OFFICIAL TRANSLATION

Translated from the Norwegian: LOV-2020-06-19-77 Lov om etterretningstjenesten

Act of 19 June 2020 no. 77 relating to the Norwegian Intelligence Service (the Intelligence Service Act)

Chapter 1. Purpose and scope of the Act

Section 1-1 *Purpose*

The purpose of this Act is to

(a) contribute to safeguarding Norway's sovereignty, territorial integrity, democratic form of government and other national security interests, including preventing, uncovering and counteracting foreign threats to Norway and Norwegian interests

(b) contribute to safeguarding confidence in and secure the basis for control of the activities of the Norwegian Intelligence Service

(c) ensure that the activities of the Norwegian Intelligence Service are conducted in accordance with human rights and other fundamental values of a democratic society.

Section 1-2 *Scope*

This Act applies to the Norwegian Intelligence Service and to other units and persons under the command of the Director of the Norwegian Intelligence Service or his power of instruction.

This Act does not apply to the collection or other processing of information that is conducted by the Norwegian Intelligence Service exclusively as part of an international operation with an international law mandate.

Section 1-3 *Definitions*

In this Act, the following terms shall mean:

(a) personal data: any information relating to an identified or identifiable natural person

(b) processing of personal data: any operation or set of operations which is performed on personal data, whether or not by automated means

(c) intelligence purpose: the purpose of fulfilling one or several of the tasks of the Norwegian Intelligence Service pursuant to chapter 3

(d) intelligence target: object, natural person, legal person or anything else at which information collection is directed

(e) target discovery: systematic efforts to identify new intelligence targets

(f) targeted collection: systematic efforts to locate information linked to identified intelligence targets

(g) surplus information: information that is irrelevant for intelligence purposes

(h) raw data: any form of unprocessed or automatically processed information whose intelligence value has not yet been assessed

(i) bulk: collections of information and data sets in bulk, where a substantial amount of the information is considered irrelevant for intelligence purposes

(j) disclosure: any dissemination of information, orally or in writing, to a recipient outside the Norwegian Intelligence Service who is not carrying out service or work for the Service.

Chapter 2. Organisation, management and control

Section 2-1 *National service*

The Norwegian Intelligence Service is Norway's national foreign intelligence service. The Service is part of the Norwegian Armed Forces and is subordinate to the command of the Chief of Defence.

The Norwegian Intelligence Service shall be subject to national control. Disclosure of information to foreign partners shall also be subject to national control.

Section 2-2 *Production Management*

The Ministry coordinates and prioritises the authorities' intelligence requirements and prepares a document of prioritised national intelligence requirements on an annual basis.

The Ministry determines procedures for prioritising civilian intelligence requirements that are not covered by the prioritisation document. The Chief of Defence determines procedures for prioritising intelligence requirements within the Norwegian Armed Forces that are not covered by the prioritisation document.

Section 2-3 *Management and control by the Ministry*

The Ministry exercises management and control of the Norwegian Intelligence Service through the Chief of Defence unless otherwise stipulated in this Act. The Coordination Committee for the Norwegian Intelligence Service performs financial control and governance.

The Ministry may stipulate other schemes and reporting procedures for maintenance of management and control.

Section 2-4 *Warning and reporting*

Within the framework of the tasks set forth in chapter 3, the Norwegian Intelligence Service shall

(a) warn the Norwegian authorities of threats and other matters that become known to the Norwegian Intelligence Service and that require immediate action or for other reasons are of a time-critical nature, and

(b) report to the Norwegian authorities any foreign matter that is of significance to Norway and Norwegian interests.

The Norwegian Intelligence Service shall warn and report to the military authorities in accordance with the provisions of the Chief of Defence, and to the civilian authorities in accordance with the provisions of the Ministry.

Pursuant to the provisions of the Ministry, the Norwegian Intelligence Service may alert and advise persons and businesses of threats within the framework of its tasks pursuant to chapter 3. Classified information may be disclosed without regard to the security clearance and authorisation requirements stipulated in section 8-1 of the Security Act when it is strictly necessary and acceptable in terms of security.

Section 2-5 *Matters that shall be submitted to the Ministry for decision*

The Norwegian Intelligence Service shall submit the following matters to the Ministry for decision:

a) the establishment of collaboration and agreements with foreign services or international organisations
b) the launching of special intelligence operations that could raise political issues
c) other cases of particular importance.

Section 2-6 *Control by the Norwegian Parliamentary Oversight Committee and the Office of the Auditor General of Norway*

The Norwegian Intelligence Service is subject to control pursuant to the Act relating to oversight of intelligence, surveillance, and security services. In accordance with section 7-11, the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (EOS Committee) conducts continuous control of the Norwegian Intelligence Service's compliance with the provisions of chapter 7.

The Norwegian Intelligence Service is subject to audit and control by the Office of the Auditor General pursuant to the Act and Instructions relating to the activities of the Office of the Auditor General. The Office of the Auditor General shall designate specific civil servants to conduct audit and control of the Service. The designated civil servants shall be Norwegian citizens and shall have received TOP SECRET security clearance. The Office of the Auditor General shall be represented in the Coordination Committee for the Norwegian Intelligence Service.

Section 2-7 *Other provisions regarding oversight and control*

The provisions of chapters 6 and 7 in the Personal Data Act and chapters VI to VIII in the General Data Protection Regulation (GDPR) concerning supervision, appeals and sanctions, etc. do not apply to the Norwegian Intelligence Service.

The provisions of chapter 10 in the Act relating to electronic communications (Electronic Communications Act) do not apply insofar as they would give the Authority access to the Norwegian Intelligence Service's activities. The first sentence does not hinder the Authority from monitoring how providers who fall within the scope of section 7-2 comply with their obligation to facilitate.

