EOS COMMITTEE

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

2014 ANNUAL REPORT

To the Norwegian Storting

Pursuant to section 8 (2) of Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services (the Oversight Act), the Committee hereby submits a report to the Storting of its activities in 2014.

Pursuant to section 8 (2) of the Oversight Act, the annual report is unclassified. According to the Security Act, the party that issues information shall determine whether the information is classified. Before the report is submitted to the Storting, the Committee shall send the respective parts of the text to the services in order for them to ascertain whether the report meets this requirement. The services will also have an opportunity to check that there are no errors or misunderstandings in the descriptions of the facts.

Oslo, 8 April 2015

Eldbjørg Løwer
Eldbjørg Løwer

Svein Grønnern
Svein Grønnern

Trygve Harvold
Trygve Harvold

Theo Koritzinsky
Theo Koritzinsky

Øyvind Vaksdal
Øyvind Vaksdal

Håkon Haugli
Håkon Haugli

Inger Marie Sunde
Inger Marie Sunde

Henrik Magnusson
Henrik Magnusson

Contents

1.	**The EOS committee's activities in 2014**	**6**
1.1	The Committee's remit and composition	7
1.2	Oversight activities	8
1.3	Matters that should be investigated by the Storting – case processing time for security clearance cases	8
1.4	Cases opened as a result of critical mention in the public discourse	9
1.4.1	Introduction	9
1.4.2	Assertion of illegal surveillance of Harald Stabell	9
1.4.3	Terror alert in the summer of 2014	9
1.4.4	Allegations of fake base stations	9
1.5	External evaluation of the EOS Committee – exemptions from the duty of secrecy	10
1.6	External relations of the Committee	11
1.7	Administrative issues	11
2.	**Developments and challenges in 2014**	**12**
3.	**The Norwegian Police Security Service (PST)**	**14**
3.1	General information about the oversight	15
3.2	The committee's six-month inspections at PST	15
3.3	Oversight of archives and registers	15
3.3.1	Oversight of PST's processing of information in the Smart intelligence register	15
3.3.2	Tips and log cases	16
3.3.3	Processing of intelligence data in Doculive and Smart	16
3.4	Processing of information outside archives and registers	17
3.5	Foreign intelligence activities in Norway	18
3.6	Individual case of the spreading of undermining information	19
3.7	PST's processing of applications for declassification and access	19
3.8	PST's requests to telecommunications providers for communications control – classification and security clearance	20
3.9	Information exchange with cooperating foreign services	20
3.9.1	Conditions for surrender and documentation	20
3.9.2	Norwegians registered on a list drawn up by the Counter Terrorism Group (CTG)	21
3.9.3	Norwegians registered in the Terrorist Screening Center (TSC) database	21
3.10	Information exchange with national agencies	22
3.10.1	Collaboration between PST and the customs authorities	22
3.10.2	Information exchange with the National Criminal Investigation service (Kripos) in the Schengen Information System (SIS)	24
3.10.3	PST's retrieval of passenger information from airlines	25
3.11	Notification upon establishment of mobile-restricted zones	26
3.12	The committee's investigation of allegations of political surveillance and PST's use of Christian Høibø as a source	26
3.13	Complaint cases considered by the Committee	27

4. The National Security Authority (NSM) 28

4.1 General information about the oversight 29

4.2 Case processing time for security clearance cases 29

4.3 Security clearance case regarding failure to disclose health details 29

4.4 Consequences of withdrawing a complaint during the appeals process 30

4.5 Case regarding procurement of information about persons for whom vetting is not required 31

4.6 Security interviews 31

4.7 Access to information in security clearance cases 32

4.8 Complaint cases considered by the Committee 32

5. The Norwegian Defence Security Agency (FSA) 35

5.1 General information about the oversight 36

5.2 Case processing time for security clearance cases 36

5.3 Questions regarding two security clearance cases that had been dropped 36

5.4 Complaint cases considered by the Committee 36

6. The Norwegian Intelligence Service (NIS) 38

6.1 General information about the oversight 39

6.2 The Committee's inspection of NIS 39

6.3 Follow-up of the Committee's investigation of information about Norwegian sources, etc. at NIS 40

6.4 NIS' procedures for deletion of operational information 41

6.5 Violation of the prohibition in section 4 of the Intelligence Service Act 41

6.6 Inspection of NIS' archives and registers in connection with complaints 42

6.7 Complaint cases considered by the Committee 42

7. Oversight of other EOS services 43

7.1 General information about the oversight 44

7.2 The Committee's access to FISBasis 44

7.3 Follow-up of the inspection of the personnel security service at the Ministry of Justice and Public Security 45

7.4 Spot checks at the Post and Telecommunications Authority 45

8. Proposed amendments to the oversight act and the oversight directive 46

9. Appendices 48

Appendix 1 – Glossary 48

Appendix 2 – Meetings, visits and conferences, etc. 49

Appendix 3 – Personnel 50

Appendix 4 – Act relating to the Oversight of Intelligence, Surveillance and Security Services 50

Appendix 5 – Directive relating to oversight of the intelligence, surveillance and security services (EOS) 52

1.
The EOS Committee's activities in 2014

1.1 The Committee's remit and composition

The EOS Committee is a permanent oversight body with the responsibility of overseeing services that monitor intelligence, surveillance and security (EOS services). The Committee's mandate follows from the Oversight Act and the Oversight Directive.[1] The Committee's oversight only applies to EOS services carried out by, under the control of or on behalf of the public authorities, and which are of relevance to issues regarding national security.[2]

Pursuant to section 2 subsection 1 of the Oversight Act, the purpose of the monitoring is to:

1. clarify if and prevent the exercise of injustice against any party, including ensuring that the measures are not more invasive than necessary, depending on the situation, and that the services respect human rights,
2. ensure that the activities do no unwarranted damage to society, and
3. ensure that the activities remain within the frames of the law, administrative or military directives and unlegislated rights.

In its oversight, the Committee must show consideration for national security and relations with foreign powers.[3] The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes, and shall as far as possible observe the concern for protection of sources and safeguarding of information received from abroad.[4] Individual cases and operations shall be monitored after the fact, and the oversight shall cause as little inconvenience as possible to the services' day-to-day activities.[5]

The Committee has seven members. The members 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. The members may be re-appointed.

The Committee is an independent body. Members of the Storting therefore cannot also be members of the Committee. The composition of the Committee is diverse, and both political backgrounds and experience from other areas of society are represented. The Committee members and secretariat employees must have top level security clearance and authorization, both nationally and pursuant to treaties to which Norway is a signatory.[7]

Below is a list of the members of the Committee and their periods of duty:

Eldbjørg Løwer, Kongsberg, chair
1 July 2011 – 30 June 2019
Svein Grønnern, Oslo, deputy chair
13 June 1996 – 30 June 2016
Trygve Harvold, Oslo
7 November 2003 – 30 June 2016
Theo Koritzinsky, Oslo
24 May 2007 – 30 June 2019
Wenche Elizabeth Arntzen, Oslo
1 July 2009 – 30 June 2014
Håkon Haugli, Oslo
1 January 2014 – 30 June 2016
Øyvind Vaksdal, Karmøy
1 January 2014 – 30 June 2016
Inger Marie Sunde, Bærum
1 July 2014 – 30 June 2019

Five of the current seven members come from different political parties. This strengthens the legitimacy of the Committee. The office of Committee member now fills close to 20 per cent of a full-time position. The Committee chair works about 30 per cent of a full-time position.

A ten-person secretariat serves the Committee. The secretariat received three new positions in 2014: a social scientist, a technologist and a lawyer. At the end of 2014, the secretariat consisted of the head, who is a lawyer, five other lawyers, one social scientist, and two administrative employees.

1 Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services (the Oversight Act) and the Directive relating to Oversight of the Intelligence, Surveillance and Security Services (the Oversight Directive), adopted through a resolution of the Storting on 30 May 1995. The Act and the Directive were last amended in July 2013.

2 Provisions that make reference to section 30 of Act No. 10 of 20 Mar ch 1998 relating to Protective Security Services (the Security Act), section 6 of Act No. 11 of 20 March 1998 relating to the Norwegian Intelligence Service (the Intelligence Service Act), section 14 of Directive No. 695 of 29 April 2010 regarding the Defence Security Service, and Act No. 16 of 28 May 2010 regarding Processing of Information by the Police and Prosecuting Authorities (the Police Register Act).

3 See section 2 subsection 2 of the Oversight Act.

4 See section 5 subsection 1 of the Oversight Directive. Section 6 of the Oversight Directive states that the Committee can make a binding decision regarding the right of access and the scope 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 to disputes about access to NIS documents.

5 See sections 4 and 7 of the Oversight Directive.

6 See section 1 subsection 1 of the Oversight Directive.

7 See section 1 subsection 1 of the Oversight Directive. This means clearance and authorization for TOP SECRET and COSMIC TOP SECRET.

1.2 Oversight activities

The Committee's oversight activities mainly take the form of the Committee conducting announced inspections of the EOS services. The Oversight Directive stipulates requirements regarding the Committee's annual inspections.[8] The Committee met these requirements in 2014. The Committee has conducted 25 inspections. The Norwegian Police Security Service (PST) has been inspected 10 times, the Norwegian Intelligence Service (NIS) 5 times, the National Security Authority (NSM) 4 times, and the Norwegian Defence Security Agency (FSA) 3 times. The Intelligence Battalion, the personnel security service at the Ministry of Justice and Public Security, and the personnel security service at the Norwegian Defence Estates Agency have each been inspected once. In 2014, the Committee did not find cause to conduct unannounced inspections.

The Committee splits its inspections into a control section and an information section. During the control section, the Committee reviews the material presented on paper or on screen. The secretariat prepares for inspections at meetings lasting one to two days, where it reviews cases, registrations and other operational information from the services. During the information section, the Committee receives briefings on the service's current activities and about special topics and cases that the Committee has requested information about in advance.

The Committee opened 39 cases on its own initiative in 2014, against 26 cases in 2013; these mainly consist of follow-up of findings from the Committee's inspections.

The Committee investigates complaints from individuals and organizations.[9] The Committee received 26 complaints regarding the EOS services in 2014, compared with 47 in 2013. Even though the number of complaints has declined, the Committee spent vastly more resources on investigating complaints than in previous years. This is particularly due to the complexity and scope of the complaints. Some of the complaints were against more than one of the EOS services at the same time. The Committee rejected four complaints on formal grounds, partly with reference to the matter falling outside its oversight area. Complaints and enquiries within the oversight area of the Committee are investigated in the services addressed by the complaint. If the Committee finds grounds to do so, it will investigate complaints in more services than those identified in the complaint. The Committee generally has a low threshold for processing complaints.[10]

The Committee had 21 internal meetings in 2014.

The intelligence, surveillance and security services have generally demonstrated an understanding of the Committee's oversight in 2014. Experience shows that the oversight helps to safeguard individuals' due process protection and to create trust that the services operate within their statutory framework.

PST's headquarters in Nydalen, Oslo.

1.3 Matters that should be investigated by the Storting – case processing time for security clearance cases

The Committee pointed out in its annual reports for 2011, 2012 and 2013 that the case processing times in security clearance cases are often far too long. In the 2013 annual report, the Committee stated that the situation gave cause for concern.

The situation deteriorated in 2014. In addition to criticizing NSM and FSA of long case processing times in five complaints, the Committee's inspections showed that security clearance cases are not investigated within an acceptable period of time. For example, the Committee has investigated cases where the first instance spent over two years determining whether its own negative decision should be reversed or sent to the appellate body. The deterioration of the situation during the year particularly appears to be related to the introduction of a new case processing system for security clearance cases (Mimir), and a lack of personnel resources.

Pursuant to the Oversight Act, the EOS Committee cannot issue instructions or sanctions, and notes that constant mentions in the Committee's annual reports have not led to improvement.

The long case processing times create great uncertainty for both employees and employers, and may result in financial losses on both sides, a loss of efficiency on the part of the

employer, and career-related difficulties for the employee. In many cases, the case processing time is now so long that it entails a disproportionate intervention in the life of the individual by the authorities.

The Committee was informed about the situation regularly in 2014 during inspections of NSM and FSA. The reasons for the long case processing times and the measures implemented by these authorities are described in further detail in points 4.2 and 5.2.

Pursuant to section 13 (3-g) of the Oversight Directive, the Committee requests that the Storting investigate the matter and consider acting quickly to remedy the situation.

1.4 Cases opened as a result of critical mention in the public discourse

1.4.1 Introduction

It follows from section 3 subsection 2 of the Oversight Act that on own initiative the Committee shall investigate all matters it deems correct to review, especially those that have been subject to public criticism. The Committee has accordingly investigated certain cases that have been subject to critical mention in the public discourse.

1.4.2 Assertion of illegal surveillance of Harald Stabell

An article in national newspaper Aftenposten in March 2014 stated that attorney Harald Stabell suspected that his law offices had been wiretapped in 2010 and 2011. During this period, Stabell worked for convicted spy Arne Treholt, with a request to reopen the criminal case against Treholt. The Committee decided to investigate the case on its own initiative, based on the serious allegations of illegal surveillance of Stabell's office.

As part of the investigation, the Committee had a conversation with Harald Stabell, who did not want to give the name of the source of his information regarding the alleged surveillance. Stabell stated that he did not suspect PST of this. The Committee nevertheless examined PST's archives and registers, and asked PST's management for information. PST stated that the service had no knowledge of the allegations other than that presented in the media.

During its investigations, the Committee did not find any trace of illegal surveillance of Harald Stabell's law offices by PST.

1.4.3 Terror alert in the summer of 2014

At the end of July 2014, PST announced that the service had received information from cooperating foreign services that a group of persons were on their way from Syria to Europe with the intention of conducting an act of terrorism in Norway. The Norwegian authorities considered it necessary to take a number of preventive security measures based on the terror alert.

The Committee has received thorough, detailed information about how PST, NIS and NSM worked with the terrorist threat, particularly regarding the cooperation and exchange of information between PST and NIS. The Committee has also been notified of suspicion of leaks of classified information regarding the matter. The Committee has further inspected PST and NIS' archives and registers in order to check whether the services' information retrieval and methods have complied with the current legal framework. This was the Committee's only task in this matter, in the light of the oversight purposes stipulated in the Oversight Act.

The investigations at PST have not resulted in a need for further follow-up by the Committee. Nor the investigations at NIS have resulted in a need for specific follow-up. However, the case highlighted certain general issues regarding due process related to the foundation in the Intelligence Service Act for the methods used by the intelligence services, which the Committee began to work on before the summer of 2014.[11]

The Committee is still working on these issues.

1.4.4 Allegations of fake base stations

On 12 December 2014, Aftenposten published an article that alleged the existence of fake mobile base stations to monitor mobile communications in central parts of Oslo, including the area around the Storting.

Pursuant to section 2 of the Oversight Act, the EOS Committee shall «clarify if and prevent the exercise of injustice against any party». It is accordingly the job of the Committee to investigate whether the services have used illegal methods. The EOS Committee has thus requested and received information from PST, NIS and NSM of a legal, factual and technical nature.

The Committee will continue to monitor the legality of PST's own use of fake mobile base stations.[12]

8 Section 11 (2) of the Oversight Directive requires a minimum of 23 inspections per year.

9 See section 3 subsection 2 of the Oversight Act.

10 See the remarks to section 8 of the Oversight Directive on page 64 of NOU 1994:4.

11 See point 6.1.

12 See section 216b of the General Civil Penal Code.

1.5 External evaluation of the EOS Committee – exemptions from the duty of secrecy

On 12 December 2014, the Committee submitted a special report to the Storting regarding the EOS Committee's duty of secrecy towards the EOS evaluation committee and its access to the EOS Committee's information.[13] The background for the report was as follows:

As explained in the 2013 annual report, that year the EOS Committee proposed an external, forward-looking evaluation of its activities. On 27 March 2014, the Storting's Presidium appointed a committee led by Chief Judge Bjørn Solbakken to evaluate the activities and framework conditions of the EOS Committee. In the view of the EOS Committee, the remit requires that the evaluation committee has access to information that is subject to a statutory duty of secrecy. Section 9 subsection 1 of the Oversight Act states the following regarding the EOS Committee's duty of secrecy:

«With the exception of matters provided for in section 8, the Committee and its secretariat are bound to observe a duty of secrecy unless otherwise decided.»

On 2 September 2014, the EOS Committee received a letter from the Storting's Presidium which presented the Presidium's decision of 26 August 2014:

> «The Presidium releases the EOS Committee and its secretariat from the duty of secrecy pursuant to section 9 subsection 1 of the Oversight Act in relation to the EOS evaluation committee within the remit of the Committee.
>
> The Presidium finds that the evaluation report can be made publicly available.»

The EOS Committee could not see that the passage «unless otherwise decided» in section 9 of the Oversight Act could be understood as delegation to the Presidium. The Committee accordingly sent the following letter to the Storting's Presidium on 11 September 2014:

> «The EOS Committee makes reference to the Presidium's letter to us of 2 September 2014, where the Presidium states that in a decision dated 26 August 2014 it released the Committee and the secretariat from its duty of secrecy towards the evaluation committee pursuant to section 9 subsection 2 of the Oversight Act.
>
> Both the EOS Committee and the evaluation committee believe that release from the duty of secrecy is necessary in order for the evaluation committee to be able to fulfil its remit.
>
> The provisions regarding right of inspection, security clearance and duty of secrecy, etc. in the Oversight Act and Oversight Directive have been factors in the 20-year building of trust between the Committee and the EOS services. This means that the Committee has generally received all of the information it has requested, regardless of the level of sensitivity. As the evaluation committee at present requires access to part of this information, it is the view of the EOS Committee that the formal grounds for this must be clarified as much as possible. This is important both in terms of the Committee's continued oversight of the services and in order to ensure that the evaluation is as real and thorough as possible.
>
> The Committee believes that the exemption from the duty of secrecy must be laid down pursuant to a (temporary) Act. The duty of secrecy is stipulated through formal law, and it follows from basic legal principles that a statutory

Photo: Torgeir Haugaard / Forsvaret

provision can only be set aside by a rule with the same status. The Committee does not find that the passage «unless otherwise decided» in section 9 of the Oversight Act changes this.

