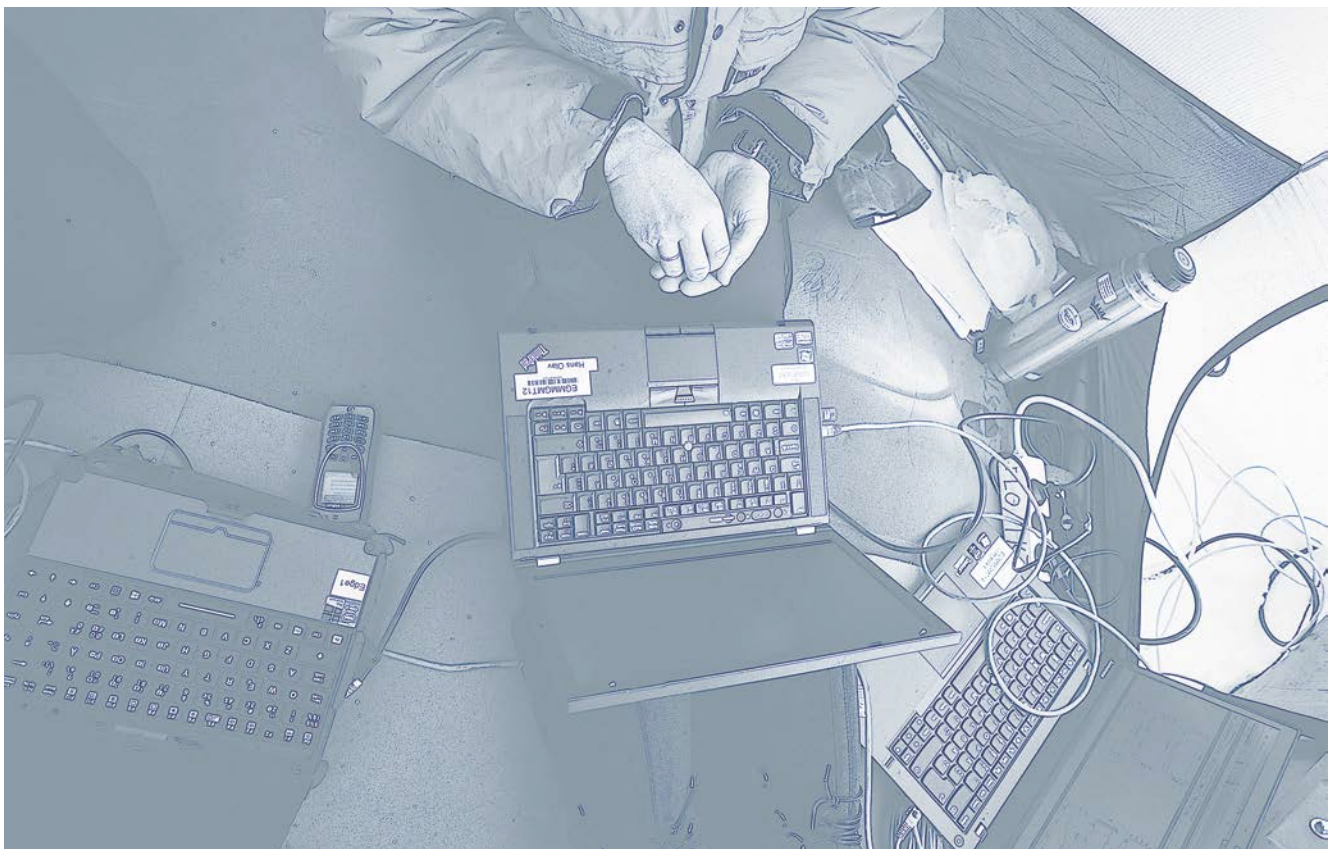


Photo: Simen Rudi / Forsvaret

clearance authority since the Storting decided in 2016 to change the clearance authority structure. The Ministry remains the appellate body for some security clearance decisions.

