# ABBREVIATED ANNUAL REPORT FOR 2012

## Preface

The Norwegian Parliamentary Intelligence Oversight (EOS) Committee is required to submit an annual report about its activities to the Storting. This abbreviated annual report for 2012 presents some of the main items in the more extensive report. You can read it on the Committee's website at www.eos-utvalget.no.

Chapter 1 describes the Committee's remit and composition. Chapter 2 provides an overview of the Committee's activities in 2012: inspections, consideration of cases the Committee has raised on its own initiative, complaint cases and some important meetings, conferences and study visits in Norway and abroad. Chapter 3 contains a brief overview of some general trends relating to the services that are of significance to the Committee's work. Chapters 4 to 7 provide information about the Committee's oversight of the different services and about some general principles that the Committee has raised with the services.

In 2012, the Committee has seen a noticeable increase in the ongoing cooperation between the Norwegian Police Security Service (PST) and the Norwegian Intelligence Service (NIS). This entails important legal challenges, among other things because the two services are governed by very different rules concerning their duties and surveillance methods. The Committee also encountered some important challenges relating to the right of inspection in 2012. Following an inspection of Telenor, the Committee has proposed a legislative amendment to clarify its right to inspect enterprises that assist PST. Moreover, both technical questions and matters of principle have been raised relating to the Committee's right to inspect NIS.

The Committee has found the services to have a consistently good understanding of its work in 2012 as well. Experience shows that oversight of the intelligence, surveillance and security services helps to safeguard individuals' due process protection and to create confidence that the services operate within their statutory framework.

## 1. The Committee's remit and composition

### 1.1 The Committee's remit

The EOS Committee is charged with continuously overseeing the intelligence, surveillance, and security services (EOS services) carried out by, under the control of or on behalf of public authorities. The EOS Committee's remit is set out in the Act relating to the Oversight of Intelligence, Surveillance and Security Services and in the Directive relating to Oversight of the Intelligence, Surveillance and Security Services. The Act and Directive were most recently amended in June 2009. The Act relating to Protective Security Services, the Act relating to the Norwegian Intelligence Service and the Instructions for Defence Security Service all refer to the Act relating to the Oversight of Intelligence, Surveillance and Security Services and state that the services are subject to oversight by the EOS Committee.

The Committee's primary function is to oversee that the EOS services do not subject individuals to unjust treatment. The Committee shall ensure that the services act within the framework of the law, directives, and non-statutory law, and respect human rights. The oversight is primarily carried out by means of inspections of the services' archives, computer systems and installations. Subsequent oversight is practised in relation to individual cases and operations. In principle, however, the Committee has full right of inspection and shall be kept continually informed about important ongoing cases. The Committee's oversight shall cause as little inconvenience as possible to the services' day-to-day activities. Particular

account must be taken of the protection of sources and information received from cooperating foreign intelligence services.

The Committee shall investigate all complaints from individuals and organisations. Any complaint or enquiry claiming that someone has been unjustly treated by the services shall be investigated in the service or services that the complaint concerns.

### 1.2 The composition of the Committee

The EOS Committee has seven members elected for a term of office of five years. The members can be re-elected. They are elected by the Storting on the recommendation of the Storting's Presidium, but the Committee works independently of the Storting on the basis of its remit. Members of the Storting cannot be members of the Committee. The Storting has emphasised diversity in the composition of the Committee, in terms of political background as well as experience from other areas of society. The Committee's members, secretariat employees and persons engaged to assist the Committee are all required to have top-level security clearance.

The chair of the Committee is Eldbjørg Løwer, former government minister and deputy head of the Norwegian Liberal Party. The deputy chair is Svein Grønnern, Secretary General of SOS Children's Villages Norway and former Secretary General of the Norwegian Conservative Party. The other committee members in 2012 were Trygve Harvold, former Managing Director of the Norwegian Legal Database Foundation, Lovdata; Gunhild Øyangen, former Member of the Storting and government minister for the Norwegian Labour Party; Theo Koritzinsky, former Member of the Storting and head of the Socialist Left Party; Wenche Elizabeth Arntzen, District Court Judge in Oslo District Court and former advocate; and Hans Johan Røsjorde, former County Governor of Oslo and Akershus and Member of the Storting for the Progress Party.

## 2. Overview of the Committee's activities in 2012

### 2.1 The inspection activities

Pursuant to Section 11 subsection 2 of the Directive relating to Oversight of the Intelligence, Surveillance and Security Services, inspection activities shall, as a minimum, comprise six-monthly inspections of the Intelligence Service headquarters, quarterly inspections of the National Security Authority (NSM), six inspections per year of the Headquarters of the Police Security Service (PST) and three of the Defence Security Agency (FSA). Inspections shall also be carried out of PST entities in at least four police districts, at least two intelligence service entities and/or intelligence/security service functions in military staffs and units, and the personnel security service of at least two ministries or government agencies outside the National Security Authority. The Committee can carry out on its own initiative inspections of other police entities and other agencies or institutions that assist PST, and otherwise such inspections as indicated by the purpose set out in the Act relating to the Oversight of Intelligence, Surveillance and Security Services.

The regulatory requirements for the Committee's inspection activities were met in 2012. One third of the Committee's inspections have targeted PST. The reason for this is the regulatory requirement for the number of inspections of that service. The Committee has conducted a total of 30 inspections, including 17 at the central level. The Committee has inspected five external and local entities in 2012: PST Rogaland, PST Midtre Hålogaland, PST Agder, PST Nordre Buskerud and the Norwegian Armed Forces' station at Andøya (FSTA). In addition, the Committee has conducted inspections of the personnel security services of the Norwegian Defence Estates Agency, the Intelligence Service, the Office of the County Governor of Rogaland and the Norwegian Post and Telecommunications Authority, as well as the security and intelligence functions of the Coastal Ranger Command at Trondenes.

Pursuant to Section 11 of the Directive relating to Oversight of the Intelligence, Surveillance and Security Services, the Committee can carry out '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'. In accordance with this provision, the Committee has in 2012 inspected the National Bureau of Crime Investigation's (Kripos) computer crime entity and Telenor's police contact centre at Fornebu. The Committee has also carried out one unannounced inspection of the Intelligence Battalion at Setermoen as part of the investigation of a complaint. The Committee's investigation resulted in criticism of the Intelligence Battalion for processing information about the complainants in violation of the Personal Data Act.

## 2.2 Complaint cases and cases raised on the Committee's own initiative

The Committee received 21 complaints against the EOS services from private individuals in 2012, compared with 21 and 29 complaints in 2010 and 2011, respectively. In addition, the Committee has received several enquiries by e-mail and telephone that have not formed grounds for opening complaint cases. The Committee has rejected some complaints on formal grounds, among other things with reference to the matter in question not falling within the Committee's oversight area or because the complaint was not sufficiently specific for the matter to be considered by the Committee. The Committee has raised 22 cases on its own initiative in 2012.