The Committee requests that the Presidium take the initiative to introduce a bill as mentioned above. Out of consideration for the work of the evaluation committee, this must be done as soon as possible, and preferably by 9 October 2014, the date of the next meeting between the evaluation committee and the EOS Committee.»

In a letter to the Committee dated 8 October 2014, the Presidium reported that it still believed that legal authority was not required to exempt the EOS Committee from its statutory duty of secrecy. The EOS Committee then tried to explain to the Storting's administration, represented by the director, the considerations that formed the Committee's position, which were expressed in the EOS Committee's letter of 11 September 2014. When such an approach did not succeed, the EOS Committee believed that it found itself in a situation that required formal clarification from the Storting. The special report provided further information about the EOS Committee's duty of secrecy, and its processing of information which the Committee believes necessitates a statutory foundation for the exemption from the duty of secrecy.

On 15 January 2015, the Storting's Presidium submitted a recommendation for an Act regarding a committee to evaluate the EOS Committee.[14] In the recommendation, the Presidium stated that «it has turned out to be desirable to clarify that the duty of secrecy is not an obstacle to the evaluation committee being able to procure relevant information from the EOS Committee», without reference to the EOS Committee's correspondence with the Presidium, and the Committee's special report on the matter. Based on the recommendation, Act No. 10 of 13 February 2015 regarding a committee to evaluate the EOS Committee was passed by the Storting, and the EOS Committee was released of its duty of secrecy towards the evaluation committee.

The Committee's special report was unanimously enclosed with the records by the Storting on 3 February 2015.

In 2014, the EOS Committee expended considerable resources to prepare for the evaluation, and will continue to do so in 2015.

1.6 External relations of the Committee

It is important to the Committee and its secretariat that it has contact with relevant external environments. The external contact is with the supervisory authorities of other countries, domestic and international research environments, other national supervisory agencies, and the media and society in general. When possible, the Committee wants to inform society about its work.

The Committee must ensure that it is updated on trends like changes to the threat picture, technological developments, and the services' response to these changes. In this context, it is natural and useful to note how other comparable countries carry out and improve their oversight of the secret services.

In 2014, the Committee members and the secretariat participated in a number of events, like debates, seminars and conferences. The Committee and the secretariat also hosted several visits from abroad. A list of such visits can be found in Appendix 2 of this report.

The Committee wants to continue developing its contact with relevant national and international external communities. Specific measures include closer cooperation with research institution the Geneva Centre for the Democratic Control of Armed Forces (DCAF), further development of the contact with supervisory authorities in other European countries, and greater contact with national research environments, actors in society and media interested in the EOS services and their democratic oversight.

1.7 Administrative issues

The Committee's 2014 expenses were NOK 11,805,854 against the budget, including NOK 12,312,000 in transferred funds. The unused allocation will be transferred to the 2015 budget. The spending shortfall is mainly due to it taking more time to fill the three new positions than expected.

A list of the secretariat's personnel as at 31 December 2014 is enclosed as Appendix 3.

In 2014, the Committee revitalized its website (www.eos-utvalget.no) and logo.

13 Document 7:2 (2014–2015).

14 Recommendation to the Storting 134 L (2014–2015).

2.
Developments and challenges in 2014

In their open threat assessments, PST and NIS identified a negative trend. The services found that they face a more complex threat situation. Priority has been given to preventing people with ties to Norway from being involved in acts of terrorism. The services also point to greater pressure on intelligence in Norway.

The Snowden disclosures shone a light on digital monitoring and showed that technological systems are becoming increasingly advanced, making it easier to retrieve and analyze information. These systems offer the services new ways of performing their tasks. At the same time, the developments place great demands on how the services handle the information, and may influence subsequent inspection opportunities. Greater international mobility raises several questions regarding affiliation, nationality and whereabouts. While the division of the services and their areas of responsibility requires a distinction between Norway and abroad, this is difficult in process. Both the tasks of the services and the oversight of the EOS Committee are affected by these trends.

A clear distribution of roles and responsibilities between the EOS services is important in order for the services to be able to keep their activities within the frames of their own framework, and for the cooperation between the services to take place within the legal frameworks of each service. It is important for the Committee's oversight activities that the rules governing the EOS services always reflect the current distribution of roles and responsibilities, which may precisely be challenged by social and technological developments.

The Committee performs oversight in order to ensure that injustice is not exercised against individuals. The Committee faces several dilemmas as a result of a democratic society also having a legitimate need for secret services. It is difficult to balance the individual's right to privacy against society's need for protection. Also expanded discretionary powers for the secret services can complicate for oversight activities.

In connection with the new provision regarding the right to privacy in Article 102 of the Norwegian Constitution, the Standing Committee on Scrutiny and Constitutional Affairs stated that technological development is a benefit, but requires more from us in order to protect privacy.[15] Article 102 of the Constitution expressly protects the right to private «communication». The right to privacy can only be interfered with when there is legal authority for this – see Article 113 of the Constitution.

National, international and technological trends raise a number of questions regarding the methods of the EOS services. The EOS Committee checks legality based on current legislation. Expanded methods and legal authority for the EOS services must be accompanied by reinforced mechanisms for democratic oversight. The following considerations are key here:

- **A clear material and procedural legal authority.**
  The annual report includes examples of certain unclear points and dilemmas identified by the Committee. The Committee's oversight requires that the legal authority for intervention is adequately clear in order to determine whether the services carry out their activities in accordance with the intentions of the Storting. Reference is accordingly made to point 3.10.1.

- **Facilitation obligation for the services.**
  Section 4 subsection 2 of the Oversight Act imposes an obligation on the services to provide all of the material, equipment, etc. required to carry out the oversight. New systems and methods for collection of information have an impact on the type of oversight that may be carried out. The Committee is of the opinion that the facilitation obligation must be understood to mean that the services are under an obligation to provide information about new forms of activity within the Committee's oversight area, and actively facilitate oversight within the area. Reference is accordingly made to point 4.7.

The Committee is familiar with the trends that influence oversight, and is monitoring the situation closely. The secretariat has been given extra resources in the form of social science and technical competence.

15 See Recommendation to the Storting 186 S (2013–2014) point 2.1.9.

3.
The Norwegian Police Security Service (PST)

Photo: Daniel Nordby/Hæren/Forsvaret

3.1 General information about the oversight

In 2014, the Committee conducted six inspections of the PST Headquarters (DSE). The Committee inspected the PST units in the police districts of Gudbrandsdal, Romerike, Nord-Trøndelag and Follo.

During the inspections of the service, the Committee particularly investigated the following points:

- The service's archives and registers.
- The service's new and closed preventive cases and cases under investigation, and two half-year inspections of all open preventive cases and cases under investigation.
- The service's use of covert coercive measures.
- The service's exchange of information with domestic and foreign partners.

During the inspections, the Committee was regularly informed about PST's current activities, including the service's new preventive cases and cases under investigation, PST's threat assessments, and the service's collaboration with other EOS services, especially NIS.

3.2 The committee's six-month inspections at PST

Following the requirements in the Oversight Directive[16], the Committee conducts six-month inspections of all ongoing cases at PST. Considering the large number of cases at the service, it is not possible for the Committee to thoroughly review all of the cases twice a year. During the four remaining inspections at DSE, the Committee regularly inspects new and closed cases, and cases that involved use of covert coercive measures. On the whole, they make up a relatively large share of PST's cases.

The issue, including the extent to which six-month inspections as a required oversight method are expedient, has been part of the Committee's discussions with the evaluation committee.

3.3 Oversight of archives and registers

3.3.1 Oversight of PST's processing of information in the Smart intelligence register

The Committee's oversight of the processing of personal data in PST's registers resulted in a large number of people being deleted from Smart also in 2014. We will discuss the issues brought up with PST by the Committee, as a result of the inspection of Smart.

Lack of object registration and working hypotheses

The Committee has had remarks regarding several cases where PST has processed personal data in Smart without establishing the persons as separate objects in the intelligence register. By not registering them as objects, it is not possible to deduce whether an individual assessment was made regarding the meeting of the conditions for processing. Neglecting to establish objects in the intelligence register also means that the processing cannot be re-evaluated regularly, and that the information may be stored for longer than necessary, considering the purpose of the processing.[17] On several occasions the Committee has also remarked on non-existent or defective working hypotheses upon initial registration.[18] In cases where PST argues that processing continues to be necessary and relevant to PST's performance of duties, the Committee has asked PST to draw up working hypotheses that show the source of PST's concern, and the basis on which the persons were actually registered.

Based on a free text search in Smart of the expression «not found in Smart», the Committee found that this term was used as a dedicated category for persons who were not established as objects. The explanation given for the registration was that the service's system for communications control «has been set up to search the 1890 directory inquiries service, so that information is provided about the owner of the telephone number that is called / calls the person subject to communications control». The Committee stated that is was concerned about the large number of people whose personal data appeared to have been processed in Smart in this category. PST has made changes to the technical solution that automatically transferred the subscriber data from the communications control into Smart. The Committee is satisfied with the rapid response from the service that the subscriber data on the present and former owners of phone numbers that call / receive a call from a person under communications control from now on will only be entered into Smart when the information is deemed to be relevant and necessary for PST to perform its duties.

The Committee considers it positive that PST has found a technical solution that adequately protects privacy.

Lack of grounds for processing «informants/tipsters»

In 2014, the Committee brought up several cases where PST processed data on persons characterized as «informants/ tipsters» without these persons having been in direct contact

16 See section 11 (2-c) of the Oversight Directive.

17 See section 22-3 subsection 3 of the Police Register Regulations.

18 See section 21-4 of the Police Register Regulations.

with PST. The service had previously stated that PST must have had contact with a person for them to be registered as a «source/contact». The Committee has remarked that the conditions in section 3-2 of the guidelines of the time regarding whose information PST[19] may process. In the view of the Committee, the grounds for processing do not include information about informants/tipsters who the service itself has not had a direct dialogue with.

Unclear grounds for processing information from cases in which PST provided assistance

The Committee queried an intelligence registration established as a result of a case where PST was asked to help the ordinary police. The Committee noted that the grounds for processing information associated with the case in which it provided assistance were unclear. PST agreed with this assessment. The service will contact the Ministry of Justice and Public Security to discuss the ambiguity in the rules regarding processing of information associated with cases in which it provides assistance.

Lack of re-evaluations

It follows from section 22-3 subsection 3 of the Police Register Regulations that intelligence registrations to which no new information has been added after five years shall be reviewed and deleted if they are no longer required for the purpose of the processing. In 2014, the Committee found several examples of objects not being re-evaluated in accordance with the five-year rule. This resulted in information being processed for longer than necessary in terms of the purpose of the processing.

In the 2013 annual report, the Committee pointed out that an error in the script for re-evaluation of intelligence registrations had led to persons not being re-evaluated according to the five-year rule. These were people who were also subject to vetting in connection with security clearance, and people who were linked to entries in the so-called meeting and documentation log.[20] In 2014, PST stated that it had designed a technical solution that handled the re-evaluation requirement.

In the 2012 annual report, the Committee criticized PST of having granted certain categories of persons an exemption to from reassessment after five years. When the service was questioned in 2014 about whether the lack of re-evaluation of information about a person was due to the practice that had been criticized, PST responded that the changes to the practice of exempting certain categories from re-evaluation would nevertheless not be implemented in full, as a result of an assessment by the service. The Committee was astounded by this. The Committee noted that PST continues to practice an exception from the five-year rule, in contravention of section 22-3 subsection 3 of the Police Register Act. The Committee stated that it considers it likely that there will occasionally be erroneous registration of the category of persons in question as well. The Committee also stated that PST's practice allows (erroneously) registered objects to remain in the service's registers, even though it turns out that the conditions for processing are not present (anymore). The Committee disagreed with the service's arguments in favour of practising such an exemption. The Committee could not see good arguments in favour of PST receiving a better overview of the persons by not re-evaluating them five years after their last registration in Smart than it would receive by re-evaluating the persons regularly.

In the 2012 annual report, the Committee stated that it was unfortunate if the roles «contact» or «source» prevented re-evaluation according to the five-year rule, considering the fact that negative information may be registered about these persons in Smart. The Committee concluded that PST should also re-evaluate sources and contacts in accordance with the five-year rule, as long as the rules do not provide an exception for any groups of persons. In 2013, the Committee criticized PST for having registered a person as a «positive contact» when there was negative information about that person.[21] In 2014, the Committee became aware that positive contacts at PST are still not re-evaluated after five years. With reference to the case mentioned in the 2012 annual report, the Committee therefore stated that it expected also contacts, including «positive contacts» to be re-evaluated according to the five-year rule.

The Committee noted that it expects to be informed when the service does not follow up matters which have been criticized by the Committee, and which have been reported to the Storting in the annual report.

3.3.2 Tips and log cases

In general, the Committee has noted that PST's «tips or log cases» do not appear to clearly fall under the definitions of cases under investigation or preventive cases at PST. In the view of the Committee, using cases that are not directed towards concrete main objects, where information about persons is included as a result of more or less concrete 'tips' challenges the consideration of the individual's privacy and the requirements regarding processing of personal data. When PST was asked whether it was correct to use such tips and log cases, the service responded that it has now stopped the practice of processing tips exclusively in connection with cases. In the future, tips will be processed in Smart, which is the best tool for them. PST has stated that the service will review old cases used to process tips. It has informed the Committee that these processes are time-consuming, and that it is not very likely that such work will be completed before the end of the first half of 2015.

3.3.3 Processing of intelligence data in DocuLive and Smart

In the 2010 and 2012 annual reports, the Committee discussed PST's processing of intelligence data in the DocuLive archive and records system.[22] The Committee has again found it necessary to discuss the processing of personal

data in DocuLive with PST. Like in 2012, this was a matter of processing of personal data in minutes from PST meetings, written after its meetings with contacts.

The Committee has stated that the practice of processing personal data in minutes in DocuLive is fairly problematic in terms of the requirements in the Police Register Act regarding processing of information. This applies to information procured by PST for intelligence purposes through the service's meetings with contacts.

The Committee's view is that all personal data procured and processed by PST for intelligence purposes should as far as possible be processed in the same way.

At meetings with the service's contacts, PST's officers need to determine there and then whether the personal data provided in conversations is necessary and relevant to the purpose of its processing, in relation to the duties performed by PST. The Committee has nevertheless asked whether the necessity and relevance of a piece of information can be assessed adequately when writing down a record of a conversation, and before the service places the information in a larger context / PST's intelligence picture. The Committee cannot see that considerations of storage and documentation call for such information to be recorded in minutes when this would lead to the information being subjected to a different, less due process-oriented processing regime than for corresponding information in Smart, where the requirements of the Police Register Act have been met.

In the view of the Committee, all personal data procured by the service through meetings with its contacts, and which is considered relevant and necessary on the date of recording, should be entered directly into Smart. This is to ensure that as far as possible personal data is subjected to the processing regime in the Police Register Act for personal and intelligence data.

The Committee has noted that registration of persons in Smart will be checked and approved by a superior, precisely in order to check that the conditions for processing have been met. Among other things, PST will establish a working hypothesis when a person is registered for the first time, the person registered will be assigned a role, and the information will be reviewed after five years; sometimes already after four months. The information must be deleted if it is not found to meet the processing requirements in the police register legislation. When entering personal data in meeting records in DocuLive, there will be no corresponding quality control, approval or review.

The Committee has made reference to the processing of information according to the four-month rule, see sections 65 and 8 of the Police Register Act, when the requirements regarding necessity, relevance and use for explicit purposes may be unclear on the processing date. This illustrates why it may be difficult to process personal data in minutes in DocuLive. The Committee finds it difficult to see that processing of corresponding personal data in minutes in DocuLive which does not turn out to be necessary or relevant information for PST is consistent with the provisions of the Police Register Act or the requirements in the Archive Act (regarding archive restriction).

The fact that PST at present does not have a regime for blocking data that is not necessary (anymore) or relevant for the service also makes the current practice of processing of personal data in minutes in DocuLive problematic.

The Committee has noted that PST has contacted the Ministry of Justice and Public Security again in order to clarify the relationship between the duty in the Archive Act to store information and the rules regarding deletion in the Police Register Act. The Committee looks forward to clarification from the Ministry.

3.4 Processing of information outside archives and registers

In the 2012 and 2013 annual reports, the Committee criticized PST for having processed intelligence and personal data outside established archives and registers.[23] The information had been processed in the so-called I, F and H directories in the directory structure of PST's computer network.[24] In practice this led to information being withheld from the oversight of the Committee, and a large volume of informa-

19 Guidelines for PST's processing of information, established on 19 August 2005. The guidelines were repealed by the entry into force of the Police Register Act and Regulations.

20 The meeting and documentation log is an administrative tool for documenting operational activities. The log must not contain intelligence data.

21 The Committee's special report to the Storting of 23 April 2013. When inspecting PST's registration of persons affiliated with two Muslim groups, the Committee criticized the service for assigning a person the role of «positive contact» in Smart, even though the person had hundreds of negative intelligence incidents linked to him in the intelligence register. The Committee stated that the service hardly had grounds to categorize the person as a «positive contact» for the service, due to large volume of negative data registered about the person.

22 See chapter III section 3.5 of the 2010 annual report, and chapter IV section 6 of the 2012 annual report.

23 See chapter IV section 3 of the 2012 and 2013 annual reports.

24 The I and F directories are two network drives connected to PST's network. Windows Explorer makes it possible to view the drives' directory structure, including all of the files processed there. The H directory is each officer's 'personal' directory on the computer network.

tion being processed in contravention of the rules requiring necessity and relevance, in addition to the rule regarding re-evaluation after five years not being followed.

In May 2014, the Committee searched PST's network in order to learn whether PST had taken steps to address the Committee's criticism. The searches showed that some local PST units still processed intelligence data on the I directory. The Committee also discovered that intelligence data had been processed in the P directory; something the Committee had not been aware of before then.[25]

In its response, PST apologized for the finding of intelligence data in the I directory, and stated that the service had had an «ongoing focus on the storage of personal data at PST». It also said that there had been «comprehensive clean-up work locally and centrally, even though the Committee's findings ... [showed] that it [was] still ... necessary for there to be internal follow-up on this point». It further wrote that «the fact that personal data processed at PST for intelligence purposes is either stored in SMART or DocuLive ... [was] repeatedly pointed out to the local police chief and local units», which have day-to-day responsibility for compliance with internal procedures and rules at local PST units.