9.2 The Army intelligence battalion

The Oversight Act Section 7 second paragraph (5) requires the EOS Committee to carry out at least 'one inspection per year of The Army intelligence battalion'. According to the Evaluation Committee, the need for external oversight of The Army intelligence battalion relates to the risk of the tools and knowledge that the battalion possesses being used in irregular ways.

The Committee inspected The Army intelligence battalion in 2017. In connection with the inspection, the Committee was informed about the battalion's organisation, structure and capacities, cooperation with other EOS services and Armed Forces units, and the battalion's procedures for educating and training personnel in Norway. The Committee also inspected documents and information based on the Secretariat's preparation for the inspection, including thorough searches in computer systems. The inspection has helped the Committee to gain knowledge about the activities of The Army intelligence battalion. The Committee has followed up the inspection by obtaining some documents relating to what was inspected. The follow-up has not been concluded.

9.3 The Norwegian Special Operation Forces

The Oversight Act Section 7 second paragraph (6) requires the EOS committee to carry out at least 'one inspection per year of the Norwegian Special Operation Forces'. According to the Evaluation Committee, the need for external oversight relates to the unit's capacity to engage in intelligence activities and the risk of this capacity being used in Norway in peacetime or in other irregular ways. It should also be subject to oversight that the cooperation with NIS is kept within the framework of the applicable regulatory framework.

The Committee inspected the Norwegian Special Operation Command (NORSOCOM) in 2017. During the inspection, the Committee was briefed about NORSOCOM and the organisation and functions of the Norwegian Special Operation Forces, as well as their cooperation with the EOS services.

The Committee was also briefed about the Norwegian Special Operation Forces' capacity and capabilities to engage in intelligence operations, and procedures for educating and training personnel in Norway. The Committee focused on how NORSOCOM/the Norwegian Special Operation Forces handle personal data in operational contexts on Norwegian territory and during training and exercises. The Committee has obtained information about the regulatory framework that applies to NORSOCOM and the Norwegian Special Operation Forces. The inspection has helped the Committee to gain knowledge about the activities of NORSOCOM and the Norwegian Special Operation Forces.

9.4 The personnel security service of the Office of the Auditor General

The Committee carried out an inspection of the personnel security service of the Office of the Auditor General of Norway in 2017. The Office of the Auditor General remains the security clearance authority for its own personnel after the Storting decided in 2016 to change the clearance authority structure. During the inspection, the Committee focused in particular on reviewing the security clearance authority's negative security clearance decisions and case processing practices. The Committee has followed up the inspection by obtaining some documents. The follow-up has not been concluded.

9.5 Inspection of the personnel security service at the Office of the Prime Minister (OPM)

The Committee carried out an inspection of the personnel security service at the OPM in February 2017. During the inspection, the Committee noticed a security clearance case where a person had been granted clearance for a lower security classification than requested. In a letter to the OPM, the Committee referred to a number of requirements regarding case processing in security clearance cases, and requested that the OPM explain the office's processing of the case in question. The Committee also asked whether the OPM deemed the decision to be in accordance with the provisions of the Security Act.

In its reply, the OPM gave an account of the case processing and stated that the office 'considers that the case regarding security clearance of [the person in question] was processed

97 Cf. the Oversight Act Section 1 first paragraph.

98 The Evaluation Committee understands 'ordinary oversight' to mean inspections that the EOS Committee is obliged to conduct on a regular basis.

99 Doc. No 16 (2015-2016) p. 147.

100 Recommendation No 146 to the Storting (Resolution) (2016-2017) p. 49.

101 Doc. No 8:63 (Bill) (2016-2017), comments to Section 7.

in accordance with the procedural requirements that follow from the Security Act Chapter 6 on security of personnel. We also deem the actual security clearance decision to have been made in accordance with the law.¹⁰²

In its concluding statement, the Committee referred to the regulatory requirement¹⁰² that documentation is to be ensured by documenting case processing in writing. A decision to grant security clearance for a lower security classification than requested is a negative security clearance decision that triggers certain rights for the person concerned, including the requirement for the person to be informed in writing with grounds for the decision, and with information about the rights of appeal and access to information.