## 2.3 Meetings, visits and participation in conferences

During the year, the whole Committee or some of its members have attended meetings with various public authorities and supervisory bodies in Norway and abroad. In addition, members of the Committee and the Committee Secretariat have participated in several conferences. Some of them are listed below in chronological order.

An *internal technical seminar* was held in January 2012 in order to raise the level of technical expertise in the Committee and the Committee Secretariat. The Secretariat has also, together with a technical expert, held several meetings of a technical nature with PST and the Intelligence Service. The services have been accommodating and open to the Committee's wishes in connection with this.

The Chair of the Committee and the head of the Secretariat met with members of the *Storting's Standing Committee on Scrutiny and Constitutional Affairs* in February. The purpose of this meeting was to provide further information about the Committee's tasks and methods in connection with inspections, cases raised on the Committee's own initiative, complaint cases and projects etc. In April, the Chair of the Committee gave a talk about the Committee's oversight of security clearance cases at *the National Security Authority's seminar for security clearance authorities.*

In May, a member of the Committee participated at an *experience conference in Ljubljana, Slovenia*, attended by many oversight committees from South-Eastern Europe in particular. In the same month, two members attended the eighth *International Review Agencies Conference (IIRAC)* in Ottawa, Canada. The main topic of the conference was 'Strengthening democracy through effective review'. In May, the EOS Committee also met with the Swedish Commission on Security and Integrity Protection and the Danish Intelligence Services Committee in Oslo. The agenda included lectures by the heads of the Norwegian Intelligence Service and PST, who spoke about their experience of the EOS Committee, among other things. In July 2012 the head of the Secretariat took part in a *seminar in Geneva, Switzerland on 'Intelligence Governance'*, and gave a lecture about the Norwegian model and the Committee's relationship with the media.

In September, members of the Committee had a *meeting with the Traavik Commission*, whose remit was to evaluate PST's organisation, priorities, use of resources etc. In the same

month, members of the Committee met with *representatives of the Legal Affairs Committee of the Danish parliament, Folketinget*, who were considering new oversight arrangements for the Danish intelligence, surveillance and security services. In November, committee members and the head of the Secretariat participated in the *Intelligence Service's 70th anniversary seminar.* The Committee also held an *internal one-day seminar* that month on the topic *'The EOS Committee – an external perspective'.* In December, two secretariat employees and two committee members attended a *conference on 'Evaluating and enhancing the oversight of intelligence services in the Western Balkans'* in Ljubljana, Slovenia. The members contributed as speakers and chaired panels/debates at this conference, as they also did at several of the above-mentioned conferences. In December, the Committee also *met with representatives of the Norwegian Data Protection Authority* to discuss common challenges relating to the protection of privacy.

## 3. Some developments in 2012

Some long-term national, international and technological developments of significance to the secret services were emphasised in the annual report last year as seen in relation to the EOS Committee's 15-year history and the challenges ahead. Several of these developments and challenges have also been evident in 2012. They include the distinctions and connections between civilian and military threats and the increased cooperation between PST and the Intelligence Service, the increasing exchange of information between Norwegian and foreign services and the rapid technological development.

In 2012, two external evaluation reports and some proposals from the services themselves have influenced the debate about their work. The 22 July Commission's general recommendation was that 'The Police Security Service must develop leadership, organisational culture, work processes and objectives that are better adapted to the service's tasks, at the same time as parameters set out of consideration for democracy and the protection of privacy must continue to be respected. It is especially important to demonstrate more persistence, creativity and determination when it comes to identifying new threats'. The Traavik Commission endorsed this assessment.

The 22 July Commission also recommended that PST should show more initiative and more willingness to cooperate and share information with other agencies, including the ordinary police and the Intelligence Service. Moreover, the Commission also pointed out that the confidentiality provisions in legislation must not prevent PST from gaining access to relevant information from other agencies. It also pointed out that the legislation should make it even clearer that PST and the Intelligence Service can exchange information obtained by clandestine methods in cases where this is necessary. In line with this, the Traavik Commission claims that a lack of legal authority impedes the exchange of information and other forms of cooperation between the two services.

Based on, among other things, this criticism, the services have in 2012 proposed several amendments to legislation and other framework conditions for the purpose of enabling them to perform their duties in a better and more effective manner. In this connection, particular reference is made to the proposals put forward by PST in a letter to the Ministry of Justice and Public Security of 1 November 2011 for the purpose of covering the overall situation regarding the legal basis for counterterrorism in Norway. Among other things, this resulted in the Ministry distributing for consultation on 12 July 2012 a proposal to criminalise the preparation of terrorist acts and extend the right to use coercive measures. PST has also requested the general legal authority required to obtain information from other public authorities. Among other things, the service wants to see legislative amendments introduced that will ensure better and more predictable exchange of information between health personnel and PST about mentally ill persons who represent a threat to people in positions of

power. The Intelligence Service has proposed a clarification of the legal basis for the intelligence assistance it provides to the police. In 2012 as in previous years, the Committee has been informed that the Intelligence Service wishes to introduce new methods in its technical information collection.

# 4 The Norwegian Police Security Service (PST)

## 4.1 General information about oversight of the service

In 2012, the Committee conducted six inspections of PST Headquarters (DSE). The Committee has also inspected the PST entities in the districts of Rogaland, Agder, Midtre Hålogaland and Nordre Buskerud. The Committee receives regular briefings on the service's ongoing activities and about special topics and cases that the Committee has requested information about in advance. PST's investigation cases and prevention cases are also reviewed, as are the service's archives and registers.

Based on these inspections, the Committee has opened several cases on its own initiative. The majority of these cases concern PST's processing of registered information about individuals. *The Committee's oversight has resulted in information about approximately 120 people being deleted from PST's intelligence register in 2012.*

In the two previous annual reports, the Committee has described certain issues relating to the Committee's right to inspect PST. The reason for this was that the service had, for a time, suspended the Committee's access to certain types of cases. The Committee is not aware of any cases being withheld by the service from the Committee's oversight in 2012. *The Committee now has full independent access to the service's intelligence register Smart, its case work tool Smartsak, the archive and case processing system DocuLive and the folder structure, both during the Secretariat's preparations and during the inspections themselves.*

## 4.2 PST's use of covert coercive measures and other use of intrusive methods

Like the ordinary police, PST can request a District Court to authorise the use of covert coercive measures in *regular investigations*. Coercive measures include communications control, covert audio surveillance, technological tracking and secret searches. PST also has the legal authority to request the use of covert coercive measures to *avert* criminal offences that fall within the service's area of responsibility. Thirdly, PST can, as the only police authority with this right, also use covert coercive measures to *prevent* certain types of criminal offences. In addition, PST can use non-statutory methods that are not so intrusive that statutory authority is deemed necessary.