In relation to the findings on the P directory, PST wrote that until 2013 it had been technically possible for employees to store information on the P directory, and that the information found by the Committee came from the time before such access was blocked. PST pointed out that the files found by the Committee had been deleted, and that the ICT section had reviewed the rest of the P directory, and confirmed that no other intelligence information was stored there.

The Committee noted PST's input regarding the Committee's new finding of intelligence data on the I and P directories in the directory structure, and agreed that the findings showed a need for continued internal follow-up of the service. The Committee also noted that it was unfortunate that it had been technically possible for employees to store personal data on the P directory until 2013, but that it was positive that this was no longer the case.

The Committee concluded by pointing out that it viewed PST as a single entity, and that the head of PST was responsible for the PST units' processing of personal data as part of the performance of its duties.

In 2015, the Committee will continue to check whether PST processes information outside archives and registers.

3.5 Foreign intelligence activities in Norway

In one case, the Committee raised the question of foreign intelligence activities in Norway, and use of sources (HUMINT operations) on Norwegian territory. PST was asked to state whether cooperating services' use of sources / HUMINT operations in Norway in relation to persons in the case had been reported to and approved by PST, including whether PST considered that the operations were consistent with allied states' intelligence activities on Norwegian territory. PST was also asked to account for its knowledge of the extent to which the foreign cooperating service's own intelligence staff in Norway had otherwise monitored / continues to monitor persons in Norway associated with the case.

PST stated that the service had good relations with the foreign cooperating service in the specific case. The service said that «PST does not know what source the information in the document comes from, but neither does PST have a foundation on which to assume that [the foreign cooperating service] used HUMINT resources in Norway in connection with this event». PST also wrote to the Committee:

Photo: Daniel Nordby/Forsvarets ingeniørhøgskole/Forsvaret

«The nature of the cooperation leads us to believe that we would be notified if any information were acquired through HUMINT in Norway. PST also wants to point out that if [the foreign cooperating service] had a central HUMINT resource in the environment PST was investigating, this would probably have resulted in a large number of highly-detailed reports. As PST does not find any indication that [the foreign cooperating service] has used sources / conducted HUMINT operations in connection with this case, it is difficult for PST to answer the remaining questions from this Committee in this context hypothetically.»

The Committee took PST's account under advisement. The Committee nevertheless found that there would be grounds for concern if the foreign cooperating service collected information on its own or kept a source in Norway, without this being reported to PST. The Committee commented that the information in the document does not exclude this from having been the case here.

On general grounds, the Committee found that PST's attention is directed towards the intelligence activities of foreign states in Norway. The Committee pointed out that in cases where cooperating services give PST intelligence information about matters that have taken place on Norwegian territory, the service should try to clarify how the foreign cooperating service acquired the information. This is in order to establish whether the retrieval has violated the assumption of a foreign state's intelligence activities in Norway requiring the approval of PST.

3.6 Individual case of the spreading of undermining information

In connection with conclusion of a preventive case, PST planned «operational counter-measures» in the form of spreading undermining information about persons. The service determined that the exact nature of the operational counter-measures was classified information, and it cannot be reproduced here.

In its closing letter to the service, the Committee made reference to the general rules regarding performance of police service, pursuant to section 6 subsection 2 (2) of the Police Act, considering that «The means employed must be necessary and be commensurate with the gravity of the situation, the purpose of the action taken and the circumstances in general». The police and procedural basic principle of proportionality expressed in section 6 of the Police Act will consequently apply to PST's use of operational counter-measures. Based on the uncertainty associated with the 'result' of the operational counter-measures, the Committee believed that on the whole it was dubious whether the operational measures were necessary.

The Committee also made reference to section 6 subsection 3 of the Police Act that «The police shall act in a businesslike and impartial manner and with consideration for persons' integrity, so as to ensure that anyone who is the object of police intervention is not laid open to public exposure to a greater degree than required by performance of the police action». The Committee believed that it is problematic that the service consciously tries to spread undermining information about persons who cannot even be considered a suspect of a crime. Such information may also affect third-parties who are not under investigation by PST, and entails consequences that cannot be foreseen. In the view of the Committee, it was dubious whether the measures could be considered proportionate, in light of the possible consequences for the people who could be affected directly and indirectly by the information. PST has special responsibility for conducting itself impartially and correctly, something that could be questioned in this matter.

The Committee believes that the service's operational counter-measures raise issues of principle regarding how a security service can intervene against citizens.

3.7 PST's processing of applications for declassification and access

In its annual reports from 2007 to 2013, the Committee described PST's processing of applications for declassification and access. With reference to the general rule in the Security Act that classification lapses after 30 years, the Committee has asked whether individuals may access old information registered about them. After being informed of the position of the Ministry of Justice and Public Security on the matter, the Committee stated that its understanding of the Ministry was that it did not want to propose imposing legislation on old information. Following an account of the matter in the 2013 annual report, the Committee declared that it had not come any further in the work regarding access to old information at PST. In the Standing Committee on Scrutiny and Constitutional Affairs' recommendation to the Storting, a minority[26] asked the government to present a proposal to the Storting for a permanent oversight arrangement.

The Committee has noted that, on the basis of requests for access, in 2014 PST declassified and granted access to information older than 30 years. It is the Committee's understanding that PST granted access on a case-by-case basis,

25 The P directory is a network drive that is only intended to contain program files.

26 The Committee's members from the Norwegian Labour Party, the Centre Party and the Socialist Left Party.

placing emphasis on both the considerations of societal interests and privacy. The Police Register Act entered into force on 1 July 2014. The rules in the Act regarding access do not apply to PST. The Committee considers it positive that the service grants access to certain cases despite this. PST's declassification and granting of requests for access in 2014 shows that the service understands that openness is necessary in a democratic society, and that information must not be withheld from the public without there being special reasons for secrecy.

The fact that PST in individual cases grants access clearly shows that access can and should be granted in certain cases. In the view of the Committee, it is difficult to see arguments in favour of leaving administrative practice to set the conditions and discretionary aspects associated with such access. Imposing legislation on the criteria for granting access will guarantee predictability and prevent arbitrariness.

3.8 PST's requests to telecommunications providers for communications control – classification and security clearance

The Committee addressed the challenges associated with security clearance of personnel who handle communications control cases at the telecommunications providers[27] in the 2012 annual report, under the section regarding oversight of Telenor[28], and in the 2013 annual report when discussing oversight of NetCom. The inspection of NetCom in 2013 showed that PST's requests for help to carry out communications control were not classified in accordance with the Security Act. The Committee accordingly stated that in 2014 it would follow up certain issues related to security clearance of information from PST to telecommunications providers when requesting assistance with the execution of communications control, and any consequences in terms of security clearance of personnel at police service centres that help PST.

Section 8 (1-2) of the Oversight Act states that «Information concerning whether a person has been subjected to surveillance activities or not shall be regarded as classified unless otherwise decided.» PST was accordingly asked to account for the extent to which the service considers that information about persons under surveillance through covert coercive measures at PST is classified information that, by definition, must be classified according to its content, pursuant to section 11 of the Security Act. PST was also asked to explain the background for the service's requests for assistance to NetCom, among others, regarding the execution of communications control not being classified according to the Security Act with an associated authorization and/or classification of personnel and requirements regarding information systems, etc.

In its answer to the Committee, PST accounted for its practice of declassifying information in requests to telecommunications providers. The service nevertheless acknowledged that this is not the best solution. The service stated that the challenge was presented to the working group for revision of the Security Act, and that a legislative amendment as outlined in Proposition No. 1 S to the Storting (2013–2014) is highly desirable. If an arrangement is arrived at where all actors who offer telecommunications services are covered by the regime of the Security Act in a way that is manageable in practice, this will provide a far more reassuring foundation for interaction. The Committee took the service's account under advisement.

The Committee was later sent a copy of PST's letter to the Ministry of Justice and Public Security regarding these matters. In the letter, PST agreed with the Committee's concern that declassification of information in a request for communications control is not justifiable from a security perspective. The service accordingly does not want to continue the current practice. PST concluded that the service views the current practice of sending unclassified requests for communications control to entail a higher risk than acceptable. PST expressed a desire for the Ministry of Justice and Public Security to approach the Ministry of Defence without delay, so that private enterprises that handle requests for communications control become subject to the Security Act following an administrative decision.

The Committee considers it positive that PST has approached the Ministry of Justice and Public Security on this matter, and expects the case to receive the necessary follow-up.

3.9 Information exchange with cooperating foreign services

3.9.1 Conditions for surrender and documentation

In one case, the Committee queried the surrender by PST of a Norwegian person's Norwegian telephone numbers to a cooperating European intelligence service. The person had previously been part of a preventive case at PST. The Committee commented that the telephone numbers of the person had been surrendered seven months after the preventive case against the person had been closed, with the justification that «the use of methods and other information in the case has shown that their link to the grounds for concern has been weakened… Further investigations of [him] are therefore no longer necessary.» The information was provided at the same time that PST submitted a presentation of the case in question to the foreign cooperating service. The preventive case against other persons in the larger case was still ongoing.

The Committee noted that the presentation did not show that the person in question had been removed from the case seven months earlier, with the justification given above. PST's

presentation further showed that the person in question had been in contact with one of the other main objects of the case. After reviewing the case documents from PST, the Committee did not find that such contact had been confirmed at the time of the case nor later. In section 4-1 subsection 4 of the PST guidelines of the time, unverified information could only be surrendered «if the basic requirements regarding information to the recipient in question had been met, see above, and important security considerations called for this». When determining whether information can be surrendered, emphasis must be placed on the quality and importance of the information, the person in question, and the recipient. The recipient must also be informed that the information is unverified. In the view of the Committee, it was unclear whether the conditions for surrender of information about the person to a foreign cooperating service had actually been met. It appeared to the Committee that PST had surrendered misleading and unverified information to a foreign cooperating service on the date of the surrender. PST was informed of this view.

In the same case, information about the person's travel had been shared with other foreign services in states that are not known to fully respect human rights. The Committee questioned PST's assessments before the surrenders, considering proportionality and consequences for the person in question. PST's answers showed that there was no documentation of the assessments that provided the foundation for the sharing of the information.

The Committee stated that this was censurable.

3.9.2 Norwegians registered on a list drawn up by the Counter Terrorism Group (CTG)

In 2014, the Committee also brought up questions related to registration of Norwegian persons on a list drawn up in connection with international collaboration with the Counter Terrorism Group (CTG).[29] The CTG member countries place persons on the list, which is reviewed regularly by the member country responsible for administration of the list. PST has contributed information about tens of people. After having searched PST's intelligence register for persons mentioned on the list, the Committee asked the service to explain why there are persons on the updated list who have been entered by PST but are not registered in Smart as objects (anymore). The Committee also asked PST to explain which criteria it applies to the registration of Norwegian persons on the list, the purpose of the registration of persons on the list, and the plans for use of the information by cooperating services within the CTG collaboration.

PST replied that persons who are deleted as objects from the intelligence register in principle must not be on the list. The persons mentioned should therefore be removed from the list by being deleted from Smart, and at latest during the regular quarterly update to the list. PST acknowledged that follow-up of the list could be better, and that the service would review the list and remove the persons who no longer meet the registration criteria. In its closing letter to the service, the Committee remarked that it is unfortunate that there are people on the list today who are not registered in Smart (anymore). Out of consideration of individuals' privacy, it is censurable that PST had not reviewed the list earlier and removed persons who no longer meet the registration criteria. The Committee noted that the service would start such a review.

3.9.3 Norwegians registered in the Terrorist Screening Center (TSC) database

In the 2013 annual report[30], the Committee stated that it had learned that information had been processed about a fairly large number of Norwegians in a database belonging to the Terrorist Screening Center (TSC), whose purpose is to identify suspected or potential terrorists. PST itself entered information about a few persons in the database, where the criterion was that the person had been charged or convicted of a crime that is relevant to the mission of TSC. The case was brought to the Ministry of Justice and Public Security, which was asked to check whether the information about third-parties had been entered into the database in violation of the restrictions on US authorities' activities in Norway and/or whether the information was processed in violation of the assumptions regarding use of intelligence information owned by PST.

The case was followed up in 2014. In January 2014, the Ministry stated the following:

> «The Norwegian authorities have no knowledge of the background for or the effects of registration of Norwegian persons and persons affiliated with Norway in TSC's database when this takes place outside the arrangement between TSC and PST. The Ministry will contact the US authorities in an appropriate manner with a view to illuminating the matter as well as possible.»

The Committee met with the Minister of Justice and Public Security on 24 April 2014, who stated that until then, the Ministry had spoken to the authorities in Washington through the Ministry of Foreign Affairs and the embassy. It was stated that the Ministry would draw up a formal query, following a

27 Chapter VIII section 2.

28 Chapter VIII section 2.

29 CTG is a European counter terrorism cooperation forum between the security services in the EU, and Norway and Switzerland.

30 Chapter IV section 8.

request by the Americans. It was stated that the Norwegian authorities have no control over which Norwegians are reported to TSC by others, and that most Norwegians are not reported by PST. The Minister of Justice and Public Security stated that Norway has no sanctions towards the USA associated with erroneous registration, etc., and that it is unlikely that the USA will comply with a request from Norway.

In June 2014, the Committee asked PST for an updated list of Norwegian citizens registered in TSC. The list showed that twice as many Norwegian nationals were registered in TSC as when the Committee brought the matter to the Ministry in 2013. At present a significant number of Norwegians have been registered by TSC. Following correspondence with PST, the Committee has been informed that the service has still only entered a few persons into the database, based on the person having been convicted of a crime. When the Committee asked whether PST had received any further explanations for the reason for the registration of persons who the service itself had not entered into TSC, PST answered that it was unclear who had provided the information about the other persons affiliated with Norway in the database. The service has discussed this with the FBI. PST has not received a full answer as yet. PST also answered:

> «On our part, there are some doubts regarding the criteria for entry and final use of the information in the database at present. In other words, it is difficult for PST to determine what is at the heart of the different entries into the TSC database. Neither do we know what the consequences will be for each person of their being in the database, for example when travelling to the USA.»

In a new letter to the Ministry of Justice and Public Security, the Committee again pointed out that it is problematic that the FBI TSC database has processed information about a large number of Norwegians and persons affiliated with Norway without our knowing why they have been registered. The Committee pointed out that the US authorities processing information about Norwegian citizens in the database could give cause for concern in relation to due process, since the information has not been entered, approved or quality assured by PST.

In March 2015, the Ministry of Justice and Public Security stated that on several occasions in 2014 and 2015, the Ministry contacted the US authorities both in writing and verbally, asking for an explanation for the registration of information about Norwegians and persons affiliated with Norway in the TSC database. The Ministry has not received an answer from the US authorities regarding, among others, the reason for the registration of Norwegians in the database, who registered the information, who the end-user is, and the possible consequences for the persons registered. In or prior to March 2015, the Minister of Justice and Public Security asked for an answer from the US authorities to the questions posed by the Norwegian authorities. The Minister of Justice and Public Security informed the Committee that he will continue to follow up the case with the US authorities, and provide a full answer to the Committee's questions when such clarification has been provided.

The Committee believes that it is important that the Ministry follow up the case.

3.10 Information exchange with national agencies

3.10.1 Collaboration between PST and the customs authorities

In its 2006, 2007 and 2008 annual reports, the Committee discussed issues related to the collaboration between PST and the customs authorities. In the 2013 annual report, the Committee wrote that in two specific cases it had asked questions about the collaboration between PST and Norwegian Customs, partly in relation to requests for customs control and exchange of information about individuals who pass the Norwegian customs border, and in relation to surrender of information from the TVINN declaration system for goods. The Committee followed up the cases in 2014.

Request for customs control and subsequent notification to PST.

During an investigation at DSE, the Committee saw a reference to a meeting between PST and the Directorate of Customs and Excise (TAD), where TAD received a list of names and personal identification numbers for a number of persons, «requesting entry of information into their registers, the objects being subject to customs control when passing a Norwegian customs office, with subsequent notification of PST».

The Committee found reason to question whether the exchange of information between TAD and PST had taken place outside the legal frames of their cooperation. The case also raised the question of whether TAD's surrender of information to PST complied with the provision regarding a duty of secrecy in in section 12-1 of the Customs Act.

In the request for customs control with subsequent notification to PST, the service argued that it in reality was a 'tip' to Norwegian Customs about persons who might to worth checking, in accordance with the legal authority of Norwegian Customs. PST nevertheless acknowledged that its communication should have been clearer in order to distinguish between tips and requests for customs control within PST's own legal authority and authorization from the court. However, TAD interpreted PST's query partly as tips and partly «as a request for customs control of these persons, and a request for information about the result». TAD told the Committee that «because we were aware that the reason

PST had provided the names of specific named persons was linked to suspicion of financing terrorism», the surrender was considered pursuant to the exemption from the duty of secrecy in section 12-1 subsection 2 (f-2) of the Customs Act.[31] TAD argued that «reasonable grounds for suspicion had to be established in and with the specific name list» from PST.

The Committee commented to PST that the service's preventive work focuses on environments and persons who are not necessarily suspected of a specific crime. Following the Committee's search of persons in the intelligence register, the Committee noted that from a control perspective it was difficult to ascertain the grounds for suspicion applied by PST to the persons at the time in question.

In further correspondence with PST, the service stated that it agreed with the Committee that section 12-1 subsection 2 (f-2) of the Customs Act did not provide a legal authority for information exchange from TAD to PST for the customs controls. One could not therefore expect reasonable grounds for suspicion «to be established in and with the specific name list» from PST, as argued by TAD. PST nevertheless believed that it is TAD itself that must determine whether the requirement of suspicion is present and whether the conditions for surrender in section 12-1 subsection 2 (f-2) of the Customs Act have been met.

Point 3 paragraph 3 of the cooperation agreement between TAD and PST states that «the exchange of information must not be used as a source of information for the parties to the agreement that could not be carried out within the frame of own legal authority». PST apparently agreed that it would conflict with the cooperation agreement, and thus entail circumventing the conditions for secret searches as a coercive measure if PST asked TAD for customs control without the service itself having legal authority for secret searches. PST nevertheless asserted that the information had been surrendered to TAD as a tip, and that TAD was not used as a source for information outside the legal authority of PST.