The Committee remarked that the person in question had not been informed of the result of the security clearance decision in writing, and that the OPM had obtained information from the person's referee at a former employer without minutes etc. being prepared to ensure documentation of the conversation.

The Committee also had comments to the OPM's internal grounds in the case. It is stated in NSM's guide to the Security Act Section 25 that '[t]he grounds must, in NSM's assessment, as a minimum mention the provisions and facts on which the decision is based'. The Committee could not see from the documents in the case that the OPM had referred to the legal basis for its assessment in the security clearance case. The reference to the legal basis only emerged in the OPM's reply to the Committee's questions.

The Committee also noted that in the OPM's reply to the Committee's questions, the office mentioned information from its security interview with the person in question that could not be found in the office's own notes from the security interview. Nor did the documents in the case give an unambiguous picture of the circumstances on which the OPM had based its assessment in the case. This complicated the Committee's oversight of the office's case processing and assessment.

The Committee stated that the review of the case had identified several weaknesses in the case processing as regards procedural and material requirements in security clearance cases, and found that it gives cause for concern that the OPM was of the opinion that the office had acted in accordance with the law.

The Committee referred to the purpose of the case processing rules in security clearance cases, namely to safeguard the due process protection of the person concerned, and urged the OPM to comply with all provisions in the Security Act and pertaining regulations in its future security clearance cases.

The above-mentioned circumstances emphasise the importance of ensuring that every step of the case processing is documented. It shall be possible to verify the security clearance authority's processing of security clearance cases, particularly with regard to any subsequent appeals to NSM from the person concerned and the EOS Committee's subsequent oversight.

9.6 Follow-up of the inspection of Haakonsvern in 2016

In its annual report for 2016, the Committee wrote that, following an inspection of the Royal Norwegian Navy's main base Haakonsvern, the Committee had urged the base to establish procedures to ensure compliance with the requirements concerning processing of personal data stipulated in the Personal Data Act in connection with the registration of personal data among other things in a list of persons who were to be denied entry to the base. In 2017, Haakonsvern informed the Committee that the base has now revised its procedures and that it has put good procedures in place for processing, storage, access control and revision of the no entry list. The Committee took note of Haakonsvern's account.

¹⁰² The security clearance authority is to prepare internal grounds (ISB) at the same time, inform the person concerned about the decision in writing, and provide written information about the right of appeal, cf. the Security Act Section 25, the Regulations concerning Personnel Security Section 4-4 second paragraph first sentence, and the guide to the Security Act Chapter 6 and the Regulations concerning Personnel Security pages 16 and 38. The requirement for the content of security interviews to be documented in writing follows from the Personnel Regulations Section 4-2.



10.

External relations and administrative matters

10.1 The Committee's external relations

The EOS Committee has had contact with various external environments in 2017, including other Norwegian oversight bodies, research communities and foreign EOS oversight bodies.

It is important to the Committee to communicate openly about its work, and the Committee has given interviews to the media, researchers and organisations on several occasions.

After a successful 20th anniversary conference in 2016, the EOS Committee organised its first annual conference in 2017 in connection with the submission of the annual report to the Storting. The three main topics for the annual conference were: 1. How does oversight of the secret services function in Norway today? 2. 'The surveillance society' – chilling effects and reduced freedom of expression? 3. How will oversight of the secret services deal with technological development? This conference was open to the public, and the Committee plans to make it an annual event.

The annual conferences are held as part of the Committee's work to communicate its findings and make the oversight of the EOS services known to the public.

The EOS services are increasingly cooperating across national borders. The Committee can see advantages of international cooperation in oversight too, among other things in order to share experience at an unclassified level and further develop the oversight. Among other things, the Committee met the Swedish oversight body *Statens inspektion för försvarsunderrättelsesverksamheten* (SIUN), which oversees the Swedish system for collection of information transmitted via cables, in connection with the debate on digital border defence in Norway. The Committee attended a meeting of the Scandinavian countries' oversight bodies where effective oversight was one of the topics.