The Committee's inspections of PST include regular checks of the use of covert coercive measures in individual cases. It is particularly important to the Committee to check that petitions submitted by PST to the courts are in accordance with the service's need for necessary information and whether the service uses the coercive measures in the manner authorised by the court. It is also checked that such measures are discontinued if the grounds for the court's permission cease to exist. The extent of PST's use of covert coercive measures is also a matter of interest to the Committee.

In the annual report for 2011, the Committee reported a trend towards increasing use of covert coercive measures compared with previous years, particularly in prevention cases. The court-sanctioned use of coercive measures appears to have increased further in 2012. In this context, the Committee would like to point out that the Storting's intention is that covert coercive measures for preventive purposes shall be a limited supplement to be used only to prevent the most serious criminal offences.

In 2012, the Committee inspected PST's technical support entity, with particular attention being devoted to communications control, covert video surveillance and covert audio surveillance. As in previous years, the Committee has reviewed court rulings concerning the use of covert video surveillance in public places. In such cases, the court will not be shown images of how the surveillance is actually conducted. The Committee therefore actively checks whether the information provided to the district court corresponds to what is actually under surveillance, and receives image print-outs in cases where covert video surveillance has been initiated. The Committee has noted that, in several cases, PST has conducted covert video surveillance aimed at or in places that the Committee defines as private, for example a front door. The court has sanctioned the surveillance in all cases. In the Committee's opinion, it is doubtful whether the Criminal Procedure Act Section 202a authorises such video surveillance.

The Committee finds that PST generally seems to be aware of the limits that legislation and the principle of legality sets for the use of coercive measures and other measures of an intrusive nature. The Committee will continue to closely monitor PST's use of methods in its subsequent control in 2013.

### 4.3 Processing of information outside archives and registers

During the inspection of a local PST entity in 2011, the Committee found that some intelligence and case-related information was stored in separate folder structures (on the 'I area') in PST's computer network. After the inspection, the Committee asked PST about the service's practice as regards processing information outside the intelligence register Smart and the case work tool Smartsak. PST emphasised in a letter to the Committee of December 2011 that the service only had one intelligence register, and that, consequently, no intelligence information shall be processed outside Smart. The service nevertheless acknowledged that this had happened.

The Committee followed up the case in February 2012 by conducting a comprehensive search of all local PST entities' parts of the computer network. The searches showed that the extent of information processed in the folder structure was significantly greater and partly of a different and more worrying nature than the Committee's initial impression had indicated. Based on this, the Committee asked the service several follow-up questions in March 2012. PST's response of April 2012 stated that the folder structure had been investigated, and that the service '[b]ased on these investigations (…) agrees with the assessments expressed by the Committee in its letter' and that 'it [is] an undesirable situation that information is stored without being subject to the quality assurance and deletion procedures implemented in Smart'. The service also reported that a working group would shortly be appointed to prepare new case processing procedures. These procedures would clarify what is to be processed in Smart, what shall be processed in the archive and case processing system DocuLive and limitations on the use of the folder structure. It was also stated that all departments and local entities would review their information in the folder structure, and then transfer all information that could or should not be stored there to the appropriate location in Smart or DocuLive. Any remaining information would be deleted.

The Committee stated the following in its concluding remarks to the service in June 2012: 'The Committee has not been aware of the service's use of the I area in the processing of information. This practice has been inconsistent with the intention that no intelligence information shall be processed outside Smart. (…) [This] has in practice resulted in information being withheld from the Committee's oversight. (…) In its review of the folder structure, the Committee has seen several examples of information that seems to have been processed in violation of the requirements for necessity, relevance and purpose that follow from the PST Regulations Sections 13 and 14. (…) The Committee takes a critical view of the fact that PST Headquarters has not been aware of the scope of information processed in the I area, but notes that action will now be taken to remedy the current situation. (…) In the

Committee's opinion, satisfactory case processing procedures and internal control should have been in place much earlier.'

## 4.4 Inspection of archives and registers

### General information about the inspection work and its results

The archive and register inspections have comprised a significant proportion of the Committee's oversight activities in relation to PST in 2012 as well. It is particularly the requirements relating to quality of information, purpose, necessity and relevance that are subject to control by the Committee – and that information is deleted when there are no (longer) grounds for processing such information. It is also important to check that PST carries out individual assessments of the basis for registration, and that information in the intelligence register is deleted when the conditions for processing such information cease to exist.

The Secretariat conducts searches in the intelligence register Smart and other systems before each inspection of PST Headquarters. Spot checks and print-outs are presented to the Committee during inspections. An increasing proportion of the Committee's oversight takes place by computer. This has simplified and improved oversight work. It has also made it easier for the service to prepare for the inspections.

*In several cases, the Committee has pointed out that the requirement for individual assessment has not been met. The Committee's oversight of the processing of personal data in PST's registers has resulted in the service deleting information about approximately 120 people in 2012.*

### Failure to review in accordance with the five-year rule, including reviews of certain categories of persons

It follows from Section 3-7 of the guidelines for PST's processing of information that '[i]ntelligence registrations to which no new information has been added after five years shall be reviewed' and that '[t]he information shall be deleted if it is no longer required for the purpose'.

The Committee's spot checks have identified several cases in which PST had not deleted information about persons, even though the information was no longer required for the purpose of the processing.

In 2012, the Committee has criticised PST for having practised exemptions from the five-year rule without the Committee being aware of it. PST's practice has meant that information about old and deceased persons has been registered in the intelligence register for periods of up to 72 years without being reviewed. Following this criticism, PST has changed its practice and deleted nine persons from the register. *Since then, PST has endeavoured to strike off deceased persons. This has resulted in a number of persons being prepared for deletion from the register. PST is considering whether to introduce a procedure that registers deaths, so that the information about deceased persons can be subjected to extraordinary review.*

In continuation of this case, the Committee managed to clarify that PST has exempted *three* categories of person from review under the five-year rule, including the service's sources and contacts. PST stated that 'the reason why they have not been subject to such review is that they are aware of their contact with the service' and that 'continuous evaluation regimes [are] in place in both areas'. In response to this, the Committee remarked that it has seen several examples of the services' contacts being assigned several roles in the intelligence register, and that contacts can also be registered for surveillance purposes. It was pointed out that these persons may feel that their relationship with the service is a burden, and the Committee referred to concrete examples.