The Committee believes that PST's assertion that the request in reality (only) was a tip, which was also partly confirmed by TAD, had to be disregarded. The Committee stated that PST does not have legal authority to control persons through secret searches as a coercive measure in preventive cases regarding financing of terrorism. See section 17d of the Police Act – which does not cover section 147b of the General Civil Penal Code.[32]

The Committee stated that PST's requests for customs control require an 'arrangement' between the services, which means that TAD is used as a source of information for PST, and which could not be carried out within the frame of PST's own legal authority. The Committee believes that this practice may contravene point 3 of the cooperation agreement, and may entail circumvention of the conditions for secret searches as a coercive measure. The Committee noted that this gives cause for concern from the perspective of due process.

In its closing letter to PST and TAD, the Committee noted that TAD has independent responsibility for assessing whether the conditions for surrender of confidential information pursuant to the Customs Act are present, see section 12-1 of the Customs Act. The Committee nevertheless stated that:

> «Also PST has independent responsibility for not requesting information that the service itself cannot procure legally (or cannot procure without a prior court ruling). Such a request would conflict with the limitation in point 3 paragraph 3 of the cooperation agreement between TAD and PST, that «the exchange of information must not be used as a source of information for the parties to the agreement that could not be carried out within the frame of own legal authority». In the view of the Committee, this is precisely the situation here, where PST requested customs control of the 36 persons, with subsequent notification to PST.»

Surrender of information from the TVINN customs declaration system

In a related case, the Committee looked at the question of the legal authority for surrendering information from the TVINN customs declaration system from TAD to PST in connection with a package belonging to a person.

Following a discussion of the exemptions from TAD's general duty of secrecy, see section 12-1 subsection 2 of the Customs Act, the Committee stated that the rules should be clearer if PST is to receive information in the preventive track, pursuant to section 12-1 subsection 2 (b) or (f-1).

Following from its general conclusions, the Committee believed that it is unclear whether section 12-1 subsection 2 (b) of the Customs Act provided legal authority for the surrender of information from TVINN to PST in the specific case.

It was the Committee's view that it was not the intention for the information from TVINN to be used by PST to prevent «a possible breach of the Act relating to Control of the Export of Strategic Goods, Services, Technology», as found by TAD in agreeing to the surrender. It looks like PST's actual focus

31 The provision is as follows: «If the information relates to punishable acts outside the administrative area of the customs authorities, the information may be given only if there are reasonable grounds to suspect the commission of an offence that is punishable by a sentence of imprisonment of more than 6 months.»

32 In investigation cases, secret searches as a method requires a Court ruling pursuant to section 200a of the Criminal Procedure Act.

was preventive counter-terrorism. When the purpose of the information retrieval is not prevention of a breach of the export control rules, the surrender from TAD for the purpose of export control appears to entail possible circumvention of the rules.

In the view of the Committee, PST thus appeared to have used TAD as a source of information outside PST's own legal authority; i.e. conducted secret searches without legal authority.

The question of documentation

In connection with the review of the cases mentioned above, the Committee noted that «At present PST does not have a complete overview of the information we receive from Norwegian Customs after the service has given TAD tips». The Committee told PST that it would be expedient to have better documentation of information received from TAD than one assumes is the case, following PST's reply. This would also make it easier for the Committee to check that the information exchanged between agencies complies with the rules.

3.10.2 Information exchange with the National Criminal Investigation Service (Kripos) in the Schengen Information System (SIS)

The Committee has studied the basis for Kripos' registration of a wanted person in the Schengen Information System (SIS)[33], based on a request from PST in a case.

20 days after the service decided to open a preventive case in order to investigate whether a person was preparing a crime which it is PST's duty to prevent, PST asked Kripos to issue a wanted notice with so-called discrete observation[34]. There was no suspicion of a criminal offence at the time. When asked about the basis for its request for registration in SIS, PST only made reference to the conditions for wanted notices, as follows from the wording in section 8 (2) of the SIS Act:

> «There are specific grounds to assume that data on whereabouts, itinerary, destination, passengers, objects carried or the circumstances under which the person [...] was found are necessary in order to prevent serious threats from [the person concerned]. The reason is information held by the Norwegian Police Security Service (PST), but which cannot be exposed.»

According to the preparatory works to the SIS Act, fairly strict requirements govern the registration of information about persons with a view to observation (surveillance) or targeted control.[35] The Committee accordingly questioned Kripos and PST about the foundation for registration of the person in SIS. The Committee also had questions regarding extensions of the wanted notice[36], and the foundation for its continuation after the preventive case was closed.

Kripos confirmed to the Committee that the SIRENE office does not perform an independent assessment of whether the material conditions for initial registration have been met, «as PST cannot expose the information that provides the foundation for the assessment». In relation to the specific request, Kripos wrote that «the letter stated that there had been a specific material assessment that the conditions had been met. The assessment had been performed by a police attorney at PST». The assessment was not available in any documents. Neither had it been made known to Kripos. When requesting continuation of the SIS registration, it was clear that Kripos assumed that the conditions for issuing the wanted notice still existed.

In its closing letter to Kripos and PST, the Committee noted that the SIS Act requires that the SIRENE office at Kripos performs quality assurance of all requests for registration in SIS. The Committee stated that there therefore was cause for concern in that all of PST's requests to Kripos from 2009 to 2014 regarding wanted notices in SIS had been registered

without any such form of quality control. The Committee also had the following remark to Kripos:

> «It is difficult for the Committee to see that an exception should be made to SIRENE's control obligation in relation to requests from PST. The Committee wishes to point out that chapter 6.4.6.4 of the preparatory works states that the former Police Surveillance Agency (POT) stated in its consultation document that «POT will not use the SIS system much, as SIS will entail spreading of information, which from a security perspective makes it unsuitable as a communications system for sensitive information». Even though PST's position has obviously changed in relation to the use of the SIS system, SIRENE will keep its role as a quality assurer of wanted notices in SIS. A prerequisite for use of the system is that Kripos has enough information to determine whether the conditions for registration have been met. If not, the current practice may serve to undermine the consideration of each person's privacy.»

The Committee has asked PST to consider giving a small number of persons at the SIRENE office security clearance at the right level and giving them a secure information system, so that Kripos can assure the quality of the requests from PST in the future.

Based on the strict conditions regarding registration in section 8 of the SIS Act, the Committee believed that it was not clear whether the conditions regarding registration of the person in SIS had actually been met, including whether «the importance of the specific case indicates that the information should be registered» – see the basic condition for registration in section 5 of the SIS Act.

The Committee also stated that, under the assumption that the conditions associated with initial registration had been met, it was also doubtful whether the foundation for continued registration in SIS was present. In its closing letter to PST, the Committee also made reference to the person continuing to be registered in SIS seven months after closing the preventive case, despite the concluding report for the case expressing that there no longer were grounds for linking the person in question to the concern that led to the opening of the preventive case. The Committee noted:

> «The Committee believes that the SIS wanted notice for [NN] should have been cancelled by PST after the concluding report [for the preventive case] had been written … given the conclusions in the case. The Committee otherwise notes that new guidelines and procedures for registration in SIS according to the SIS Act will be finished soon, and asks for them to be sent to the Committee when they are ready.»

In 2015, the Committee will direct its attention towards PST's requests to Kripos regarding registration of persons in SIS.

3.10.3 PST's retrieval of passenger information from airlines

In one specific case, the Committee asked PST to account for the legal authority for requesting surrender of travel information about a person from airlines.

PST had the following reply about the case in question:

> «It is our view that the surrender has legal authority, see section 8 subsection 1 of the Personal Data Act, in conjunction with section 20 a of the Immigration Act, and section 4-24 of the Immigration Regulations, and that this must be seen as satisfactory grounds for processing in order for the airlines to surrender [NN's] travel details. PST had a legitimate need at this time to obtain information about [NN's] travel in order to be able to clarify whether an act of terrorism was being prepared.»

The Committee noted that section 20 subsection 1 (a) of the Immigration Act states that the Regulations can determine that «the commander of an aircraft arriving from, or departing for, another country shall give the police a list of passengers and crew members». As mentioned by PST, this is regulated in section 4-24 of the Immigration Regulations:

> «On request, the commander of an aircraft which is coming from or going abroad shall give the police a list of the passengers and crew, after the check-in process is complete, see section 20, subsection 1 (a) of the Act. The list shall contain the same information as the passenger list…»

However, the Committee noted that the purpose of the Immigration Act is to «provide grounds for regulation and

33 SIS is a shared computerized information system that guarantees fast and safe exchange of information between the Schengen countries. The information system has two components. It partly consists of a central database and a technical support function located in Strasbourg, and partly of national registers that are established and operated by each Schengen country. In Norway, this has been implemented in Act No. 66 of 16 July 1999 regarding the Schengen Information System (the SIS Act). Each Schengen country establishes and operates the national part of the Schengen Information System at own risk. Each Schengen country has established a national unit that is responsible for use of the system – a SIRENE office – which in Norway is localized at Kripos. The SIRENE office at Kripos checks that the conditions in the Convention for issuing wanted notices in SIS have been met; this means that there is legal authority. See Proposition to the Odelsting (1998–1999), page 55, point 6.2.4, last paragraph, and page 65, point 6.4.5.1, in the remarks to Article 99.

34 See section 8 (2) of the SIS Act.

35 Proposition to the Odelsting No. 56 (1998–1999) page 54 point 6.2.2.3, paragraph 1.

36 When it was extended the first time, the person was no longer linked to preventive cases at PST.

control of entry and departure, and foreign nationals' stays in the realm, in accordance with Norwegian immigration policy and international obligations»[37]. The Act's scope of action is «the entry of foreign nationals into the Kingdom of Norway and their stay in the realm»[38]. It follows from the Act that «a foreign national means any person who is not a Norwegian national».[39]

The Committee pointed out that the person whose travel information PST had requested from airlines is a Norwegian national. The Committee also noted that the information that PST received from, among others, airline [X] did not appear to be limited to such information that the commander of an aircraft is under an obligation to provide, pursuant to the above-mentioned provisions in the immigration legislation.

The Committee accordingly believed that surrender of passenger information about the person to PST did not appear to have legal justification in the immigration legislation as argued by PST.

3.11 Notification upon establishment of mobile-restricted zones

Section 6-2a was added to the Electronic Communications Act in 2013.[40] The provision covered «mobile-restricted zones». Points 1 and 2 of the second subsection state:

> «The Police and National Security Authority shall notify the Authority without undue delay once frequencies allocated to others are used. Notification shall state the frequency area, time period and location.»

In 2014, the Committee asked NSM and PST to account for its practice regarding the requirements in the Act to notify the Norwegian Communications Authority (Nkom).[41] The reason was that in the autumn of 2014, Nkom told the media that the Directorate had not received notification of the establishment of mobile-restricted zones following the entry into force of section 6-2a of the Electronic Communications Act.

During an inspection of NSM, the Directorate stated that the legal authority had not been applied yet.

PST stated in an inspection that it had not complied with the notification obligation to Nkom when using mobile-restricted zones. The service argued that this was due to a conflict between the notification obligation and the rules regarding duty of secrecy that apply to PST's use of coercive measures. In its view, the duty of notification may also mean that classified information is compromised. PST also stated that the service's use of mobile-restricted zones is carried out precisely in order to not disrupt the network. It further stated that the service had contacted the Ministry of Justice and Public Security about the matter.

The Committee has noted that it follows from the preparatory works[42] to section 6-2a of the Electronic Communications Act that the Ministry of Justice and Public Security determined that the provisions regarding the duty of secrecy in section 216i of the Criminal Procedure Act and section 17f of the Police Act were not an obstacle to the proposed duty of notification pursuant to section 6-2a subsection 2 of the Electronic Communications Act. The reason was that this must be considered as notification in the interest of the recipient when it is necessary to promote the recipient's statutory duties or to prevent the activities from being carried out improperly, pursuant to section 31 subsection 1 of the Police Register Act.

The Committee will regularly check the use of methods in each case, and will follow up PST's notification to Nkom.

3.12 The Committee's investigation of allegations of political surveillance and PST's use of Christian Høibø as a source

On 13 March 2014, the Committee submitted a special report to the Storting about its investigation of allegations of political surveillance and PST's use of Christian Høibø as a source[43]. The Standing Committee on Scrutiny and Constitutional Affairs submitted its recommendation on 3 June 2014[44]. The Committee's recommendation contained several remarks. The special report was discussed by the Storting on 11 June 2014. Its decision matched the recommendation of the Committee.[45]

Based on the investigation, the Committee concluded that PST's use of the source did not result in registration of persons merely as a result of affiliation with political organizations. In relation to PST's use of sources, the special report stated that the Committee had not previously requested access to the service's system for work with sources (KildeSys). This is because no previous cases had directly required such oversight, and because the Committee must «observe the concern for protection of sources» in its oversight activities, see section 5 subsection 1 (2) of the Oversight Directive. The investigation led to four remarks regarding PST's source work in particular by the Committee. In 2014, PST presented its view to the Committee, and concluded that it is not expedient to further specify which information is necessary for use of sources, because the present systems and procedures are presumed to function adequately.

In a letter to PST dated 23 October 2014, the Committee stated the following:

> «PST's account contains several elements that the Committee wishes to take into consideration during future oversight of the service and its work with sources.

This includes points that the Committee assumes would be relevant if guidelines are drawn up. The Committee has noted the impact of the reorganization on the work with sources. The Committee has further noted that the reorganization may lead to adjustments to the rules for work with sources.

The Committee is pleased that the biased references to Høibø have been deleted. PST's answer does not show whether the service, for example, ran spot checks in KildeSys in order to check whether the biased references to Høibø were one-off events, and thus not representative of the service's references to its other sources. The Committee expects PST to ensure that all references to sources is justified, and that the service facilitates the Committee's oversight of information processed in KildeSys.»

In 2014, the Committee also received information about the service's work with sources during an inspection of PST. So far the Committee has taken the service's account of its view on the need for guidelines under advisement. With reference to the remarks in the special report, and the Committee's notes in the recommendation, the Committee has decided to conduct spot checks of KildeSys in 2015, with special focus on the matters that were pointed out in the special report.

The Committee will notify the Storting of the result of these checks.

The Committee's reports to the Storting must be unclassified. Before the special report was submitted to the Storting, the text of the report was sent to PST in order to clarify whether it contained classified information. The Committee's conclusion was presented in the media before delivery of the special report on 13 March 2014. The EOS Committee contacted the head of PST on the same date, who was quickly able to ascertain that an employee of the service had responded to a question from the media in such a way that the conclusion could be derived. The Committee has made it clear to PST that the Committee's reports are made to the Storting, and that they must not be made public before that time. The Committee expects PST to handle the Committee's reports in accordance with the intention of submission to the service before submission to the Storting.

3.13 Complaints sent to the Committee

The Committee received 13 complaints regarding PST in 2014. Out of the cases closed by the Committee that year, the following two cases resulted in remarks by the Committee.

In one complaint regarding illegal surveillance involving PST, the Committee found several matters that resulted in censure of the service. In another complaint, the Committee directed some criticism towards PST for having processed information about the complainant that the service no longer had reason to process.

The Committee's statements to complainants must be unclassified. Information about someone having been the object of surveillance or not is considered classified, unless otherwise determined. Section 8 (2) of the Oversight Directive also states:

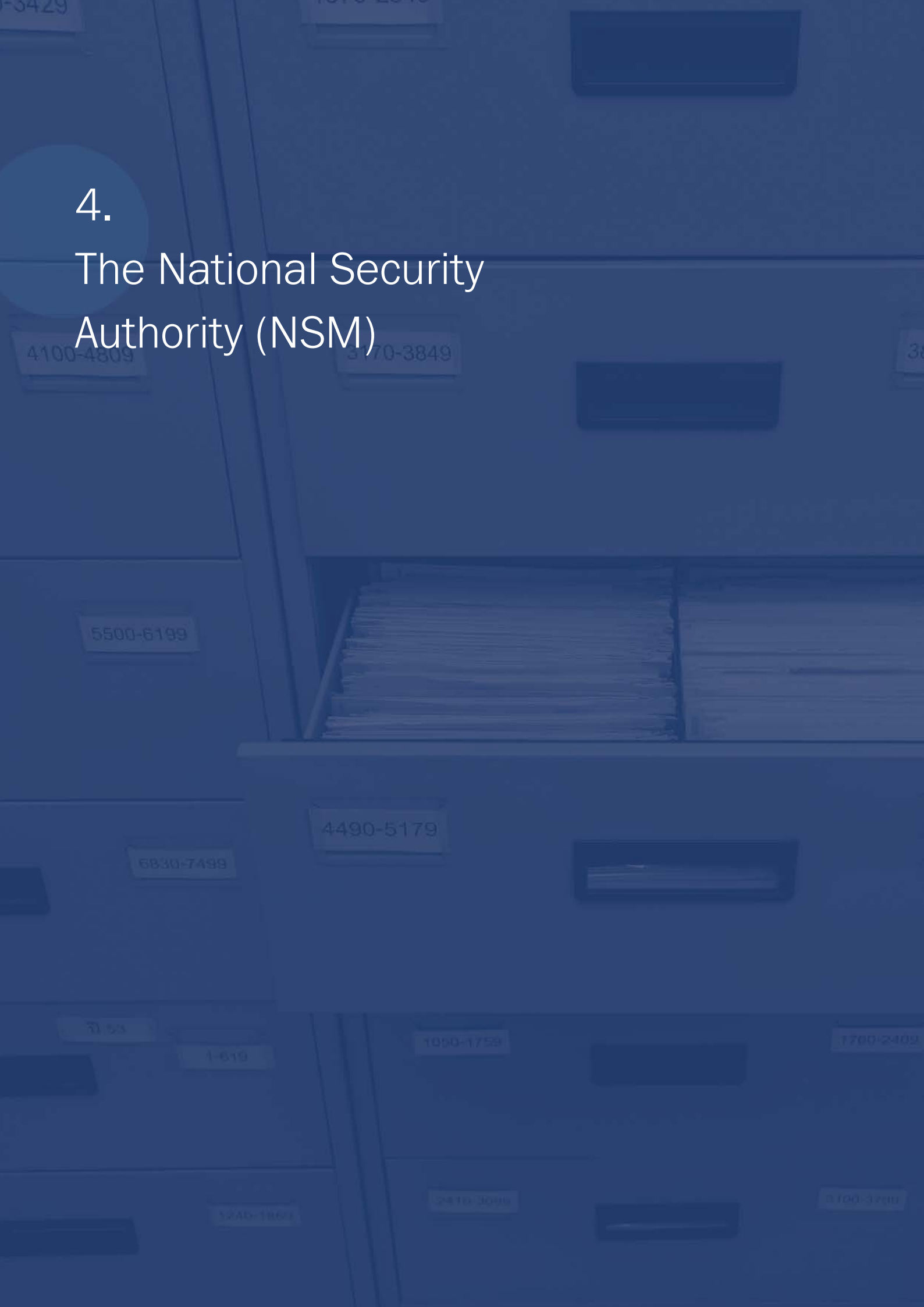
> «Statements to complainants should be as complete as possible without providing classified information. When there are complaints against the Norwegian Police Security Service regarding surveillance activities, a statement shall only be made as to whether the complaint has resulted in censure or not. If the Committee believes that a complainant should receive a more detailed justification, it shall suggest this to the Ministry in question.»