In November, part of the Committee attended a new cooperation forum organised by the UN Special Rapporteur on the right to privacy, the International Intelligence Oversight Forum. This was the second time the forum was held, and it took place in Brussels. Oversight bodies from large parts of Europe took part, but there were also participants from North America and Oceania. The EOS Committee is in contact with relevant bodies to share experience of oversight of the secret services in different countries, both here and in other forums.

The Committee, represented by the Secretariat, is still engaged in a cooperation project with the oversight bodies of Belgium, the Netherlands, Switzerland and Denmark on democratic oversight of the services' exchange of personal

data about foreign fighters across national borders. Read more about this in Section 5.10.

In 2017, the Committee has hired a communications adviser to work with external communication, strengthen external relations in Norway and abroad and contribute relevant information to the Committee's work.

An overview of the meetings, visits and conferences that the Committee and the Secretariat have taken part in is provided in Appendix 2.

10.2 The EOS Committee in the media

The EOS Committee has been mentioned in many Norwegian media outlets in 2017. The media attention helps to increase knowledge and transparency regarding the oversight of the EOS services.

In May, committee chair Løwer wrote an op-ed article in the newspaper *Aftenposten* about the case concerning the Committee's then inadequate access to PST's source material. The article was followed up by Minister of Justice Per Willy Amundsen and Harald Stanghelle of *Aftenposten*.

Last summer, a case where a lawyer complained to the EOS Committee and the Committee criticised PST attracted some media attention. There were several misunderstandings in the media, and committee chair Løwer specified that the basis for the criticism was that personal data about the lawyer had been processed without basis.

In the autumn, the Committee found reason to give a clarification to the Norwegian Bar Association's periodical *Advokatbladet* after the head of the Bar Association commented on this complaint case in his annual speech. It is a challenge to the Committee that it is legally prevented from providing further information about the basis for criticism in complaint cases.

The special report on 'the Committee's duty of secrecy vis-a-vis the Evaluation Committee and the Evaluation Committee's access to the EOS Committee's information' that the EOS Committee submitted in 2014 was also mentioned in several media outlets. This was a result of the Storting's Standing Committee on Scrutiny and Constitutional Affairs taking action and sending a letter to the Presidium. Løwer was interviewed in *Aftenposten* about the matter.

In an interview with the newspaper VG, the chair referred to the fact that the Committee has requested that the Storting consider whether it should be enshrined in law that the Committee should be entitled to make statements about the public administration's liability in damages.

It was the case concerning FSA's unlawful processing of personal data about several journalists that received the most attention after the annual report for 2016 was published in April 2017.

10.3 Administrative matters

The Committee's expenses amounted to NOK 13,632,788 in 2017, compared with a budget of NOK 15,185,000, including transferred funds. The main reason for the underspending was vacancies and leaves of absence in the Committee Secretariat. The Committee has applied for permission to transfer NOK 750,000 (5%) in unused funds to its budget for 2018. In a letter of June 2017 to the Presidium of the Storting, the Committee requested funding to move to bigger and more secure premises. The request was denied. Another request was submitted in November 2017, and is under consideration by the Presidium. A lot of time has been spent on the planning of new premises in 2017 as well. There is still a need to expand the Secretariat by hiring more staff. The Committee will return to this matter as part of the budget process for 2019.

11.

Appendices

Appendix 1 – Definitions

Authorisation

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

Classified information

Information that shall be protected for security reasons pursuant to the provisions of the Security Act. This information shall be marked with a security classification, for example CONFIDENTIAL.

Covert coercive measures

Investigation methods whose use the suspect is unaware of, for example monitoring of communications, equipment interference, covert audio surveillance and secret searches.

Covert collection

Collection of information for intelligence purposes that is kept secret from the person about whom information is collected.

Digital border defence

A method proposed by the Government for use by the Intelligence Service. It will involve intercepting information and monitoring metadata from telephone and data cables that cross the Norwegian border.

Equipment interference

A method that involves taking control over a mobile phone/computer through a cyberattack. The method, which entails monitoring all activity on the device in question, can be used by PST subject to court approval.