*In the Committee's opinion, it is unfortunate if the role of 'contact' or 'source' prevents a review being carried out under the five-year rule, given that negative information can also actually be registered about these people in the intelligence register. The Committee concluded that PST should also review sources and contacts under the five-year rule.*

**The Committee's project work**
In 2012, the Committee has examined in more detail registrations relating to two selected groups that PST monitors for preventive purposes. The registrations have been evaluated in relation to the necessity and relevance requirements in the PST Regulations Sections 13 and 14 in particular, and in relation to the PST Regulations Section 15, which reads as follows: 'Information about a person cannot be processed based solely on what is known about the person's ethnicity or national background, political, religious or philosophical conviction, trade union membership or information about health-related or sexual matters.'

*After being informed about the Committee's project work, PST stated in June 2012 that the service recognised that it was necessary to examine its registrations in the two groups in question. PST informed the Committee that the internal review showed that the service has registered persons and processed information that are not relevant to the service's performance of its duties. The Committee will submit a special report about the project to the Storting in spring 2013.*

### 4.5 Processing of intelligence information in DocuLive and Smart
In connection with the consideration of a complaint against PST for unlawful surveillance, the Committee's investigation revealed that a local PST entity processed intelligence information about the complainant in documents stored outside the intelligence register, electronically stored in the 'I area' in the PST network's folder structure, and in documents in the correspondence records system DocuLive. The latter document concerned *'Reporting of parties that threaten people in positions of power'* from local PST entities to PST Headquarters. None of these documents were found by PST itself, a fact that led to criticism from the Committee. The Committee remarked that the reporting of intelligence information via DocuLive illustrates the due process protection concerns relating to the use of DocuLive in an intelligence context, a matter which the Committee discussed in its annual report for 2010. The Committee's concern was that the requirements set out in the PST Regulations can become illusory when intelligence information is processed outside the intelligence register, particularly because it is only in Smart that intelligence information is reviewed under the five-year rule.

At the Committee's request, the service also confirmed that it will maintain focus on the use of intelligence information outside the intelligence register. The service stated that DocuLive would no longer be used to report intelligence information from district offices to PST Headquarters. In future, such reporting will take place via the intelligence register.

### 4.6 Disclosure of personal data to cooperating foreign services
PST has legal authority to disclose information about Norwegian and foreign citizens to cooperating foreign services. The Committee regularly checks that PST does not disclose personal data to foreign parties in contravention of the applicable regulatory framework or of international human rights commitments. Among other things, the Committee checks which parties information is disclosed to, that the disclosure meets a specifically defined purpose and that the consequences for individuals are proportionate to the purpose of the disclosure. The Committee also considers the nature and quality of the disclosed information. As is known, one important aspect of the Committee's oversight is to check that information is not disclosed to states that fail to respect human rights.

*On this point, the oversight in 2012 has not given grounds for criticising PST. However, the Committee will follow up matters relating to the disclosure of biometric data to foreign parties and the disclosure of information about persons that PST has no unfavourable information about. The Committee will also look more closely into whether documentation considerations are sufficiently addressed in connection with disclosure to foreign parties.*

## 4.7 PST's processing of applications for declassification and access

In all its annual reports from 2007 until the present, the Committee has described PST's processing of applications for declassification and access. The main question is whether individuals should be given access to registered information about themselves that is more than 30 years old. The Security Act's general rule is automatic declassification after 30 years at the latest. Information about whether or not an individual is registered in PST's registers is also deemed to be classified information. In several cases, PST has refused individuals information that they were not registered in the service's registers 30 or more years ago. The Committee has pointed out that even though the new Police Register Act gives PST legal authority to reject applications for access from individuals, the Security Act's general provision concerning automatic declassification after 30 years will continue to apply. In the Committee's opinion, there are no good reasons for denying access to older information in cases where the special conditions for upholding classified status for more than 30 years are not met.

The Committee contacted the Ministry of Justice in connection with this matter both in 2009 and 2010. In February 2011, the Ministry confirmed that it will examine whether 'it can be confirmed that persons are not registered in the archives or registers of the Norwegian Police Security Service (PST) in the case of inquiries concerning a possible registration period that lies far back in time'. In January 2012, the Ministry informed the Committee that no further work has been done on this matter due to the Ministry's work situation and its many duties following the terrorist attacks on 22 July 2011. The Ministry expected it to be some time before work on the matter can resume.

*The Committee contacted the Ministry of Justice and Public Security again in November 2012 to request information about the current status of this matter. The Ministry has not yet responded. The Committee feels that it is important that the question of access to old information be clarified as soon as possible, and it has put the consideration of several complaint cases on hold pending the Ministry's assessment.*

### 4.8 PST's handling of confidential communication between lawyers and clients

In connection with the Committee's review of PST's prevention cases, it questioned in two cases the legal basis for obtaining, recording and storing information originating from confidential communication between the persons in the cases and their lawyers. In one case, the Committee agreed that the receipt and processing of the information communicated to the source by the client was unproblematic in relation to considerations of protection of confidential communication between lawyers and clients. In the other case, the Committee questioned the legal basis for recording and storing a text message (SMS) sent from the client to the lawyer, which was obtained by PST by means of communications control. In its consideration of the case, the Committee noted that PST considers that the Criminal Procedure Act Section 216 g is not applicable to PST's prevention cases, but that the service 'nonetheless [finds] grounds, also in prevention cases, for complying with the principles set out in the provision and the important considerations it safeguards'. PST was therefore willing to carry out necessary deletion of the relevant documents originating from this confidential communication.

The Committee also remarked that PST should have internal procedures for processing confidential communication between lawyers and clients in connection with communications control and other covert methods of obtaining information.

## 4.9 Complaint cases

The Committee received 14 complaints against PST from private individuals in 2012, compared with eleven complaints in 2011. Most of the complaints concern allegations of unlawful surveillance. Two of the complaints were also complaints against the Intelligence Service. One complaint was also against the National Security Authority and the Defence Security Agency. All complaints that were not dismissed on formal grounds were investigated by PST. *None of the concluded complaint cases have given grounds for criticism of the service for unlawful surveillance.*

One of the complaints stated that the complainant had sent a complaint directly to PST as early as October 2010. PST neither responded to the complaint nor forwarded it to the EOS Committee as the correct addressee. It was not until a year later, when the complainant again contacted PST, that the complaint was forwarded to the Committee. The Committee reminded PST of the fundamental principle of administrative law that the administration shall reply to written enquiries in writing. *The Committee expects future enquiries received by the service concerning allegations of unlawful surveillance to be promptly forwarded to the EOS Committee, and the sender to be notified of this by PST. The service has followed up the Committee's request in connection with subsequent complaints against PST in 2012.*

The Committee's investigations in a complaint case showed that PST had not forwarded all relevant documents about the complainant, cf. section 4.5. The Committee followed up this case, and found that information sent by the service from its own archives, registers and systems in connection with complaint cases has been incomplete. This was partly because the processing of intelligence information in the 'I area' has resulted in information being withheld from the investigations and thus from oversight by the Committee. The Committee remarked that this was most unsatisfactory. The Committee then decided to examine all previous complaint cases against PST (1996–2012). On this basis, PST has facilitated searches in the folder structure on PST's network to enable the Committee to search for any information that could relate to old complaint cases that the Committee has concluded. This work will continue in 2013.