The Committee was given the opportunity to give one of the complainants an explanation that was more detailed than merely stating that the complaint had led to censure.

The Committee finds it to be a great challenge that it can only give complainants a limited justification of the Committee's censure of PST regarding complaints.

37 Section 1 of the Immigration Act.
38 Section 2 of the Immigration Act.
39 Section 5 of the Immigration Act.
40 Act No. 83 of 4 July 2003 regarding Electronic Communications.
41 The former Norwegian Post and Telecommunications Authority (PT).
42 Proposition to the Storting 69L (2012–2013) chapter 9.6.4 page 84.
43 Document 7:2 (2013-2014).
44 Recommendation to the Storting 229 S (2013–2014).
45 Decision 463.

4.
The National Security Authority (NSM)



4.1 General information about the oversight

In 2014, the Committee conducted four inspections of NSM, including one inspection of NSM NorCERT.[46]

The inspections of NSM mainly focus on personnel security. The Committee performs special inspection of cases where clearance is refused, reduced or suspended by the security clearance authorities. NSM performs the general functions in preventive security services pursuant to the Security Act. As well as being the security clearance authority for all CTS clearance in Norway, NSM is also the appellate body for lower levels of clearance. There are 43 security clearance authorities in Norway.

Also NSM's cooperation with other EOS services is an important area for oversight.

In the 2013 annual report, the Committee reported that it considered it positive that NSM had established an experience base for settled security clearance cases. An experience base may result in more equal treatment. Due to problems associated with the new case processing tool for security clearance cases (Mimir), and long case processing times in the field of personnel security, the work with the development of the experience base was not prioritized by NSM in 2014. At year-end 2014/2015, NSM started a project to develop the experience archive, which will be completed by the end of 2016.

In its inspection of security clearance cases, the Committee became aware of cases where the person concerned or their close relatives were affiliated with another state. These cases appear to have been processed differently by the different security clearance authorities. The Committee reported this to NSM in its role of oversight authority for all security clearance authorities.

4.2 Case processing time for security clearance cases

The case processing time for certain security clearance authorities is disproportionately long. In point 1.4, the Committee therefore asked the Storting to consider taking rapid action to remedy the situation.

During inspections of NSM in 2014, the Committee was notified of the case processing time for security clearance cases. NSM itself stated that there were challenges associated with the case processing time. NSM has informed the Committee that there was a substantial increase in the number of requests for security clearance from 2012 to 2013. The efficiency of NSM's case processing was reduced in 2014, as a result of the problems with the new Mimir case processing tool. For example, NSM told the Committee that the average case processing time for complaints in 2014 was 13 months. At the beginning of 2015, NSM had a backlog of 520 cases.

NSM has reported that personnel have been reassigned internally and new positions have been established in order to improve the case processing capacity. NSM expects the long case processing time to last for much of 2015.

4.3 Security clearance case regarding failure to disclose health details

In a security clearance case decided by NSM, as the appellate body, the Directorate denied the person concerned security clearance, with a three-year period of observation. The security clearance case showed that section 21 subsection 1 (d) of the Security Act[47] was granted most weight in the assessment of the suitability of the person concerned with respect to security. The Directorate believed that the person concerned had failed to disclose facts regarding their health that they must have understood were of importance to the security clearance.

The Committee's questions included why the Directorate believed that letter d was the crux of the matter, and pointed out that questions 10-1 to 10-3 on the personal health data form are discretionary, in the sense that it is up to the person concerned to decide how medicine and diseases, etc. can affect their judgement. The GP of the person concerned had stated that use of medication did not have a negative impact on judgement or affect the mental state of the person concerned.

In its closing letter to NSM, the Committee wrote the following regarding this point:

> «The Committee's notes that NSM does not share its view that points 10-1 to 10-3 on the personal health data form are discretionary, in the sense that it is up to the person concerned to decide how medicine and diseases, etc. can affect their judgement.
>
> The Committee accordingly wishes to point out that it is not obvious what is meant by «mental illnesses» in

46 NSM NorCERT (Norwegian Computer Emergency Reponse Team) is Norway's national centre for the coordination of incident management in connection with serious IT security breaches. NSM NorCERT is a function provided by NSM's operational division.

47 Section 21 subsection 1 (d) of the Security Act states: «Importance may be attached to information regarding the following matters ... Falsification or misrepresentation of or failure to present facts which the person concerned must have understood are of significance for the security clearance.»

question 10-1. This is not defined on the personal data form or in the guide to the form. If the question is viewed in the context of the guide, the question appears to focus on mental illnesses that may be of importance to suitability with respect to security, in that they affect the loyalty, reliability and sound judgement of the person concerned. With this focus, it is the Committee's view that this should be clear from the question, and the guide should provide examples of illnesses.

In relation to question 10-3, the person concerned must consider whether they regularly use medication that can affect their judgement. The guide provides examples of medication, and states that the packaging information for regular medication must be checked, or a doctor must be contacted if there are any questions. The Committee thus believes that the assessment of the person concerned when answering the questions requires the use of discretion. The person concerned cannot be expected to have any medical or security expertise.»

Based on the wording of the questions on the personal data form and their explanation in the guide, the Committee believed that misrepresentation of or failure to present facts related to these questions should be judged more mildly than misrepresentation or failure to mention crimes recorded in the registers of criminal offices. The responses to these questions by the person concerned had little discretion attached to them. The Committee accordingly believed that NSM placed too much emphasis on section 21 subsection 1 (d) of the Security Act in this case.

4.4 Consequences of withdrawing a complaint during the appeals process

In the 2013 annual report[48], the Committee discussed a security clearance case that was dropped during the appeals process. After the complaint regarding revocation of security clearance was submitted to NSM as the appellate body, the complaint was withdrawn because there no longer was a need for security clearance. The consequence was that the security clearance status of the person concerned remained SECURITY CLEARANCE DENIED, with a five-year period of observation. NSM was asked to reopen the security clearance case, partly because it was unclear whether the person concerned was aware of the negative consequences associated with withdrawing the complaint, and partly because questions could be raised regarding the grounds for the negative decision regarding security clearance in the first instance.

In 2014, NSM reported back to the Committee that the Directorate would not reopen the security clearance case. NSM disagreed with the Committee that the person concerned had received inadequate information about the negative consequences of withdrawing the complaint during the appeals process. NSM also disagreed with the Committee

Photo: Erlend Aas / NTB scanpix

that the Directorate had not met its duty of guidance towards the person concerned.

The Committee noted that NSM would not reopen the security clearance case. The Committee still stated that the emphasis on poor judgement and reliability by the first instance due to the medical history of the person concerned appears to conflict with the expert statements in the case. In the view of the Committee, this might indicate that the case had not been properly illuminated by the security clearance authorities. The Committee remarked that the fact that the case did not appear to be properly illuminated might have led to the security clearance authorities forming an incorrect or incomplete picture of the facts.

Neither could the Committee see, as argued by NSM, that there was a requirement pursuant to section 4-1 subsection 5 of the Personnel Security Regulations that there must be «strong reasons to consider a reversal» or that the decision is «obviously ... invalid or clearly outside the frame of good discretion» in order for NSM to be able to consider a reversal of the case.

4.5 Case regarding procurement of information about persons for whom vetting is not required

Personnel must be vetted in connection with security clearance, which entails «procurement of relevant information in order to assess security clearance».[49] Vetting of personnel primarily covers information provided by the subject.[50] The control must also include information that the security clearance authorities themselves possess and examination of relevant public registers.[51] In certain cases, vetting is required of the person's «close relatives» (spouse, partner, cohabitant, parent of joint children,child, parents and siblings),[52] which gives NSM the right to demand the surrender of information about the close relatives of the person concerned from the same sources and registers.

In 2014, the Committee asked NSM about procurement of information about persons for whom vetting is not required. The background for the query was a security clearance case where NSM, as a result of issues on the part of the person's girlfriend that could be relevant to the security clearance, had procured information about the girlfriend from the Central Population Register. Information had also been procured about the person's girlfriend, the girlfriend's father and the girlfriend's previous spouse in the Population Register.

The fact that the person concerned and the girlfriend were not in a close enough relationship for her to be vetted appeared to be in the disfavour of the person concerned when assessing the merits of the security clearance case. It is thus possible that the person concerned would have had a stronger standing if the relationship had been formalized through cohabitation or marriage, even though issues on the part of the girlfriend were at the heart of the matter.

In the Committee's closing statement to NSM, it declared that it may be relevant to clarify whether the person concerned or their close relatives were in contact with an actor representing a threat, for example, in order for the security clearance institute to serve its purpose. However, in the view of the Committee, there was no legal authority for the procurement of information about other persons than the person concerned and their close relatives through vetting. It was accordingly pointed out that the category of people who are to be vetted is clearly specified in legislation, and that the legislator accordingly appears to have set a clear and justified limit on the information that is relevant for retrieval in a security clearance case. It also stated that information may be retrieved and processed based on consent (from the person concerned) or law (close relatives), which are the general grounds for processing of personal data in the data protection legislation.

Finally, the Committee wrote that it believed that if NSM sees a need to procure information about other persons than the one concerned and their close relatives through vetting, this should be laid down in law. The Directorate was accordingly encouraged to consider whether the issue should be discussed in connection with the work to revise the Security Act.

4.6 Security interviews

In the 2013 annual report, the Committee stated that it had asked NSM why the Directorate had not conducted security interviews in three cases that had ended in denial of security clearance due to financial matters. The Committee accordingly provided its assessment of the principle behind the function of the security interview during the security clearance process. Again following NSM's lead, the Committee accordingly had a verbal dialogue during inspections of the Directorate regarding execution of security interviews. The topic was also brought up at an inspection of FSA.The Committee further reviewed recordings of certain security interviews by NSM, FSA and other security clearance authorities.

48 Chapter V section 4.3.

49 See section 3 subsection 1 (18) of the Security Act.

50 See section 20 subsection 2 of the Security Act.

51 See section 20 subsections 4 and 5 of the Security Act, in conjunction with section 3-4 subsection 1 of the Personnel Security Regulations.

52 See section 20 subsection 3 of the Security Act.

Security interviews are based on an interview technique (the PEACE model) that is adapted to security interviews. The Committee's review of the security interviews showed that the quality of the interviews varied at the different security clearance authorities, and that certain interviews could have been conducted in a more pedagogical and targeted manner. The review also raised questions as to why the interview model used is considered the most suitable one. The Committee believes that it is particularly important that security interviews are conducted in a way that adequately secures the adversarial principle in the case processing. The Committee has also noted that the method does not appear to allow flexible security interviews, which are adapted to each case. This may make it more difficult to address doubts and illuminate the matter, which are the main purposes of such an interview.

It is the Committee's impression that certain security clearance authorities follow the template for security interviews too rigidly. In the view of the Committee, it for example takes too long before the security clearance authorities arrive at the topic that called for a security interview, and which is of relevance to the person's suitability with respect to security.

The Committee believes that it may be necessary to conduct an external evaluation of service interviews.

4.7 Access to information in security clearance cases

The security clearance authorities began using a new fully-electronic tool for vetting (Mimir) in July 2014, to replace the old case processing tool (TUSS). The Committee has been notified of defects in the system in relation to the case processing of vetting cases, including technical errors and inadequate functionality. When the system was introduced, it did not allow the inspection of security clearance cases either, so the Committee has been unable to adequately monitor security clearance cases since its introduction. It is the Committee's impression that no thought was given to granting it access to Mimir when it was developed or when NSM moved to new premises in Sandvika, which is also where the vetting section is based.

It has been difficult for NSM and FSA to print security clearance cases from Mimir in order to present them to the Committee. In the view of the Committee, the inspections must also be fully electronic. This will save NSM, FSA and the other security clearance authorities from much work, and will make it easier for the Committee to inspect security clearance cases.

Satisfactory electronic inspections means that the Committee needs access to at least seven computers with Mimir with a dedicated user. The Committee does not have such access today. By way of comparison, the Committee has access to users and one computer per committee member when PST and NIS are inspected. The Committee has asked NSM to give it corresponding access to Mimir.

4.8 Complaints sent to the Committee

The Committee received six complaints regarding NSM in 2014. Out of the cases closed by the Committee that year, the following five cases resulted in remarks by the Committee.

Complaint 1 – Links to a motorcycle club

In a complaint to the Committee regarding NSM sustaining a security clearance denial during the appeals process (and five-year period of observation), the Committee had questions regarding part of NSM's case processing. FSA was the security clearance authority, and the case was in reference to revocation of security clearance due to links to a motorcycle club. When the case was closed, the Committee made the following remarks regarding the case processing at NSM, which were also presented to the person concerned when the Committee finished processing the complaint:

> «The Committee does not disagree that the relationship or contact of the person concerned with the one-percenter bikers as defined by the police and the Armed Forces, may raise doubts about the person's suitability with respect to security. The threat constituted by contacts or relations with defined one-percenter clubs towards the Armed Forces and persons with security clearance is a clearly discretionary and security-based assessment. In the view of the Committee, a qualified connection with the clubs is necessary, and it must be so great as to raise such security-related doubts as to justify the loss of security clearance for the level in question. In the view of the Committee, the relationship between the pressure on the person concerned (letter c) and the extent to which a person with security clearance can be said to have misrepresented the facts (letter d) are of importance to the security clearance. Keeping in mind due process in relation to the person concerned, it is therefore necessary that the case is illuminated as well as possible, in order to determine whether the person concerned has misrepresented the facts of the case.
>
> The Committee has noted that [the person concerned], as an active member of an established motorcycle club in Norway, has a different view than the police and the Armed Forces on the influence of established motorcycle gangs, the Norwegian model and Hells Angels on the environment, etc. In the view of the Committee a different view of the situation is not synonymous with [the person concerned] having misrepresented the facts to the security clearance authorities.

The Committee believes that FSA's security interview with [the person concerned] in May 2011 did not adequately examine the issues related to grounds for pressure pursuant to section 21 subsection 1 (c), and that it did not adequately illuminate the misrepresentation of the facts of the case by [the person concerned]. The security clearance was withdrawn 10 months after the interview; March 2012. NSM sustained SECURITY CLEARANCE DENIED during the appeal some three years later, based on FSA's security interview with [the person concerned] in May 2011, among other factors.

Together with the fact that NSM extended the period of observation during the appeals process to a maximum period of five years because [the person concerned] consciously misrepresented facts of importance to his security clearance, this gives the Committee reason to question whether it was obviously unnecessary to conduct a new security interview with [the person concerned] during the appeals process. A security interview helps secure the adversarial process during the case processing, and provides an important guarantee of due process for the person concerned ... [who] has no other negative entries registered, other than the doubts on the part of the security clearance authority due to his affiliation with a motorcycle gang. In the view of the Committee, a security interview should have been conducted during the appeals process in order to ensure that the case was illuminated as fully as possible before the decision was made.»

The Committee pointed out to the person concerned that it did not find reason to criticize NSM's assessment of the merits of the case; i.e. the decision to sustain the denial of security clearance during the appeals process. The Committee specified that its criticism of part of NSM's case processing still means that in the view of the Committee, NSM should have conducted a security interview with the person concerned during the appeals process. This was partly in order to illuminate the person's presentation of the facts of importance to the decision regarding security clearance, and in connection with determining the period of observation. The Committee believed that the error is not of such a nature to render NSM's decision invalid.

Complaint 2 – Requirement of justification and duty of investigation in connection with a negative decision

In another complaint regarding security clearance, the Committee queried NSM in its role of appellate body as to whether the complainant could have been given more detailed justification of the negative decision. The Directorate complied with the Committee's request. The Committee also asked NSM whether the person's statement regarding a matter could be considered failure to present facts. Based on the case papers, it was unclear to the Committee whether it was possible to conclude that the complainant had not presented the matter to the degree deemed necessary by NSM. The Committee stated that this aspect of the case should have been illuminated better before it could be given negative emphasis. The Committee notified the complainant that it had criticized NSM about this. The complainant was also notified that in the Committee's view, the matters brought up with NSM did not appear to be determinative for the content of the decision, and that it thus believed that the negative decision was not invalid. The Committee therefore did not ask NSM to reconsider the case.

Complaint 3 – Long case processing time

In a third case, the Committee criticized NSM of long case processing on a security clearance case, as the case had lain with the Directorate for 16 months. In its closing letter to NSM, the Committee stated the following, which was also passed on to the complainant:

Photo: Comnet / NTB scanpix

> «It is clear from NSM's answer to the Committee that there are several reasons for the long case processing time so far in this case. The Committee sees that these matters can impact on the case processing time. Despite this, it is the view of the Committee that the case should have been decided more quickly.
>
> The Committee assumes that NSM will settle the case within the time-frame specified by the Directorate of three months. If not, the Committee expects the complainant to be notified of further delays in writing, together with an indication of when processing of the case is expected to have finished.»

Complaint 4 – Long case processing time and incomplete personal history of close relatives

In a fourth case, the Committee stated the following to NSM in relation to the Directorate's (and also FSA's) case processing time during the appeals process for a security clearance case:

> «After [the person concerned] submitted a complaint regarding FSA's security clearance decision on 14 August 2012, it took FSA 306 days to sustain its decision – 16 July 2013. After this, it took a further 42 days before NSM received the case from FSA on 27 August 2013. It then took 294 days before NSM made a final decision in the appeals process on 16 June 2014.»