Foreign fighters

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

FSA computer network

A case processing system for the department's operational work outside the area of personnel security.

Information processing

Any form of electronic or manual processing of information – including storage.

Intelligence register

Register of intelligence information that is deemed necessary and relevant for PST in the performance of its duties. PST uses the intelligence register Smart.

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 of or processing in a prevention case.

Internal grounds (ISB)

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 21 of the Security Act, and which facts the decision is based on.

Investigation case

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

Legal person

Any person with rights and obligations. This includes not only people, but also legal persons such as associations, foundations, companies, municipalities, county authorities and the central government.

Metadata

Information about data, such as times, duration, to/from identifiers and type of traffic, that describes a technical event that has taken place in a communication network. Information about a telephone call is one example of metadata.

Mobile-restricted zone

A limited geographic area in which mobile phone or computer communication is monitored or obstructed using legal identity capture and/or jamming.

Monitoring of communications

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.

Non-statutory methods

Methods that are not directly regulated in law, such as observation, use of open written sources and the use of human intelligence sources and contacts.

Observation period

Decision regarding how much time must pass before a person can be reconsidered for security clearance.

Oversight gap

A term that describes the situation that arises e.g. when one of the Norwegian EOS services discloses information about a Norwegian to a cooperating foreign service. The EOS Committee has no way of knowing how the personal data is processed by the foreign service.

Particularly sensitive information

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

- 1) The identity of the human intelligence sources of NIS and its foreign partners
- 2) The identity of foreign partners' specially protected civil servants
- 3) Persons with roles in and operational plans for occupational preparedness
- 4) NIS's and/or foreign partners' particularly sensitive intelligence operations abroad* which, if they were 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 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.

Personal data

Information or assessments that can be linked to an individual.

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.

Prevention case

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

Requesting authority

A body that requests vetting of personnel in connection with a security clearance.

Restriction of access to information

Marking of stored information for the purpose of limiting future processing of the information in question, cf. the Police Register Act Section 2(10).

Review of legality

Process to review compliance with laws and regulations.

Script

A program that is designed to e.g. automatically identify registrations that are due for a manual review, see the five-year rule.

Security clearance

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

Security clearance authority

Public body authorised to decide whether or not people should be granted security clearance.

Security clearance case

Case to determine a person's suitability for security clearance.

Security interview

Interview conducted by the security clearance authority in order to assess a person's suitability in a security clearance case.

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.

Sensitive personal data

The Personal Data Act defines certain data as sensitive: information about a person's racial or ethnic background, political, philosophical or religious views, that a person has been suspected, indicted, charged or convicted of a criminal offence, the person's health, sex life or trade union membership. (This definition will change when a new Personal Data Act comes into force in 2018.)

Smart

PST's intelligence register.

Specification of purpose

Principle stating that personal data can only be processed for a specific purpose defined in advance.

Submission case

Pursuant to the Intelligence Service Instructions, the Intelligence Service must submit 'matters of particular importance or that raise questions of principle' to the Ministry of Defence.

Surplus information

Information that has been obtained by means of e.g. covert coercive measures and is relevant to criminal offences other than that which formed the basis for the use of coercive measures, or information that is not relevant to the criminal offence at all.

The five-year rule

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

The four-month rule

PST can process information for up to four months if it is necessary to do so in order to determine whether the information meets the statutory requirements regarding specification of purpose, necessity and relevance.

Vetting

Obtaining information of relevance to the security clearance assessment.

Working hypothesis

PST's statement of the purpose of processing information, which includes a professional assessment of the specification of purpose, necessity and relevance in relation to PST's tasks.

Appendix 2 – Meetings, visits and participation in conferences etc.

Visit to the Ukraine

Three committee members and one secretariat employee went to the Ukraine in February on the invitation of the Ukrainian parliament (the Rada) and the NATO Representation to Ukraine. The main purpose of the trip was to disseminate knowledge and experience of the Norwegian oversight of the secret services to the Rada, the Ukrainian security service and the president's staff.