In 2012, the Committee received a complaint from a person who had been charged in a criminal case in which the investigation had made extensive use of coercive measures for avertive purposes. During the investigation, the complainant contacted PST and started a collaboration that lasted until the arrest. On the basis of this collaboration, the charge was limited to offences committed before the complainant became a PST contact. The service made audio recordings of all conversations with the complainant without informing him of this. The complainant argued that PST had omitted to inform Oslo District Court of his cooperation with PST in its petitions for authorisation to use coercive measures. On the basis of the complaint, the Committee carried out investigations in PST, among other things by submitting questions to the service in writing. PST confirmed that the service had not informed the District Court of the collaboration. In a concluding letter to PST, the Committee stated, among other things, that, in the Committee's opinion it 'warrants criticism that PST failed to inform Oslo District Court that it had entered into collaboration with [the complainant], and thus also the official counsel appointed, even though [the complainant] was still a suspect in the case'.

The complainant was informed of the criticism of PST in a concluding letter to the complainant's lawyer.

# 5 Inspection of Telenor

Telenor and other telecommunications/internet providers assist PST and the ordinary police, among others, in carrying out communications control. Telenor's police contact centre was inspected in September 2012. This centre was established in 2002, and it is open round the clock every day of the year. The Committee has previously held an orientation meeting with Telenor. The question of the Committee's right of inspection was not an issue at that time. Before the inspection in 2012, however, it was questioned whether the Committee has a right to oversee Telenor. The Committee referred to the wording of Section 11 subsection 2 of the Directive relating to Oversight of Intelligence, Surveillance and Security Services, whereby the Committee can inspect 'the remainder of the police force and other bodies or institutions that assist the Police Security Service'.

The wording of the Act relating to Oversight of Intelligence, Surveillance and Security Services Section 4 first paragraph is that the Committee 'may demand access to the administration's archives and registers, premises, and installations and of all kinds' in pursuing its duties. It is specified that ' [e]stablishments, etc. that *are more than 50 per cent publicly owned* shall be subject to the same right of inspection' (Committee's italics). The wording can give rise to doubts about the Committee's right to inspect private companies that assist PST. This raises problems in practice, since there are at present about 200 internet providers, in addition to more than 200 telecommunications providers, of which only one company, namely Telenor, is more than 50 per cent publicly owned.

Therefore, the Committee proposes a more precise wording to clarify that the Committee is entitled to inspect all parties that assist PST in the performance of its duties. In the Committee's opinion, Section 4 first paragraph of the Act relating to Oversight of Intelligence, Surveillance and Security Services should be worded as follows:

> 'Establishments etc. that are more than 50 per cent publicly owned shall be subject to the same right of inspection. The same right of inspection shall apply to enterprises that assist in the performance of intelligence, surveillance, and security services.'

Telenor informed the Committee of challenges relating to the security clearance of personnel that deal with PST's communications control cases. The company has been in dialogue with the Norwegian Post and Telecommunications Authority (PT) about the requirements for security clearance of such personnel. PT has allegedly stopped security clearance of telecommunications and internet providers' personnel because there is no legal authority for requiring security clearance for such personnel. The Committee is not aware of any initiative having been taken to change these rules. *However, the Committee considers it a cause for concern that personnel who work with PST's communications control cases do not have security clearance.*

*The Committee sees a need to follow up the matter by conducting inspections of private telecommunications and internet providers in 2013. This indicates that it is necessary to quickly clarify the Committee's right to inspect these enterprises.*

# 6 The National Security Authority (NSM)

## 6.1 General information about the oversight of NSM

During inspections of NSM headquarters, three in 2012, the Committee is given general updates and overviews of the directorate's ongoing activities. The inspections of archives and files are mostly related to security clearances. During the reporting year, the Committee has reviewed all submitted complaint cases concerning security clearances that have been finally decided by NSM as the appellate body, as well as negative decisions that have not

been complained against in cases where the directorate has made initial security clearance decisions. The Committee has also continued its practice of making spot checks of negative decisions that have not been complained against in cases decided by security clearance authorities other than NSM. In addition, the Committee has carried out many spot checks of dropped cases and positive security clearance decisions, among other things in order to compare positive and negative decisions based on the principle of equal treatment.

### 6.2 Equal treatment, case processing times and security interviews

In 2012, the Committee has seen several examples of security clearance authorities reaching different decisions about the same person, even if the basis for assessment had not changed in the period between clearance and reclearance. As the Committee pointed out in the report for 2011, the security clearance authorities do not have an experience archive that shows administrative practice in this area. It is therefore difficult for security clearance authorities to adjust their own practice in relation to each other. *NSM will now consider establishing such a base. The Committee takes a positive view of this.*

During the reporting year, the Committee has focused on case processing times in security clearance cases. In the Committee's opinion, case processing times are often too long, particularly for complaint cases. The Committee has noted that NSM acknowledges that several complaint cases have taken too long, and that some people have had to wait for a decision for a very long time. The Committee has been informed that NSM's normal case processing time for complaint cases is 100 days. On average, 206 days elapse from a case is initially processed until NSM considers a complaint. The explanation for the long case processing times is often the complexity of the case and a lack of personnel. It is good that NSM is considering simplifying case processing for some types of cases, while maintaining the quality and traceability of case-by-case assessment, and that vacancies will be filled.

The Committee has continued to evaluate the threshold for conducting security interviews in 2012. The Security Act Section 21 third paragraph last sentence states that a '[s]ecurity interview shall be conducted if it is not deemed to be obviously unnecessary'. It is the Committee's opinion that several security clearance authorities conduct far fewer security interviews than envisaged in the Act, which is a problem in relation to due process protection. The Committee's impression is that this is often due to a lack of resources.