The Committee stated that the case processing time at both NSM and FSA had been disproportionately long, and that the total case processing time of 642 days during the appeals process was highly censurable, regardless of the facts. The Committee therefore found reason to criticize both FSA and NSM of a disproportionately long case processing time when reviewing the person's security clearance case during the appeals process.

The Committee also had questions regarding the merits of the case. After the person concerned married his foreign girlfriend of the past eleven years, upon reclearance, the person was denied security clearance with a period of observation until November 2016. The reason given for the denial of security clearance was an incomplete personal history for the spouse. The security clearance authority clearly had not previously considered the relationship to be of importance to the person's suitability with respect to security, see section 21 subsection 1 (k) of the Security Act – connection with foreign states. When looking at the merits of the case, the Committee believed that at present, and before the end of the period of observation, it ought to be possible for NSM to perform a concrete and individual overall assessment of the person's suitability to receive security clearance, and also to conduct a security interview with the person.

Pursuant to section 2 (1) of the Oversight Act, the EOS Committee shall clarify if and prevent the exercise of injustice against any party. The Committee has therefore asked NSM to reconsider the person's security clearance case, and to notify the Committee of the outcome of the case.

Complaint 5 – Processing of a complaint regarding access to documents of a case

In a fifth case, the Committee criticized NSM of having decided the merits of the security clearance case before reviewing a complaint regarding denial of access to the documents of the case. The Committee stated, among other things, that the right of access is generally critical to a party being able to safely protect their interests in an underlying case. The Committee further pointed out that one of the main purposes of the right of access is to be able to prepare a complaint as best possible, and that it is not possible to fulfil this right if processing of a complaint regarding denial of access is not completed before a decision has been made regarding the security clearance case. The Committee was also concerned because NSM could not identify the reason why the merits had been decided before the complaint regarding access, and that it was presumed that changes would be made to Mimir quickly in order to prevent this from happening again in the future.

The Committee further criticized NSM for having written to the complainant regarding the complaint about denied access after the merits had been decided. Here the person was informed that NSM had limited case processing capacity. The person was therefore asked to state whether they would sustain the complaint regarding denial of access. The Committee believed that NSM's conduct in this case was highly unsatisfactory, and was of the opinion that the Directorate had acted contrary to good administrative practices. The Committee pointed out that such a request can undermine the right to request access and that it could therefore be said to be at the expense of the person's due process. Even though the merits have already been established (which should not have been the case here, see above), the Committee pointed out that a case can be brought before the courts if, for example, a claim is presented that the decision is defective, so that the question of access remains important. There may also be intrinsic value in gaining access to information that a state body has processed and reviewed in a case regarding oneself.

The complainant was informed of the Committee's criticism of NSM.

5. The Norwegian Defence Security Agency (FSA)

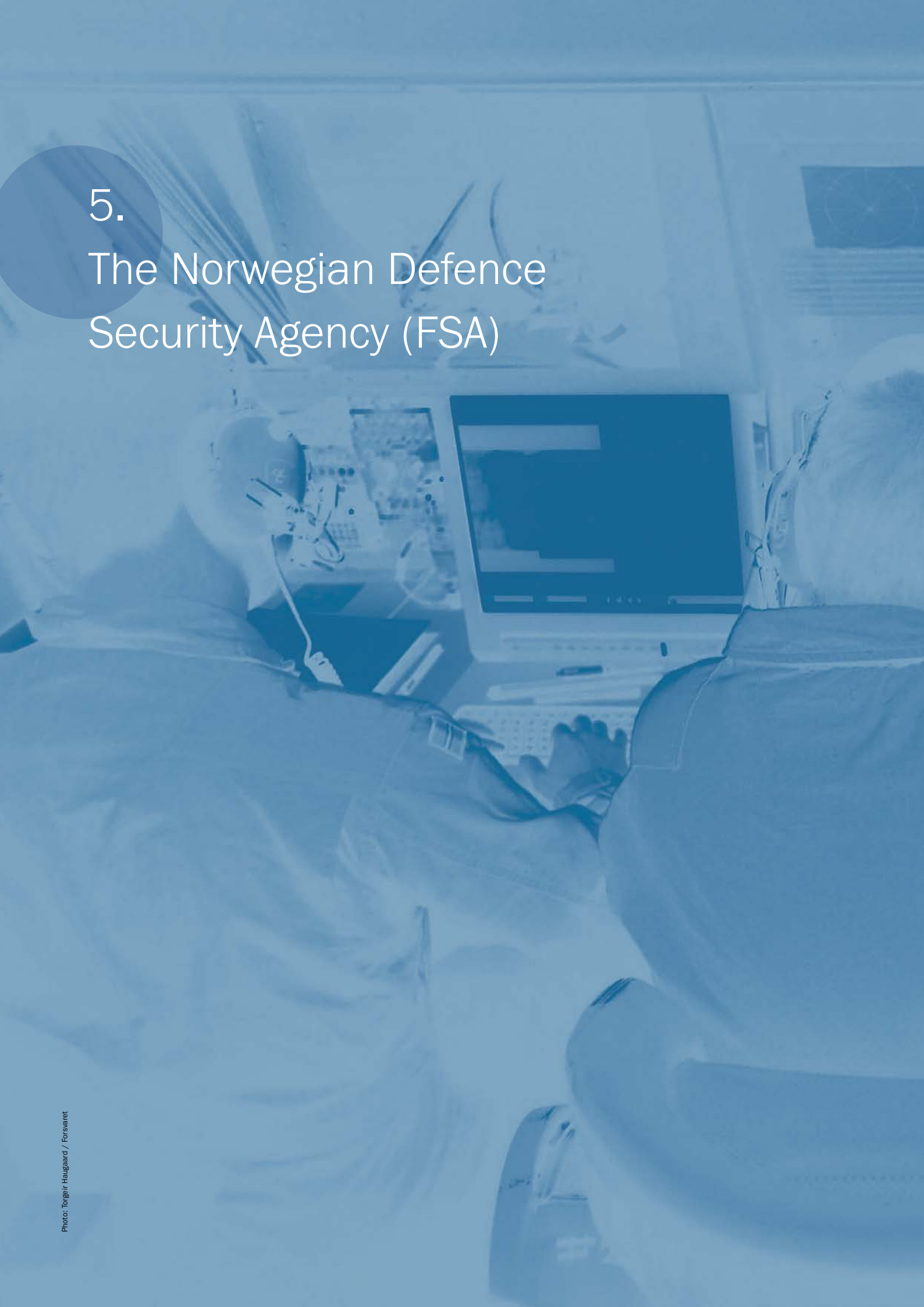


Photo: Torgeir Haugaard / Forsvaret

5.1 General information about the oversight

The Committee conducted three inspections of FSA in 2014.

FSA is Norway's largest security clearance authority. In 2014, the agency made decisions on 18,000 security clearance cases. The agency's processing of security clearance cases is therefore particularly important in the Committee's oversight of FSA. The Committee also performs oversight of FSA's preventive security activities in the Armed Forces. The Committee oversees the agency's investigations of activities that represent a threat to security in the Armed Forces (security investigations), and operational cases opened by FSA as part of the agency's responsibility for military counterintelligence n Norway in peacetime. FSA's processing of personal data is a key aspect of this oversight.

5.2 Case processing time for security clearance cases

The case processing time for certain security clearance authorities is disproportionately long. In point 1.4, the Committee therefore asked the Storting to consider taking steps soon to remedy the situation.

During inspections of FSA in 2014, the Committee was notified of the case processing time for security clearance cases. FSA has told the Committee that it believes that the case processing time is critically long. FSA has redistributed human resources internally, and added new positions in order to improve case processing times. Based on the lack of functionality in the new case processing tool (Mimir), FSA has been unable to provide an average case processing time for security clearance cases. FSA has informed the Committee about the problems with the new case processing tool and its impact on case processing times. FSA states that it is implementing substantial resources in order to improve this system.

5.3 Questions regarding two security clearance cases that had been dropped

Following an inspection of FSA, the Committee had questions regarding two security clearance cases that had been dropped.

Dropped case 1

A security clearance case was dropped by FSA on the grounds that it was no longer necessary, as the person was about to be discharged. Security clearance had been requested in October 2012 in connection with compulsory military service, and the case was dropped in September 2013. With reference to the requirements in the Public Administration Act regarding case processing time,[53] FSA was asked to explain why the agency had not finished processing the security clearance case before the person was to be discharged.

In its closing remarks to FSA, the Committee stated that it agreed with the agency, which replied that it was unfortunate that the case had not resulted in a justified decision after such a long time and after a security interview.

Dropped case 2

In the second case, the Committee stated that it generally believed that FSA should try to avoid nine months passing from completion of the personal data form to a security clearance decision being made. In such cases, the form must be filled in again in order to be valid.

5.4 Complaints sent to the Committee

The Committee received seven complaints regarding FSA in 2014. Out of the cases closed by the Committee that year, the following three cases resulted in remarks by the Committee.

Complaint 1 – Long case processing time

In one case, the Committee noted that seven months had passed since a person had filed a complaint regarding the agency's revocation of security clearance and no decision was yet made. The Committee believed that the case processing time had already been too long. It therefore expected a decision to be made by the agency soon, and that the case would be sent to the appellate body immediately if FSA sustained the denial of security clearance.

Complaint 2 – Long case processing time

The second case was about NSM sustaining a negative decision in the appeals process, see the discussion of complaint 4 in point 4.8, where the Committee criticized FSA of a disproportionately long case processing time when assessing whether its negative decision regarding security clearance was to be reversed or sent to the appellate body.

Complaint 3 – Long case processing time and sharing of vetting information

The third complaint was also in reference to NSM sustaining a negative decision during the appeals process. See the discussion of complaint 1 in point 4.8. In connection with processing the complaint, the Committee commented to FSA that it had taken some nine months from the agency conducting a security interview with the person concerned until FSA made a negative decision. After FSA received a complaint from the person concerned regarding the agency's revocation of their security clearance, it took FSA a full 15 months before the complaint was sent to NSM as the appellate body. The Committee therefore criticized the agency for the total case processing time having been far too long, especially during the appeals process.

In the same case, the person concerned also complained about what they called «a connection between FSA and the police». The background was that the person concerned claimed that they had been subject to pressure in connection with a meeting between the person and an ordinary police officer. The person concerned argued that the police was in possession of information that the person at the time had an open security clearance case at FSA, and that in the situation, the person felt pressure due to the police holding the information.

The Committee's investigations revealed that FSA had shared information about the person's security clearance case with the ordinary police. The investigation showed that in advance of the police's conversation with the person concerned, when asked by the police, it had confirmed that FSA had an open case regarding the person's security clearance, and that FSA would be revoking the person's security clearance. The Committee conducted interviews with a police officer and an employee of FSA, and they confirmed the Committee's findings in the case.

In the closing letter to FSA, the Committee stated that it follows from section 20 subsection 6 of the Security Act that «Information provided to the clearance authority in connection with vetting shall not be used for purposes other than the evaluation of security clearance». It follows from NSM's guide to the provision that:

> «Strict practice of the provision is required for the relationship of trust between the subject of security clearance and the security clearance authority. The provision must be seen as curtailing of the general duty of secrecy that otherwise follows from section 13 of the Public Administration Act.
>
> It must be considered to be within the frame of the provision to be able to share information with other public authorities when necessary in order to illuminate a security clearance case. Sharing information in order to investigate general crimes is obviously inconsistent with the provision.»

The Committee noted that the curtailed provision regarding secrecy in section 20 subsection 6 of the Security Act means that no information of importance to the assessment of suitability with respect to security of the person concerned must be used for other purposes. Information about the security clearance status of a person who has already received security clearance and their suitability for such security is covered by section 20 subsection 6 of the duty of secrecy. The Committee accordingly could not see that vetting information can be shared with other public authorities, including the police, without this «being necessary in order to illuminate a security clearance case». The Committee criticized FSA for a breach of the provision.

The Committee also commented to FSA that the person concerned experienced pressure from the police based on the surrender of the information. Even though the Committee did not find a reason to conclude that there was censurable pressure, the Committee pointed out the level of seriousness of the case, which illustrates why vetting information should not be used for other purposes than assessment of security clearance.

The complainant was informed of the Committee's criticism of FSA.

FSA took the Committee's criticism under advisement, and stated that the subject of the case and its level of severity had been discussed internally. The agency further stated that the Vetting Office had conducted a more thorough review of the subject of the case, in order to increase awareness of current provisions and procedures.

53 See section 11a of the Public Administration Act.

6.
The Norwegian Intelligence Service (NIS)

Photo: Terje Mortensen / VG / NTB scanpix

6.1 General information about the oversight

The Committee conducted four inspections of NIS in 2014. There was also one inspection of the service's technical information activities at the Armed Forces Experiment Station Vadsø.

The Committee must ensure that NIS' activities remain within the service's set tasks, and that injustice is not exercised against any party, see section 11 subsection 1 (a) of the Oversight Directive. During the inspections of NIS, the Committee oversees the following points:

- The service's technical information retrieval.
- The service's information exchange with domestic and foreign cooperating services.
- The service's archives and registers.
- Cases submitted to the Ministry of Defence and internal approvals.

During the inspections, the Committee was regularly updated about NIS' current activities, including the service's cooperation cases with other EOS services, the threat picture and cases submitted to the Ministry of Defence, and internal approvals. These can be approvals of retrieval or sharing of information about Norwegian legal entities abroad, in retrieval disciplines or case types that have already been approved by the Ministry of Defence. Such approval may for example give NIS internal permission to monitor a Norwegian person's communications equipment when the person is abroad. Here the legislation does not require external permission from the court, as required for PST in relation to communications control.

In its oversight of NIS, the Committee is particularly concerned with avoiding violations of the statutory prohibition against monitoring or in other covert manner procuring information concerning Norwegian natural persons or legal entities on Norwegian territory, see section 4 subsection 1 of the Intelligence Service Act.

The legal status of Norwegian legal entities located abroad is not regulated by the Intelligence Service Act, but the service is still under an obligation to respect the rights in the European Convention on Human Rights (ECHR), including Article 8 of the Convention regarding the right to respect for privacy. In 2013, the Ministry of Defence adopted provisions regarding collection of information relating to Norwegian persons outside Norwegian territory.[54] Three conditions must be met in order for NIS to be able to monitor or in other covert manner procure information about Norwegian persons abroad. First, the procurement must be part of NIS' performance of statutory tasks. It must then be possible for the information retrieved to be stored by NIS pursuant to section 4 subsection 2 of the Intelligence Service Act.[55] Finally, the retrieval must be considered necessary following a proportionality assessment, balancing the considerations of securing important national interests against the consequences for the person who is the subject of the retrieval. This is why also this is an important focus of the Committee's oversight.

6.2 The Committee's access to NIS' documents

In 1999, the Storting adopted a plenary decision for a special procedure to apply to disputes about access to NIS documents, without amending the Act and Directive.[56] The Storting's 1999 decision was based on the particular sensitivity associated with NIS' sources, the identity of persons with roles in occupation preparedness and particularly sensitive information received from cooperating foreign services. In the 2013 annual report, the Committee stated that it had been accordingly cautious in the practice of its inspection of NIS. The Committee pointed out that the situation is challenging and gives cause for concern in light of the Committee's oversight responsibility. The Committee accordingly conducts less extensive oversight of NIS than the other EOS services.

The Committee is awaiting the Storting's conclusion regarding the fundamental question of whether the provisions regarding the Committee's right of access in legislation and directives should also fully apply to NIS or whether the Storting's resolution from 1999 shall be sustained.[57]

In its annual reports for 2012 and 2013, the Committee stated that it was in a dialogue with NIS regarding practical solutions for searches in the service's computer systems. The dialogue have led to the Committee being free to search the service's systems since May 2014, with the exception of information that NIS itself considers «particularly sensitive information».[58] According to the information provided, only a few operations and documents are withheld from the

54 More detailed provisions for NIS' retrieval of information about Norwegian persons abroad and for surrender of personal data to foreign cooperating services. Laid down by the Ministry of Defence on 24 June 2013, pursuant to section 17 of the Directive regarding the Norwegian Intelligence Service. The Directive can be found at the Lovdata website.

55 It follows from section 4 subsection 2 of the Intelligence Service Act that NIS only can «hold information concerning Norwegian physical persons or legal entities when such information is directly associated with the duties of the Norwegian Intelligence Service pursuant to section 3 or is directly associated with such persons' work or assignments for the Norwegian Intelligence Service.»

56 See Document No. 16 (1998–99), Recommendation to the Storting No. 232 (1998–99) and the minutes and resolution by the Storting of 15 June 1999.

57 See chapter VII section 2 of the 2013 annual report.

58 NIS' unclassified definition: «Information about Norwegian and foreign sources, persons in and operational plans for occupation preparedness, and a small number of particularly sensitive operations is 'particularly sensitive information'.»

Committee. The practical facilitation of the Committee's access has made oversight of NIS far more thorough. NIS has accordingly facilitated the Committee's access to the service's computer systems.

6.3 Follow-up of the Committee's investigation of information about Norwegian sources, etc. at NIS

In 2013, the Committee submitted a special report to the Storting about its investigation into information about Norwegian NIS sources.[59] In the report, the Committee pointed out that NIS' legal foundation for processing sensitive personal data about the sources' close relatives was dubious, that it was difficult to see that the service could process other information about potential sources than necessary for reasons of documentation, and that the service had occasionally processed information that appeared to be irrelevant and/or unnecessary. The service was accordingly asked to follow up the need for a clearer legal authority for processing information about sources' close relatives.

In the 2013 annual report, the Committee stated that it would follow up the clarification of the legal authority.