Meeting in Stockholm with SIUN

In March, representatives of the Committee and the Secretariat went to Stockholm to visit the Swedish oversight body for the military intelligence services, SIUN, *Statens inspektion för försvarsunderrättelsesverksamheten*. A meeting was also held with the Swedish defence intelligence court, *Försvarsunderrättelsesdomstolen*. The purpose of the visit included familiarising oneself with the oversight system for the Swedish system for collection of information transmitted via cables in connection with the digital border defence debate in Norway.

Talk for the Fritt Ord Foundation and Norwegian PEN

In March, a member of the Committee gave a talk about the EOS Committee's work at a seminar for the boards and important committees of the Fritt Ord Foundation and Norwegian PEN.

The EOS Committee's annual conference

The venue for the Committee's first annual conference was Gamle Logen in Oslo. The three main topics for the annual conference 2017 were: 1. How does oversight of the secret services function in Norway today? 2. 'The surveillance society' – chilling effects and reduced freedom of expression? 3. How will oversight of the secret services deal with technological development?

Visit from the Ukraine

A delegation from the Ukrainian parliament visited the Storting in May. The chair of the Committee gave a talk about how the EOS Committee works and the Norwegian system.

Meetings on cooperation projects with foreign oversight bodies

The Committee, represented by the Secretariat, is cooperating with the oversight bodies of Belgium, the Netherlands, Switzerland and Denmark on a project on democratic oversight of the exchange of personal data about foreign fighters between the respective countries' secret services. In connection with this project, there was one meeting in May in Oslo and one in November in Brussels, which two secretariat employees attended.

Meeting with Swedish researcher

In September, the Committee had a meeting with Professor Iain Cameron of Uppsala University in Sweden. The topic of the meeting was human rights and the activities of the intelligence and security services.

Meeting with German researcher

Project Director Thorsten Wetzling of the German think tank Stiftung Neue Verantwortung met with the Committee in October. One of Wetzling's areas of expertise is research on oversight of intelligence services. During the meeting, he described developments in Germany in the field of intelligence and security and oversight of German services.

Lecture at the Norwegian Defence University College

In October, the chair of the Committee and the head of the Secretariat each gave a lecture on the topic 'Surveillance: more than protection of privacy' as part of the intelligence course at the Norwegian Defence University College. The participants were from the ministries, the intelligence and security services and the Armed Forces.

Nordic meeting in Copenhagen

The Nordic countries with oversight bodies (Denmark, Sweden and Norway) meet every two years. In 2017, the meeting took place in Copenhagen. Nearly the whole Committee and several secretariat employees attended the meeting in Copenhagen.

UN conference in Brussels

Two committee members and one secretariat employee took part in the second International Intelligence Oversight Forum held in November. Oversight bodies, politicians and representatives of the services met to discuss challenges and possibilities for oversight of the services.

Anti-terror conference in Trier, Germany

In November, a secretariat employee took part in an anti-terror conference organized by the EU to learn more about

recent developments in countering terrorism in Europe. Most of the participants represented courts, prosecuting authorities or police forces.

Speech to the Ossietzky Prize winner

Committee chair Løwer gave a speech for Tormod Heier, winner of the 2017 Ossietzky Prize, in November. Norwegian PEN awarded the prize to Lieutenant Colonel Heier for his contribution to a critical public debate on Norway's defence and foreign policy.

Meetings with the Norwegian National Human Rights Institution (NIM)

The Committee and Secretariat have had several meetings with the newly established institution. General information about how the EOS Committee and NIM work have been an important topic. Digital border defence has been another topic of discussion.

Meeting with the Parliamentary Ombudsman's National Preventive Mechanism

In December, the Secretariat met with the unit that works to prevent torture and ill-treatment to learn how the unit works when they visit different institutions in Norway.

Meeting with the Standing Committee on Scrutiny and Constitutional Affairs

The Storting's new Standing Committee on Scrutiny and Constitutional Affairs visited the EOS Committee in December to learn about and discuss different issues and challenges relating to the Committee's work.