### 6.3 Inspection of NorCERT

In addition to the three inspections of NSM headquarters conducted in 2012, the Committee has also carried out one inspection of the directorate's NorCERT department – the Norwegian Computer Emergency Response Team. During its inspections of NorCERT, the Committee focuses, among other things, on the cooperation between the department and other intelligence, surveillance or security services that take place within the legal frameworks that govern the respective services, and that protection of privacy is safeguarded in NorCERT's performance of its activities. *The inspection of NorCERT did not give grounds for follow-up. It is positive that NSM has revised its instructions for NorCERT's activities in 2012, particularly as regards clarification of the framework for information sharing and cooperation with PST and the Intelligence Service.*

### 6.4 Complaint cases

In 2012, the Committee has received one complaint against NSM concerning unlawful surveillance. The complaint was also against PST, the Intelligence Service and the Defence Security Agency. The case was concluded without follow-up or criticism. In addition, the Committee has received three complaints against NSM concerning security clearance cases. So far, two of these complaints have been dismissed on formal grounds.

In the third complaint, the Committee was asked to look into the case processing, case processing time, whether the security clearance authority complies properly with the Security

Act, the question of access to documents and the material basis for the refusal to grant security clearance and the observation period. The Committee has previously considered a complaint from the same person concerning the security clearance case, which primarily concerned the issues of access and right of appeal when security clearance cases are dropped, and of case processing times and access to case documents. The security clearance case was initially decided by the FSA, and the decision was upheld by NSM when the appeal was considered. The complaint led to questions being raised about information, access and right of appeal when security clearance cases are dropped.

The Committee reviewed the case in its entirety and made some remarks regarding its processing in a concluding letter to both the FSA and NSM. The Committee referred to the fact that it has commented on the case processing time in the case on several previous occasions. The Committee found 'that the processing of the security clearance case itself and of the complaint concerning the security clearance case, applications for access and the complaint concerning rejection of access has taken an unreasonably long time at all stages of this extensive case'. The Committee also wrote that: 'The issue of security clearance can be decisive for an individual's professional career, and thus has a bearing on the options available to the person concerned. The time aspect is also very important to the requesting entity, and will have a bearing on personnel planning, among other things.'

The Committee also remarked that the complainant had requested access to documents in the case on several occasions. The complainant was first denied access on the grounds that the FSA did not deem the dropping of the case to be a decision that confers right of access under the Security Act Section 25a. An appeal against the denial of access was rejected, but not forwarded to NSM as the appellate body. Another appeal was rejected before the complainant submitted a complaint directly to NSM, which then returned the case to the FSA with a request for a new assessment. The processing of requests for access has proven to take a long time and has been characterised by case processing errors, also in later cases.

In conclusion, the Committee referred to the fact that it has previously assumed that its correspondence with security clearance authorities about complainants' security clearance cases was deemed to constitute part of the 'documents of the case' under the Security Act Section 25a. The Committee also referred to the fact that the Storting's Standing Committee on Scrutiny and Constitutional Affairs endorsed the Committee's opinion in its consideration of the Committee's annual report for 2009. *The Committee therefore requested that the FSA and NSM consider declassifying a copy of the Committee's letter, so that the complainant could be given access to it. The request was complied with, and the complainant was given access to a declassified copy of the letter.*

# 7 The Norwegian Defence Security Agency (FSA)

## 7.1 General information about the oversight of the agency

The Committee conducted three inspections of the FSA in 2012. During these inspections, the Committee receives updates about ongoing activities, including status updates from the agency's office for personnel security on the processing of security clearance cases. The FSA remains Norway's largest security clearance authority by far, and it carries out more than two thirds of the nearly thirty thousand security clearances processed each year. The Committee reviews all negative security clearance decisions made by the FSA during the reporting year that have not been complained against. The Committee also conducts spot checks of dropped cases and positive security clearance decisions in order to assess equal treatment internally in the agency and compare the agency with other security clearance authorities.

In 2012, the review of the FSA's security clearance cases gave grounds for further follow-up of cases concerning dual citizenship, the practice of the requirement for a ten-year personal history for the person concerned and/or closely related persons, the significance of financial circumstances, insufficient use of security interviews etc.

The Committee also inspects the FSA's protective security services work, including security reporting and operational conditions. The Committee requests regular updates about activities carried out by the FSA's office for activity and its underlying sections, including any training exercises, incidents, important cases and cooperation with other agencies/intelligence, surveillance and security services. The Committee also reviews spot checks relating to investigations of reported events that represent a threat to security, and operational cases conducted by the FSA as part of the agency's responsibility for military counterintelligence (Mil CI) in Norway in peacetime. *The review of these cases did not give grounds for further follow-up of the FSA in 2012.*

In 2012, the Committee has had particular focus on the FSA's processing of personal data and whether the processing is authorised by the Instructions for Defence Security Service Chapter 4. Among other things, the Committee has followed this up in the case concerning the FSA's processing of information about MC connections that was discussed in the annual report for 2011.

The Committee received two complaints against the FSA in 2012. One of the complaints concerned loss of security clearance. The case was dismissed on formal grounds, as the security clearance case was under consideration as a complaint case. The Committee also received one complaint against the FSA concerning unlawful surveillance. This complaint was also against PST, the Intelligence Service and NSM, but the investigation gave no grounds for follow-up or criticism of the agency.

## 7.2 The FSA's practice in financial matters

In the Committee's opinion, the FSA's practice regarding the use of authorisation in financial matters does not comply with the applicable regulations. The Security Act Section 21 third paragraph third sentence states that security interviews shall be conducted 'if it is not deemed to be obviously unnecessary'. The threshold for conducting a security interview must therefore be low. For the security clearance authorities, security interviews are an instrument for clearing up doubts and illuminating a case. A security interview also helps to safeguard the adversarial principle in case processing.

During an inspection of the FSA in November 2011, the Committee reviewed several negative security clearance decisions that had not been complained against. Several of these decisions were cases where the person concerned had not collected and/or responded to the FSA's request for authorisation to obtain information from private debt collection enterprises. In such cases, the person was not invited for a security interview. In response to a question from the Committee, the FSA stated that a new practice had been introduced in cases where a person does not collect the registered letter in which the service requests authorisation: the case is dropped.

In its concluding statement to the agency, the Committee stated that 'concluding a case by "dropping" it can only be done if the need for security clearance has lapsed, not as an alternative to considering a case on its merits. In the Committee's opinion, the FSA's new practice is incorrect case processing. This practice also entails a weakening of the due process protection of the persons in question, among other things because no grounds are given and no right of access or appeal apply when cases are dropped.'

In 2012, the Committee has seen that several other security clearance authorities resolve similar cases by obtaining information from the person him/herself about their financial

situation and by conducting security interviews. Many of these cases have ended in security clearance being granted.