In June 2014, the Committee received a copy of a letter from the Ministry of Defence to NIS where the Ministry provided an assessment of the legal authority for processing sensitive personal details belonging to third-parties in connection with use of sources.[60]

The Ministry of Defence concluded that section 4 subsection 2 of the Intelligence Service Act provides adequately clear legal authority for the processing of sensitive personal data from third-parties in connection with use of sources. The Ministry accordingly pointed out that without an explicit wording, other legal sources are key to the assessment, including the purpose, preparatory works, practice and real considerations. The Ministry's specific justification was as follows:

> «The purpose of section 4 subsection 2 of the Intelligence Service Act is to allow the service to store information also about Norwegian citizens when such information has a direct link to the source. The legislator has not imposed any restrictions on the type of information covered by the provision. The need to be able to process sensitive personal data about third-parties who have such a direct link to and are critical to the service's ability to use a source was given great emphasis in the assessment. In the preparatory works to the Intelligence Service Act, reference is made to the prohibition on retrieval of information about Norwegian citizens pursuant to section 4 of the Intelligence Service Act only focusing on covert retrieval. Sensitive personal data stored according to section 4 subsection 1 subsection 2 must not be considered covertly retrieved as the service receives it from the sources themselves, and it therefore is not covered by the general prohibition in section 4 subsection 1, which in turn is the basis for the exemption regarding storage of information pursuant to subsection 2. The assessment has also placed emphasis on the long-standing practice at the service of storing such information in connection with using sources. The Ministry has noted that this practice has become even further entrenched, as the procedures for use of sources and information associated with source use were presented in writing after the specialized archive case.»

The Ministry further believed that also the consequences in terms of privacy are of importance to the matter of the legal authority. It accordingly stated that very few people within NIS have access to the archive in question, where such sensitive personal data is stored, and that the information kept will not be linked to other registration about the third-party in ques-

Photo: Torgeir Haugaard / Forsvaret

tion, but only to the source in question. There thus would not be a systematic collation of information about a third-party. The Ministry also pointed out as an aspect of the matter that information linked to using sources, except for identification of the sources themselves, is covered by the oversight of the EOS Committee.

Finally, the Ministry made reference to it being an absolute condition that the general requirements in the Personal Data Act regarding use for explicit purposes, including the requirement of deletion, necessity and relevance fully apply to the service's processing of personal data in general, and particularly to sensitive personal data. The Ministry therefore expected the service's internal rules and guidelines regarding use of sources to reflect the conditions for processing of personal data and that the service had clear procedures and guidelines for internal control.

The Committee notes that the Ministry of Defence does not agree that the legal authority for processing sensitive information about the source's close relatives is dubious, and notes the Ministry's assessments on this point.

The Committee will continue to monitor NIS' processing of sensitive personal data about sources' close relatives and other third-parties when necessary, including pointing out any unclear issues related to the legal authority. NIS has now made it possible for the Committee to perform such monitoring at any time, without the service first having to remove information that can identify the sources. This makes the oversight work easier.

6.4 NIS' procedures for deletion of operational information

Following an inspection of NIS, the Committee asked about its procedures for deletion of information processed in its operational activities. The question was in relation to both a specific case, and was raised on general grounds.

In the Committee's closing letter to NIS, it noted the service's acknowledgement that the consideration of documentation and subsequent opportunities for oversight should not take precedence ahead of the consideration of information not being stored longer than necessary, based on the purpose.[61] This resulted in information about a person in the specific case being deleted.

The Committee also noted that practice in this type of case will change, and that the change in practice has been expressed in the service's guidelines for registration and deletion of information about Norwegian persons in a system for technical information retrieval. The Committee was positive towards the service having drawn up such guidelines for deletion, and towards the principles in the guidelines applying accordingly to storage of information in other information systems. NIS wrote that the service will consider developing general rules for deletion of operational information, especially for information about Norwegian physical persons and legal entities. The Committee stated that it looks forward to such rules.

The Committee also stated that it could not see that NIS had directly answered its questions regarding how NIS ensures that the service does not process personal data that is no longer considered necessary, based on the purpose of the processing.[62] However, the service stated that it would hardly be relevant to introduce a corresponding regime as for PST, with processing and deletion procedures based on deadlines (e.g. the five-year rule). The Committee stated that there are good reasons in favour of the service having a regime that ensures that the aforementioned requirement in the Personal Data Act is met.

The Committee will ask for further details about this in 2015.

6.5 Violation of the prohibition in section 4 of the Intelligence Service Act

In 2014, the Committee was notified that NIS had erroneously surveilled a Norwegian person for four months after the person returned to Norway from abroad. However, the surveillance did not lead to the procurement of any information about the person's communication. The deviation was due to the collection not being stopped in one of the service's systems. NIS has introduced new routines in order to prevent this from happening again.

The Committee expects NIS to provide notification of such deviations in the future.

In another case the Committee criticized NIS for having begun information retrieval from a Norwegian citizen in violation of section 4 of the Intelligence Service Act, which prohibits covert information retrieval from Norwegian persons in Norway. However, the service had not procured information about the person in question during the periods in question; a total of 47 days.

59 Document 7:1 (2013-2014).

60 The Ministry of Defence informed the Storting about the assessment in connection with its review of the Committee's 2013 annual report.

61 See section 11 subsection 1 (e) of the Personal Data Act and section 28 of the Security Act.

62 Ibid.

The Committee wrote the following in its closing remarks to NIS:

> «The Committee has ... found reason to criticize NIS for having monitored a Norwegian citizen on Norwegian territory in violation of section 4 of the Intelligence Service Act. NIS placed [the person] under collection [date], even though the service already on [date] received information that [the person] had returned to Norway on [an earlier date]. The Committee notes accordingly that it is also clear from the minutes from the service's update meeting with PST ... [date] that PST provided information that [the person] had returned on [date], without the retrieval stopping. ...
>
> With reference to the two other above-mentioned periods [the person] was under retrieval while [the person] was in Norway, the Committee wishes to point out that the flow of information between PST and NIS does not appear to have worked, as PST could have informed NIS earlier about [the person's] return to Norway. The Committee expects the flow of information between the services to be better than in this case, with a view to providing timely information about relevant persons' movements in and out of Norwegian territory. In a letter from hete to PST today, the Committee has pointed this out.
>
> With reference to NIS' information that «nothing actually was collected regarding the person during the period in which the person was in Norway», the Committee notes that the severity of the error was reduced in fact, but not in principle.
>
> The Committee notes that the service makes reference to «the internal flow of information having improved considerably after this time», and expects the service to actively work to prevent persons' information from being retrieved while they are on Norwegian territory, in violation of the service's legal foundation.»

6.6 Inspection of NIS' archives and registers in connection with complaints

The Committee searches the services' archives and registers as soon as possible after receiving a complaint regarding illegal surveillance.[63] The services are routinely asked to conduct their own investigations in both electronic and physical archives and registers, and for any documents, registrations and records to be sent to the Committee. The practice is based on confidence that the services perform complete investigations – also in parts of information systems and archives that the Committee is unfamiliar with.

In connection with a complaint, NIS reported that the complainant was not registered in the service's archives and registers. However, the Committee had hits on the complainant's name in seven documents when it conducted its own searches of the service's computer systems. The service apologized for the matter to the Committee, and stated that the reason for the error was that the access rights to the computer directories where the documents were located were not updated, so that the personnel who had searched for the complainant's name had been unsuccessful. The service took immediate steps to prevent this from happening again.

In a letter to the service in February 2015, the Committee noted that it was very unfortunate that lack of access rights led to no hits on the complainant when the service investigated the archives and registers. With reference to the fact that the Committee was unable to freely search the service's systems until the beginning of 2014, it was pointed out that these defects in theory may have led the Committee to close other complaints cases without the cases having been adequately illuminated. However, the Committee pointed out that it did not have reason to believe that this had been a conscious action on the part of the service or that information had been withheld from the Committee's oversight. The Committee has subsequently run searches on all people who filed a complaint with it before 2014. The searches gave no reason for follow-up.

The matter had no impact on the Committee's processing of the concrete complaint, which was closed without criticism of the service.

6.7 Complaint sent to the Committee

The Committee found matters that resulted in censure of the service in one complaint regarding illegal surveillance. The Committee was prevented from giving the complainant more information than that the complaint led to censure of the service.

The Committee finds it to be highly problematic that it can only give complainants a limited justification of the Committee's censure of NIS regarding complaints.

63 At present this is not done for complaints regarding security clearance decisions, as the Committee does not have adequate access to the computer system that processes security clearance cases. Read more about this in point 4.7.

7.
Oversight of other EOS services

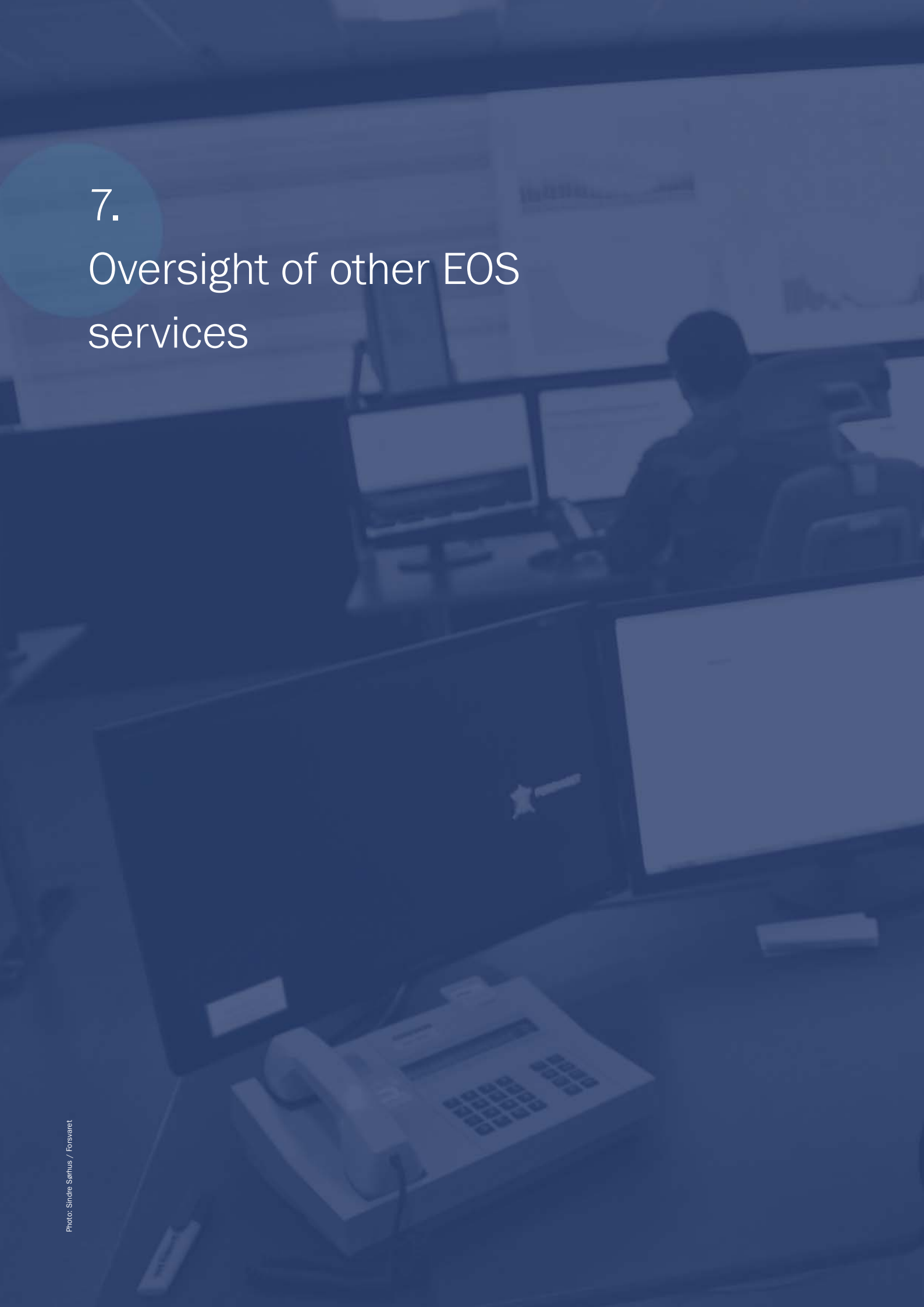


Photo: Sindre Sørhus / Forsvaret

7.1 General information about the oversight

The Committee continuously oversees the intelligence, surveillance and security services carried out by, under the control of or on behalf of public authorities.[64] In other words, the oversight area is not linked to particular organizational entities, but is defined by function.

Pursuant to section 11 (2-e) of the Oversight Act, the Committee must annually inspect at least two of NIS' stations and/or security and intelligence functions in military staffs and units, and the personnel security service of at least two ministries/agencies.

In 2014, the Committee inspected the security and intelligence functions of the Intelligence Batallion, and the personnel security service at the Norwegian Defence Estates Agency.[65]

The inspection of the Intelligence Battalion was prepared by the secretariat before the inspection, partly through searches of the Battalion's computer systems. The Committee has not prepared such inspections this way before.

7.2 The Committee's access to FISBasis

The 2012 and 2013 annual reports stated that the Committee does not have actual access to the Armed Forces' FISBasis systems, and that the Armed Forces Staff had been asked to give the Committee general access to these systems.[66] Reference was made to section 4 subsection 1 of the Oversight Act stating that in order to perform its office, the Committee may «demand access to the administration's archives and registers, premises, and installations of all kinds».

In 2014, the Committee discussed practical matters related to user access with the Norwegian Cyber Force, which took responsibility for drawing up a procedure to describe solutions for the Committee's access to FISBasis. Based on the lack of progress in the case, the Committee asked the Chief of Defence for immediate clarification of the Committee's user access.

The Committee expects satisfactory access to FISBasis to be set up within a short period of time.

7.3 Follow-up of the inspection of the personnel security service at the Ministry of Justice and Public Security

The Committee inspected the personnel security service at the Ministry of Justice and Public Security in 2014. During the inspection, the Committee was presented with a number of security clearance cases. Based on the review of the cases, the Committee questioned the clearance authorities' compliance with the requirements regarding written documentation of case processing in the Security Act. In its answer to the Committee, the Ministry confirmed that in some cases documentation in accordance with the requirements in the Security Act had not been written. The Ministry told the Committee this could be traced to matters following the 22 July 2011 terrorist attack, and further stated that measures had been taken to remedy the situation. In its closing letter to the Ministry, the Committee stated that when inspecting security clearance cases, it is concerned with following the guarantees regarding due process in the rules, including the requirement of written communication. In certain cases the Committee criticised the Ministry for not having drawn up internal explanations or written minutes after security interviews.[67]

In past annual reports, the Committee has pointed out that the assessments and the result of comparable security clearance cases vary considerably among the different security clearance authorities. The inspection of the personnel security service at the Ministry of Justice and Public Security showed that the Ministry's assessments and decisions in several cases deviate from the practice among other security clearance authorities. This is unfortunate from the perspective of equal treatment, and the Committee informed NSM as the general authority of the result of the inspection. The Committee assumes that NSM's heralded experience archive in security clearance cases will contribute to more equal treatment.

After closing the case, the Committee was notified by the Ministry that changes would be made to the case processing practice, in order to comply with the requirements in the Security Act regarding written communication. The Ministry also stated that the case processing capacity in the personnel security service was strengthened on 1 January 2015.

7.4 Spot checks at the Post and Telecommunications Authority

In 2014, the Committee conducted spot checks of security clearance cases decided by the Post and Telecommunications Authority (PT)[68]. Based on the review of the cases, the Committee asked questions about the authority's case processing time in cases where a security interview had been conducted. In its answer to the Committee, the authority confirmed that the total case processing time in the cases in question was one to two years. The authority explained that this was due to the staffing situation, and stated that it would consider taking action.

The Committee stated in the closing letter that a case processing time of up to eighteen months before a security interview and up to two years before a decision is made is unfortunate, and cannot be accepted with the reasons given by the Post and Telecommunications Authority. The Committee stated that such cases must be given greater priority. The Committee underlined the importance of decisions regarding security clearance, which can be critical to an individual's ability to perform their work. The Committee expected the authority to take action to remedy the situation.

After closing the case, the Post and Telecommunications Authority told the Committee that it had decided to increase staffing in the area with one man-labour year, through a temporary increase in the ceiling on the number of posts. In the view of the authority, this will reduce the case processing time in cases with a security interview to an acceptable level.

64 See section 1 subsection 1 of the Oversight Act.

65 In 2014, the Committee also inspected NIS' technical information activities at the Armed Forces Experiment Station Vadsø – see point 6.1.

66 The committee has requested access to FISBasis LIMITED/UNCLASSIFIED and FISBasis SECRET / NATO SECRET.

67 See section 25 final subsection of the Security Act and section 4-2 subsection 2 of the Personnel Security Regulations.

68 On 1 January 2015 the Post and Telecommunications Authority changed its name to the Norwegian Communications Authority (Nkom).

8.
Proposed amendments to the oversight act and the oversight directive

The Committee proposes some amendments to the Oversight Act and the Oversight Directive.

First, it proposes the introduction of an official short title for the Oversight Act and the Oversight Directive. Second, it proposes amendments to the Oversight Directive in order to remedy reference errors and FSA's name.

The following amendments are proposed:

1. The following amendments are proposed to Act No. 7 of 3 February 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services (amendments underlined):

   The title of the Act may be:

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

2. The following amendments are proposed to Directive No. 4295 of 30 May 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services (EOS) (underlined):

   The title of the Directive may be:

   Directive No. 4295 of 30 May 1995 relating to the Monitoring of Intelligence, Surveillance and Security Services (the EOS Oversight Directive).

   Section 11 (1-d) and (2-d) may be worded as follows:

   d) For the Norwegian Defence Security Agency: to oversee that the agency's exercise of personnel security and other security services is kept within the frame of the act and regulations and the agency's formal tasks, and otherwise ensure that injustice is not exercised against any party.

   Section 11 (2-d) may be worded as follows:

   d) three annual inspections of the Norwegian Defence Security Agency, with a review of the agency as a security clearance authority, and such inspection of other security services as required.

   Section 13 (3-e) and (3-f) may be worded as follows:

   e) specification of any measures that have been requested and their results, see section 7 subsection 5.

   f) a presentation of any protests pursuant to section 6.

9. Appendices

Appendix 1 – Glossary

Authorization
The decision that a security-cleared person will be given access to information with a specific classification level.

Avertive investigation
Investigation in order to avert the commission of a crime.