In addition to the events mentioned above, the chair of the Committee has given talks on the EOS Committee's work in some more informal contexts.

Appendix 3 – Act relating to oversight of intelligence, surveillance and security services¹⁰³

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.

¹⁰³ Act No 7 of 3 February 1995 relating to the Oversight of Intelligence, Surveillance and Security Services (the Oversight Act).

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 investigated and if the processing has been completed, or when it will be completed.

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

Section 17. Relationship to the Storting

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

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

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

The annual report should include:

1. an overview of the composition of the Committee, its meeting activities and expenses.
2. a statement concerning inspections conducted and their results.
3. an overview of complaints by type and service branch, indicating what the complaints resulted in.
4. a statement concerning cases and matters raised on the Committee's own initiative.
5. a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 14, sixth subsection.
6. a statement concerning any protests pursuant to Section 8 fourth subsection.
7. a statement concerning any cases or matters which should be put before the Storting.
8. the Committee's general experience from the oversight activities and the regulations and any need for changes.

Section 18. Procedure regulations

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

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

Section 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.

Appendix 4 – Consultation statement – processing of surplus information from monitoring of communications etc.

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

18 December 2017

Consultation statement from the EOS Committee – consultation concerning processing of surplus information from monitoring of communications etc.

1. Introduction

The EOS Committee refers to the Ministry of Justice and Public Security's consultation letter of 22 September 2017 regarding consultation concerning processing of surplus information from monitoring of communications etc.

2. Processing of surplus information from coercive measures used for preventive purposes

The EOS Committee notes that the Ministry's consultation letter concerns processing of surplus information from monitoring of communications etc. under the provisions of the Criminal Procedure Act, and that the intention behind the proposal is, among other things, to place the provisions that in reality concern the police's processing of information from monitoring of communications in criminal cases in the appropriate legislation (the Police Register Act).

The conditions for PST's use of coercive measures *for preventive purposes* have their legal basis in the Police Act Section 17d. The Committee would like to comment that, regardless of whether coercive measures are used for preventive purposes or as part of an investigation, the nature of the information and of the coercive measures remains the same, and the methods used entail a corresponding infringement on the right to privacy of the individuals directly or indirectly affected by their use.

In a letter to the Ministry of Justice and Public Security dated 31 August 2017,¹⁰⁴ the EOS Committee requested that the Ministry clarify the legal understanding of the application of the Criminal Procedure Act Section 216g in PST's preventive activities/prevention cases. As far as the Committee can see, the processing of surplus information from coercive measures *for preventive purposes* appears not to be mentioned in the Ministry's proposal to transfer parts of Section 216g to the police register legislation.

The Committee is therefore of the opinion that the rules for processing surplus information from coercive measures used for preventive purposes should be clarified in connection with the Ministry's work to transfer the provisions on such processing from the Criminal Procedure Act to the police register legislation.

3. Surplus information from equipment interference

Among other things, the Ministry points out that '[w]hether further restrictions should be imposed on the use of surplus information should, as shown in 7.1, be considered as part of the work on a new criminal procedure act'. The EOS Committee would like to comment that in such case, such restrictions should also be considered for the use of equipment interference as a method *for preventive purposes*, cf. the Police Act Section 17d and the Criminal Procedure Act Section 216o.

4. Restriction of access to information

As regards restriction of access to information, the EOS Committee refers to the fact that it has remarked on several occasions that no satisfactory solution has been implemented for restricting access to information that shall no longer be available for intelligence purposes or operational activities in PST, most recently in section 4.5, page 18 of the Committee's annual report for 2015.

Yours sincerely,



Eldbjørg Løwer
Chair of the EOS Committee



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



©Photo: KienVictor / Shutterstock.com

fdesign.no

Contact information

Telephone: +47 23 31 09 30

Email: post@eos-utvalget.no

Postal address: PO box 84 Sentrum, N-0101 Oslo, Norway

Office address: Akersgata 8, Oslo

www.eos-utvalget.no