The Committee sent the Ministry of Defence a copy of its concluding statement to the FSA. The covering letter stated that the Committee is concerned about the way in which the agency practises the regulations. The Committee has repeatedly raised matters relating to the FSA's practice in the area of security clearance. In the Committee's experience, the FSA or NSM frequently fail to follow this up in a satisfactory manner. The Committee understands that striking a balance between resource use and satisfactory case processing is demanding, but the requirements set out in the Security Act and the Personnel Regulations must nevertheless be complied with. *In 2013, the Committee will carry out a broader assessment of the inadequate use of security interviews and subsequent dropping of security clearance cases.*

### 7.3 Dual citizenship cases – differing practices in the FSA and the Ministry of Defence

In a security clearance case where the person concerned held both Norwegian and foreign citizenship, the FSA made the decision NO CLEARANCE in connection with reclearance. The basis for the assessment of reclearance did not differ from the basis on which the Ministry of Defence granted security clearance for SECRET level to the person in question five year earlier, and there were no negative circumstances relating to the person during the period until reclearance. In its concluding letter to the Ministry and the FSA, the Committee remarked that this differential treatment was unfortunate seen in relation to the principle of equal treatment.

In 2012, the Committee has seen one other case where both the FSA and NSM reached a different conclusion than the Ministry of Defence in their assessment of ties to a foreign state in a case involving dual citizenship. The Committee noted that NSM itself expressed that 'it is also very unfortunate that both the FSA and NSM have arrived at a different conclusion than the Ministry of Defence after assessing the matter of ties' in the case. *Differing practices between security clearance authorities can have great personal consequences for the persons concerned, particularly as regards their work and career, because the persons concerned must have reasonable expectations that a request for reclearance will be dealt with in the same manner as the original request, provided that no circumstances of a negative character have arisen in the meantime. This was the situation for the persons concerned in the two cases. The Committee stated that this is most unfortunate. The Committee also remarked that there is potential cause for concern in relation to security if a person can be granted security clearance for the SECRET level on the same assessment basis that results in a negative decision on reclearance five years later.*

## 7.4 The FSA's processing of information about MC connections

Last year's annual report described the Committee's examination of the FSA's processing of security clearance cases where the person concerned is affiliated to a motorcycle milieu. On the basis of the FSA's statement to the Committee, the Committee understood the agency's concerns relating to some of the persons and their MC connections. Nevertheless, the Committee found it to be unfortunate that the legal basis for each registration was not made clear. A concrete assessment of the relevance and necessity of each registration would have made it easier for the Committee to check whether the matter could constitute an event that represents a threat to security for the Norwegian Armed Forces. The fact that the FSA only provided comprehensive grounds for the basis for registration in response to the Committee's question is less satisfactory from a due process protection and oversight perspective.

Several of the persons registered as having MC connections still held their positions and valid security clearances. Among other things, the Committee asked what information the FSA believed that it could process about a person with a security clearance for purposes other than assessing the person's suitability in terms of security. The FSA replied that '[e]ven

though the office for personnel security has made its assessment and concluded that the person is suitable from a security point of view, […] this does not automatically mean that the case is also concluded for the office for activity, which can be pursuing various other purposes'. The Committee, on the other hand, was of the opinion that when the security clearance authority upholds a person's security clearance after a review, processing by the office for activity will normally no longer be required for the purpose. In the Committee's opinion, the information must therefore be regularly deleted from the register.

However, the Committee agreed with the FSA that it would be another matter if the person in question loses his/her security clearance because he/she is no longer deemed suitable from a security point of view and/or is deemed to constitute a security risk after having lost his/her position. The Committee emphasised that the FSA must 'make a concrete assessment in each case of whether there is a legal basis for processing information before information can be processed as part of an investigation of an event that represents a threat to security. The point is to avoid processing inadequate, irrelevant or unnecessary information. In the opposite case, one risks processing irrelevant and unnecessary information in contravention of the Instructions.'

The FSA informed the Committee that the agency has implemented a number of 'measures to improve the procedures for processing personal data in such cases' and that it had also 'initiated a process to prepare procedures for the investigation of events that represent a threat to security in order to improve the overview of the assessments that must be made in each case, both as regards protection of privacy and other legal authority'. *It is positive that the FSA recognises the need for clearer procedures and that the agency is working on the matter. The FSA has also stated that the Chief of Defence has ordered the FSA to clarify how personal data are processed in the Norwegian Armed Forces' security service. This work is scheduled to be carried out in 2013, and it will form the basis for developing an internal control system that will be submitted to the Ministry of Defence for approval.*

### 7.5 Cooperation between the FSA and PST

In 2012, the Committee was informed about the cooperation between the FSA and PST on a general basis as well as in concrete cases, and it has followed up one case concerning assistance given by the FSA to PST in an investigation case. PST has national responsibility for counterintelligence and counterterrorism. The FSA covers counterintelligence and counterterrorism work in the Norwegian Armed Forces, except work that falls under the Intelligence Service's area of responsibility. All the FSA's work in this field is carried out in cooperation with PST. Among other things, all reports received and obtained about events that represent a threat to security are shared with PST. PST, on the other hand, is under no obligation to share information with the FSA due, among other things, to the need to protect sensitive information.

Cooperation between PST and the FSA is discussed in the Instructions for the Collaboration between the Norwegian Armed Forces and Norwegian Police Security Service of 1980. *A new cooperation agreement is being prepared, and the Committee will keep informed about this work in 2013.*

### 7.6 Procedure document concerning personnel security

Following previous requests, the FSA submitted revised procedure documents in 2011 and 2012 concerning the agency's processing of security clearance cases. In both years, the agency requested that the documents be returned after the Committee had reviewed them. On both occasions, the Committee stated in letters to the FSA that the procedure documents are important to the continuous oversight of the agency's processing of personnel security cases. The Committee therefore has a permanent need to have the applicable procedure document at hand. *On this basis, the Committee has replied to the FSA that the submitted procedure documents will not be returned.*

# 8 The Norwegian Intelligence Service (NIS)

## 8.1 General information about the oversight of the service

In its oversight of NIS, the Committee focuses in particular on compliance with the prohibition against collecting information about Norwegian legal persons on Norwegian soil.

The Intelligence Service Act places few restrictions on surveillance by NIS, unlike for example PST, which is subject to more detailed regulations. This means that the Committee's oversight of NIS is necessarily less extensive than of e.g. PST. It is also difficult to give detailed descriptions of the Committee's oversight of the service's activities, since it is so highly classified.

The Committee conducted four inspections of NIS headquarters in 2012. In addition, inspections were carried out of the service's technical information collection activities at the Norwegian Armed Forces' station at Andøya (FSTA).