Classified information
Information that must be protected for security reasons, pursuant to the rules in the Security Act. Information labelled with a classification level, for example CONFIDENTIAL.

Covert coercive measures
Investigative measures the suspect is unaware of, for example communications control, covert audio surveillance and secret searches.

CTG
The Counter Terrorism Group (CTG) is a European counter terrorism cooperation forum between the security services in the EU, and Norway and Switzerland.

Datascript
A datascript is a program that for example is constructed to automatically locate registrations that are ready for a manual review in accordance with the requirement of five-year assessment.

Directory structure
Windows Explorer makes it possible to view the directory structure of the hard drives / network drives, including all files processed there. For example the «I directory».

DocuLive
An archive and case processing system.

Dropping
The decision to close a case without making a decision regarding the merits.

The five-year rule
The requirement that PST's intelligence registration entries must be reassessed if no new information has been added during the past five years.

Information processing
Any form of electronic or manual processing of information.

Intelligence register
Register containing intelligence data that is deemed necessary and relevant in order for PST to perform its duties. PST uses the Smart intelligence register.

Intelligence registration
Processing of information deemed necessary and relevant for PST to perform its duties, and which does not qualify for establishment of or processing in a preventive case.

Investigation case
Case established in order to discover whether a crime has been committed within PST's area of responsibility.

Preventive case
Case established in order to investigate whether someone is preparing a crime which it is PST's duty to prevent.

Security clearance authority
Public body with the authorization to determine whether a person should receive security clearance.

Security clearance case
A case where a decision is made regarding a request for security clearance, which requires an assessment of a person's suitability with respect to security.

Mimir
Case processing tool used in security clearance cases.

The PEACE model
Technique for conducting police interviews. Security interviews are based on a version of the PEACE model that is adapted to security interviews.

Personnel security
Actions, measures and assessments to prevent persons who may represent a security risk from being placed so that the risk is actualized.

Period of observation
Decision regarding the time when a request for security clearance of an individual can be resubmitted.

Person concerned
The person for whom security clearance has been requested.

Personal data
Information and assessments that are linked to an individual.

Personnel security archive
Archive for storage of personnel security cases.

Requesting authority
A body that requests vetting in its role of authority or on behalf an authority.

Security clearance
Decision made by a security clearance authority about a person's presumed suitability with respect to security for a specific classification level.

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

SIS
Schengen Information System (SIS).

Smart
PST's intelligence register.

Smartsak
PST's tool for preventive and investigative cases.

TSC
The Terrorist Screening Center (TSC) is part of the FBI. Its purpose is to identify suspects or potential terrorists.

Vetting
Procurement of relevant information in order to assess an application for security clearance.

Appendix 2 – Meetings, visits and conferences, etc.

The following is a presentation of meetings, visits, seminars, conferences, etc. attended by the Committee and its secretariat in 2014.

Breakfast seminar on data protection

In January 2014, the Committee chair attended the «Data protection – Status and trends» breakfast seminar at the House of Literature in Oslo. The seminar was organized by the Norwegian Data Protection Authority and the Norwegian Board of Technology.

Panel debate about Edward Snowden

In February 2014, Theo Koritzinsky attended the panel debate «Snowden: Hero or traitor?». The panel debate was part of the 2014 Human Rights Week, which was organized by Amnesty International at the Faculty of Law, University of Oslo.

Lecture at NSM's security conference

In March 2014, the Committee chair gave a lecture on democratic oversight of the EOS services at NSM's security conference. The purpose of this annual security conference is to provide professional updating in the form of lectures and demonstrations for enterprises that are concerned with preventive security.

Meeting with new Minister of Defence

In March 2014, the Committee met with Minister of Defence Ine Eriksen Søreide. The reason for the meeting was to present the EOS Committee's members, and to inform the Minister about the Committee's activities, etc.

Panel debate on surveillance and freedom of the press in Norway

In connection with World Press Freedom Day, in April 2014 the Committee chair participated in a panel date on surveillance and freedom of the press in Norway. The debate was organized by the Freedom of Expression Foundation, the Norwegian Union of Journalists, Norwegian PEN, the Norwegian Press Association, the Association of Norwegian Editors, IPI Norway and the Norwegian National Commission for UNESCO.

Data protection conference in Brussels

Three employees of the Committee's secretariat attended the «Annual Conference on Data Protection in the EU 2014» in April 2014 in Brussels. The two-day conference was organized by the Europäische Rechtsakademie / Academy of European Law (ERA).

Meeting with new Minister of Justice and Public Security

In April 2014, the Committee met with Minister of Justice and Public Security Anders Anundsen. The reason for the meeting was to present the EOS Committee's members, and to inform the Minister about the Committee's activities, etc.

Lecture to members of the Storting

In May 2014, the Committee chair gave a lecture on democratic oversight of the EOS services at a seminar for members of the Storting about the Storting's oversight function and external oversight bodies.

Visit from a delegation from Moldova

In May 2014, the Committee welcomed a delegation from the national security committee of Moldova's parliament. The visit was part of a two-day study trip to the Storting. The Committee, which is responsible for oversight of the security sector in Moldova, wanted to learn how Moldova can perform parliamentary oversight of the government and administration.

Conference in London

In July 2014, Theo Koritzinsky attended the «International Intelligence Review Agencies Conference» (IRAAC) in London.

The conference is held every two years, and serves as a forum for presentation and discussion of issues of common interest in the oversight of security and intelligence services.

Lecture to the Hurum Rotary Club

In August 2014, the Committee chair gave a lecture about the EOS Committee to the Hurum Rotary Club.

Secretariat meeting with the Norwegian Data Protection Authority

In September 2014, the Committee's secretariat met with the Data Protection Authority in order to discuss certain matters. This included use of big data analysis and the new Police Register Act.

Lecture at the Norwegian Defence Command and Staff College

In September 2014, Theo Koritzinsky gave a lecture on the EOS Committee for Master's students on an intelligence course at the Norwegian Defence Command and Staff College.

Lecture to the Kongsberg Rotary Club

In September 2014, the Committee chair gave a lecture about the EOS Committee to the Kongsberg Rotary Club.

Visit from a delegation from Montenegro

In October 2014, the Committee received a visit from a delegation from the national security committee of Montenegro's parliament. The visit was part of a three-day study trip to the Storting. The purpose of the visit was to see how parliamentary oversight is conducted in Norway, and how Norway handles the security challenges that also face Montenegro.

Lecture to the Bergen Young Liberal Party

In November 2014, the secretariat chair gave a lecture at a meeting for members of the Bergen Young Liberal Party. As part of the monthly topic, which was international politics and security, the group wanted a lecture from the Committee on the intersection between intelligence, security and data protection.

Meetings with the evaluation committee of the EOS Committee

The Committee held two meetings with the evaluation committee in 2014, in September and October 2014, respectively.

Appendix 3 – Personnel

The secretariat of the EOS Committee was made up of the following personnel on 31 December 2014:

Secretariat chair	Henrik Magnusson
Senior legal adviser	Silje Sæterdal Hanssen
Senior legal adviser	Steinar Sollerud Haugen
Senior legal adviser	Ole Henrik Brevik Førland
Legal adviser	Øivind Fredlund
Legal adviser	Rozemarijn van der Hilst-Ytreland
Senior social sciences adviser	Njord Wegge
Senior administrative adviser	Lise Enberget
Administrative secretary (temporary)	Tobias Grimstad

On 31 December 2014, administrative secretary Heidi Bjerkan was on leave from her position. Kjetil Otter Olsen has been engaged as a technical expert on an hourly basis. The person in the newly-created technologist position will begin working in June 2015.

Appendix 4 – Act relating to the Oversight of Intelligence, Surveillance and Security Services

Act No. 7 of 3 February 1995

Section 1. The oversight agency and the oversight area

The Storting shall elect a committee for the oversight of intelligence, surveillance and security services carried out by, under the control of or on the authority of the public administration.

Such oversight shall not apply to any superior prosecuting authority.

The Public Administration Act and the Freedom of Information Act shall not apply to the activities of the Committee, with the exception of the Public Administration Act's provisions concerning disqualification.

The Storting shall issue an ordinary directive concerning the activities of the Oversight Committee within the framework of this Act and lay down provisions concerning its composition, period of office and secretariat.

The Committee exercises its mandate on an independent basis and independently of the Storting within the framework of the law and the Directive. The Storting may nevertheless by an ordinary plenary decision instruct the Committee to undertake specified investigations within its oversight mandate under observation of the rules and within the framework that otherwise apply to the Committee's activities.

Section 2. Purpose

The purpose of the oversight is:

1. to ascertain and prevent any exercise of injustice against any person, 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 involve undue damage to civic life,
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 purpose is purely to oversee. The Committee may not instruct the bodies it oversees or be used by these for consultations.

Section 3. The responsibilities of the Oversight Committee

The Committee shall regularly oversee the practice of intelligence, surveillance and security services in public and military administration.

The Committee shall investigate all complaints from persons and organisations. The Committee shall on its own initiative deal with all matters and factors 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 2.

Section 4. Right of inspection, etc.

In pursuing its duties, the Committee may demand access to the administration's archives and registers, premises, and installations and of all kinds. Establishments, etc. that are more than 50 per cent publicly owned shall be subject to the same right of inspection.

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.

Section 5. 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 of 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 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 8 and 9.

Section 6. Ministers and ministries

The provisions laid down in Sections 4 and 5 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.

Section 7.

(Repealed by the Act of 3 Dec. 1999 no. 82 (in force from 15 Oct. 2000 in acc. with Decree of 22 Sep. 2000 no. 958).)

Section 8. Statements and notifications

1. Statements to complainants shall be unclassified. Information concerning whether any person has been subjected to surveillance activities shall be regarded as classified unless otherwise decided. Statements to the administration shall be classified according to their contents.

   The Committee shall decide the extent to which its unclassified statements or unclassified parts of statements shall be made public. If it is assumed that making a statement public will result in revealing the identity of the complainant, the consent of this person shall first be obtained.

2. The Committee submits annual reports to the Storting about its activities. Such reports may also be submitted if factors are revealed that should be made known to the Storting immediately. Such reports and their annexes shall be unclassified.

Section 9. Duty of secrecy, etc.

With the exception of matters provided for in Section 8, the Committee and its secretariat are bound to observe a duty of secrecy unless otherwise decided.

The members of the Committee and the Committee Secretariat are bound by rules concerning the handling of documents etc. that must be protected for security reasons. They must have top level security clearance, both nationally and pursuant to treaties to which Norway is a signatory. The Presidium of the Storting is the security clearance authority for the Committee's members. The vetting of personnel is carried out 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 com-

petent agency or ministry. The administration's decision is binding on the Committee.

Section 10. Assistance etc.
The Committee may engage assistance.

The provisions of the Act shall apply correspondingly to persons engaged to assist the Committee and to legal representatives appointed pursuant to Section 7. However, such persons shall only be authorised for a level of security classification appropriate to the assignment concerned.

Section 11. Penalties
Wilful or grossly negligent infringements of Section 4, first and third subsections of Section 5, first and second subsections of Section 9 and the second subsection of Section 10 of this Act shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.

Section 12. Entry into force
This Act shall enter into force immediately.

Appendix 5 – Directive relating to oversight of the intelligence, surveillance and security services (EOS)

Issued pursuant to section 1 of Act No. 7 of 3 Ferbruary 1995 relating to the Oversight of Intelligence, Surveillance and Security Services.

Section 1. On the Oversight Committee and its secretariat
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. Steps should be taken to avoid replacing more than four members at the same time.

The members of the Committee shall have the highest level of security clearance and authorisation, both nationally and according to treaties to which Norway is a signatory.

Remuneration to the Committee's members shall be determined by the Presidium of the Storting.

The chair of the Committee's secretariat shall be appointed and the chair's remuneration stipulated by the Presidium of the Storting on the basis of a recommendation from the Committee. Appointment and stipulation of the remuneration 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 to be approved by the Presidium of the Storting. The provision in the second subsection applies similarly to all employees in the secretariat.

Section 2. Quorum and working procedures
The Committee has a quorum when five members are present. The Committee shall as a rule function jointly, but may divide itself during inspection of service locations or installations.

In connection with particularly extensive investigations, the procurement of statements, inspections of premises, etc. may be carried out by the secretary 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 hearings, as mentioned in this Section, the Committee may engage assistance. It is then sufficient that the secretary or a single member participates.

The Committee may also otherwise engage assistance when special expertise is required.

Persons who have previously functioned in the intelligence, surveillance and security services may not be engaged to provide assistance.

Section 3. 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 made unless communicated in writing.

Section 4. Oversight limitations etc.
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 above when special reasons so indicate.

The oversight activities should be exercised so that they pose the least possible disadvantage for the current activities of the services. 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 5. Access limitations
The Committee shall not seek more extensive access to classified information than warranted by its oversight purposes. Insofar as possible, the concern for protection of sources and safeguarding of information received from abroad shall be observed.

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 9. If in doubt, the provider of the information should be consulted.

Section 6. Disputes concerning access to information and oversight
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. Protests following such decisions may be submitted by the head of the respective service and the Chief of Defence.

The protest shall, as mentioned here, be included in or enclosed with the Committee's annual report.

Section 7. On the oversight and statements in general

The Committee shall adhere to the principle relating to subsequent oversight. The Committee may, however, demand access to and make statements about current cases.

The Committee shall base its oversight and the formulation of its statements on the principles set down in Section 10, first subsection and Section 10, second subsection, first, third and fourth sentence, and Section 11 of the Act concerning the Storting's Ombudsman for public administration. The Committee may also propose improvements in administrative and organisational arrangements and routines where these can make oversight easier or safeguard against injustice being done.

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 8. On complaints

On receipt of complaints, the Committee shall conduct such investigations of the administration as are appropriate in relation to the complaint. The Committee shall decide whether the complaint gives sufficient grounds for further action before making a statement.

Statements to complainants should be as complete as possible without revealing classified information. Statements in response to complaints against the Police Security Service concerning surveillance activities shall however 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 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. Statements concerning complaints shall also otherwise always be sent to the head of the service against which the complaint is made.

Section 9. Procedures

Conversations with private individuals shall be in the form of an examination unless they are meant to merely 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 5 of the Act relating to the Oversight of Intelligence, Surveillance and Security Services. In connection with examinations that may result in criticism of 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 these are unclassified or the person has authorised access.

Section 10. Investigations at the ministries

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

Should the 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. Inspection

1. Responsibilities for inspection are as follows:
   a) For the intelligence service: to ensure that activities are carried out within the framework of the service's established responsibilities, and that no injustice is done to any person.
   b) For the National Security Authority: to ensure that activities are carried out within the framework of the service's established responsibilities, to oversee clearance matters in relation to persons and enterprises for which clearance has been denied, revoked, reduced or suspended by the clearance authorities, and also to ensure that no injustice is done to any person.
   c) For the Police Security Service: to oversee that the service's handling of preventive cases and investigations, its use of concealed coercive measures, its processing of personal data, and the exchange of information with domestic and foreign collaborative partners is carried out in accordance with current regulations, and meets the requirements for satisfactory routines within the

framework of the purpose stated in Section 2 of the Act.

d) For the Defence Security Section: to oversee that the service's exercise of personnel security clearance activities and other security clearance activities are kept within the framework of laws and regulations and the service's established responsibilities, and also to ensure that no injustice is done to any person.

e) For all services: to ensure that the cooperation and exchange of information between the services is kept within the framework of service needs and applicable regulations.

2. Inspection activities shall, as a minimum, involve:
   a) half-yearly inspections of the Intelligence Service, involving accounts of current activities and such inspection as is found necessary.
   b) quarterly inspections of the National Security Authority, involving a review of matters mentioned under 1 b and such inspection as is found necessary.
   c) Six inspections per year of the Central Unit of the Police Security Service, involving a review of new cases and the current use of concealed coercive measures, including at least ten random checks in archives and registers at each inspection, and involving a review of all current cases at least twice a year.
   d) Three inspections per year of the Defence Security Service, including a review of the agency as a clearance authority, and a review of other security-related activities as found necessary.
   e) annual inspection of at least four police districts, 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.
   f) inspection of measures implemented on its own initiative by the remainder of the police force and by other bodies or institutions that assist the Police Security Service.
   g) other inspection activities indicated by the purpose of the Act.

Section 12. Information to the public

Within the framework of the third paragraph of Section 9 of the Act cf. Section 8, paragraph 1, the Committee shall decide what information shall be made public concerning matters on which the Committee has commented. When mentioning specific persons, consideration shall be given to protection of privacy, including persons not issuing complaints. Civil servants shall not be named or in any other way identified except by authority 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.

Section 13. Relationship to the Storting

1. The provision in Section 12, first subsection, correspondingly applies to the Committee's notifications and annual reports to the Storting.
2. Should the Committee find that the 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.
3. By 1 April every year, the Committee shall report its activities in the preceding year to the Storting.
   The annual report should include:
   a) an overview of the composition of the Committee, its meeting activities and expenses.
   b) a statement concerning implemented supervision activities and the result of said activities.
   c) an overview of complaints by type and service branch, indicating what the complaints resulted in.
   d) a statement concerning cases and matters raised on the Committee's own initiative.
   e) a statement concerning any measures the Committee has requested be implemented and what these measures led to, cf. Section 6, fifth subsection.
   f) a statement concerning any protests pursuant to Section 5.
   g) a statement concerning any cases or matters which should be put before the Storting.
   h) the Committee's general experiences from the oversight activities and the regulations and any need for changes.

Section 14. Financial management, expense reimbursement for persons summoned before the Committee and experts

1. 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.
2. Anyone summoned before the Committee is entitled to reimbursement of any travel expenses d in accordance with the State travel allowance scale. Loss of income is reimbursed in accordance with the rules for witnesses in court.
3. Experts are remunerated in accordance with the courts' fee regulations. Higher fees can be agreed. Other persons assisting the Committee are reimbursed in accordance with the Committee scale unless otherwise agreed.

NORWEGIAN PARLIAMENTARY OVERSIGHT COMMITTEE
ON INTELLIGENCE AND SECURITY SERVICES

fdesign.no

Contact information

Telephone: +47 23 31 09 30
Email: post@eos-utvalget.no
Postal address: PO box 84 Sentrum, 0101 Oslo
Office address: Akersgata 8, Oslo

www.eos-utvalget.no