The Committee has received two complaints against NIS for unlawful surveillance in 2012. Both the complaints were also complaints against PST. One of them was also against the FSA and NSM. *None of the complaints gave grounds for follow-up or criticism of the service.*

### 8.2 The Committee's oversight of the service's technical information collection

The Intelligence Service Act Section 3 states that the Norwegian Intelligence Service shall 'procure, process and analyse information regarding Norwegian interests viewed in relation to foreign states, organizations or private individuals, and in this context prepares threat analyses and intelligence assessments to the extent that this may help to safeguard important national interests'. The service makes extensive use of technical information collection methods in the performance of its statutory duties. The Committee's inspections of NIS target this technical information collection in particular.

The Intelligence Service Act does not prohibit NIS from covertly obtaining information about Norwegian persons abroad. Nor does it stipulate any conditions for the service's use of intrusive methods. Nonetheless, the surveillance must be within the limitations set out in the Intelligence Service Act and the Intelligence Service Instructions. The service is also obliged to respect the European Convention on Human Rights Article 8 concerning the right to privacy, also outside Norway.

In 2012, NIS has publicly expressed concern about Norwegian persons travelling to conflict areas more often than before. In the Committee's experience, cooperation between NIS and PST has resulted in more coordinated attention being devoted to Norwegians abroad who could represent a threat to Norway and Norwegian interests. The Committee has seen a significant increase in the number of Norwegians abroad who are under surveillance by NIS in 2012. In most cases, such surveillance is coordinated with PST. In this connection, the Committee focuses on whether NIS's surveillance of Norwegians abroad falls within the scope of the service's own duties.

*The Committee's oversight of the service's technical information collection has not resulted in criticism of NIS in 2012.*

### 8.3 The Committee's right to inspect NIS

The matter of the Committee's inspections of NIS was raised most recently with the Standing Committee on Scrutiny and Constitutional Affairs in the annual report for 1998. The right of inspection was discussed by the Committee again in 2012 due, among other things, to the technological development and increased cooperation between NIS and PST. An important

aspect of the basis for this discussion was that the Committee is prevented from searching freely in the service's computer systems and archives because such searches *could* return information received from abroad or information about sources. This means that, in practice, the Committee's oversight of NIS is less extensive than its oversight of the other intelligence, surveillance and security services.

In 1999, the Storting specified a *procedural* method of resolving disputes regarding access to 'sources' and 'the identity of persons with roles in occupation preparedness', which meant that the service can withhold a document until it has been clarified whether or not the Committee has right of access to it, alternatively until the matter has been considered by the Ministry of Defence and the Storting. The Act relating to Oversight of Intelligence, Surveillance and Security Services and the Directive relating to Oversight of the Intelligence, Surveillance and Security Services were revised in 2001 and 2009, respectively, without the Storting adopting any amendments relating to the Committee's right of inspection/access or to the mechanism for resolving disputes.

*The Committee is in dialogue with NIS with a view to arriving at practical solutions for the right of inspection.*

### 8.4 Cooperation between NIS and PST

In 2012, the Committee has paid particular attention to the increased cooperation between NIS and PST. The basis for this cooperation is the fact that PST's area of responsibility covers what goes on within Norway's borders, while NIS's area of responsibility is outside the country. The services are required to cooperate in order to safeguard and protect the nation's interests. Cooperation must take place within the services' respective areas of responsibility and legal authority. The current Instructions for the Collaboration between the Norwegian Armed Forces and the Norwegian Police Security Service state that through exchange of information, cooperation and division of labour, the services shall be able to deal with relevant threats and security challenges in an effective manner.

In 2012, the Committee requested that all new and concluded cooperation cases be presented to it. It also requested a status report on all ongoing cases. The Committee has continued to carry out spot checks of the exchange of information between the two services. It is the Committee's impression that the services cooperate to a significantly greater extent than before.

The regulations and duties of PST and NIS are fundamentally different, and each service is only permitted to obtain information in accordance with the legal basis that applies to it. *The Committee has not seen any cases in 2012 in which the services have exceeded their areas of responsibility or asked the other service to do so. The Committee will prioritise oversight of this area in 2013.*

### 8.5 Information exchange with cooperating foreign services

Section 3 of the Intelligence Service Act allows NIS to establish and maintain intelligence cooperation with corresponding services in other countries. The Committee oversees this by keeping informed about the content of the NIS archives and the service's communications system for information exchange with cooperating foreign services. Through this network, NIS receives information from and shares information with its established partners in certain areas, mainly relating to international terrorism. The Committee can check messages sent or responded to by NIS via this communications network, as well as reports published by NIS for its partners.

If information about Norwegian citizens is retrieved during this process, the information exchanged with cooperating services must be anonymised in order to prevent the identification of Norwegian citizens, cf. the practice whereby the service can only disclose

information about Norwegian citizens to foreign parties subject to certain conditions. The Committee checks that personal data are only disclosed to cooperating services on the basis of specific case-by-base assessments. The Committee also oversees that NIS complies with the requirement laid down in the Intelligence Service Act Section 4 that the service shall not 'monitor or in any other covert manner procure information concerning Norwegian physical or legal persons' in this connection.

Like PST, NIS must also continuously assess the receiving state's attitudes to and respect for fundamental human rights when the service exchanges personal data or other information, including when information is shared as part of Norway's participation in international operations. In 2012, the Committee was informed of the preparation of instructions to seek to reduce the risk of intelligence personnel contributing to torture or other inhumane or degrading treatment in relevant partner countries. The instructions will set out a procedure to ensure management support and, if relevant, political support in the most complex cases that could involve a risk of violation of human rights. These instructions enter into force on 1 January 2013. *The Committee takes a positive view of the introduction of these instructions, which will help the service to make more systematic assessments of the risk of torture etc. in connection with intelligence cooperation with other countries.*

In 2012, the Committee carried out some searches and spot checks of messages that the service had sent to cooperating foreign services. *The oversight has not given grounds for written questions to or criticism of the service.*

In last year's annual report, the Committee reported that NIS had prepared internal guidelines for the disclosure of personal data to cooperating foreign services. Among other things, these guidelines, which are classified as RESTRICTED, specify the conditions for the disclosure of personal data about Norwegian and foreign citizens and set out more detailed case processing procedures. The annual report stated that freedom of information considerations dictate that such information should be unclassified. It should also be considered whether such provisions should be included in the Intelligence Service Act itself and/or in the Intelligence Service Instructions. The service has stated that that it will consider, in consultation with the Ministry of Defence, whether the main content of the guidelines should be set out in publicly available guidelines or regulations. *The Committee will keep up to date about the outcome of this assessment in 2013.*