The courts conduct control of facilitated collection of cross-border electronic communication pursuant to chapter 8.

Chapter 3. Tasks

Section 3-1 *Information collection on foreign threats*

The Norwegian Intelligence Service shall collect and analyse information on foreign matters which can contribute to uncovering and counteracting

(a) threats to Norway's independence and security, territorial integrity and political and economic freedom of action
(b) serious threats to public security in Norway
(c) serious threats to Norwegian interests abroad
(d) foreign intelligence activity
(e) foreign sabotage and influence operations
(f) cross-border terrorism

(g) proliferation of weapons of mass destruction and equipment and materiel that can be used to manufacture such weapons
(h) international arms trade that could constitute a serious security threat
(i) export of sanctioned, listed or sensitive goods or services.

Section 3-2 *Information collection on other foreign matters*

The Norwegian Intelligence Service shall collect and analyse information on foreign matters which can contribute to

(a) safeguarding prioritised foreign, defence or security policy interests vis-a-vis matters and trends in other states and regions
(b) national emergency preparedness planning
(c) incident and crisis management
(d) planning and conducting national or international military operations.

Section 3-3 *Occupation preparedness*

The Norwegian Intelligence Service shall secure the nation's ability to collect and disseminate information to the Norwegian authorities in the event that Norway is occupied in whole or in part.

The Ministry shall be kept generally informed about the organising and planning of occupation preparedness.

Section 3-4 *International intelligence collaboration*

When it is in Norway's interest, the Norwegian Intelligence Service may collect and analyse information on foreign threats and other matters mentioned in this chapter that are believed to be of significant relevance in bilateral or multilateral intelligence collaborations in which the Norwegian Intelligence Service participates.

Section 3-5 *Collection of capability information*

The Norwegian Intelligence Service may collect and analyse information on matters that constitute the premises for being capable of conducting collection pursuant to this chapter, in order to

(a) ensure that collection is carried out only to the extent necessary
(b) ensure the safety of Norwegian Intelligence Service personnel and operations
(c) conduct technical equipment testing and other training and exercise activity
(d) maintain and further develop the Norwegian Intelligence Service's access to information and methodological, technological and other capability to perform its tasks as instructed.

Chapter 4. Ban on collection in Norway and other specific bans

Section 4-1 *Ban on collection in Norway*

The Norwegian Intelligence Service shall not use collection methods pursuant to chapter 6 against any person in Norway.

If there is doubt as to whether a person is located in Norway or abroad, the Norwegian Intelligence Service shall seek to clarify the matter. For this purpose, only information from Norwegian authorities, foreign partners, open sources or own collection abroad shall be used.

Section 4-2 *Foreign state activity in Norway*

Notwithstanding section 4-1, the Norwegian Intelligence Service may use collection methods pursuant to chapter 6 against foreign and stateless persons in Norway who are acting on behalf of a foreign state or state-like actor.

If there is doubt as to whether a person is located in Norway or abroad, the Norwegian Intelligence Service shall seek to clarify the matter. For this purpose, only information from Norwegian authorities, foreign partners, open sources or own collection abroad shall be used.

When the nation is at war, war is imminent or the nation's independence or security is at risk, the King can decide that the Norwegian Intelligence Service may, section 4-1 notwithstanding, collect any information pertaining to the Norwegian Armed Forces' ability to handle hostile military activity.

Section 4-3 *Coordination with the Police Security Service*

The Norwegian Intelligence Service shall ask the Police Security Service for consent to collect pursuant to section 4-2 subsection 1 on matters that also fall under the description of the Police Security Service's tasks in section 17 b subsection 1 of the Police Act. In the event of other collection pursuant to section 4-2 subsection 1, the Police Security Service shall be notified.

Section 4-4 *Open sources that affect persons in Norway*

Notwithstanding section 4-1, the Norwegian Intelligence Service may collect information on foreign matters from open sources pursuant to section 6-2 even if said information has been published by or otherwise affects persons in Norway.

Section 4-5 *Source recruitment and source verification in Norway*

Notwithstanding section 4-1, the Norwegian Intelligence Service may collect information on persons in Norway in order to find, recruit and verify sources.

The information shall be collected from open sources or through disclosure by Norwegian authorities. If there are weighty security-related reasons for doing so, methods set forth in sections 6-3 and 6-4 may be used.

No more information than strictly necessary shall be collected. The information shall be used exclusively to find, recruit and verify sources.

Section 4-6 *Training, exercising and testing equipment in Norway*

Notwithstanding section 4-1, the Norwegian Intelligence Service may collect information on persons in Norway when it is strictly necessary to do so in order to train, exercise or test equipment.

The information shall be used exclusively to train, exercise and test equipment, and shall not be processed together with other information. Unless the person the information pertains to allows it to be processed further, the information shall be deleted as soon as possible, and upon completion of the training, exercise or testing at the very latest. The Archives Act does not apply to information pursuant to this section.

Section 4-7 *Accessory information regarding individuals in Norway*

The Norwegian Intelligence Service may use collection methods pursuant to chapter 6 against persons abroad even though information regarding persons in Norway may also be included.

The Norwegian Intelligence Service may collect raw data in bulk even though information regarding persons in Norway may also be included.

Section 4-8 *Ban on collecting information for police purposes*

The Norwegian Intelligence Service shall not collect or assist in collecting information in order to carry out tasks that are the preserve of the police or other law enforcement authorities.

Subsection 1 does not prevent exchange of information pursuant to chapter 10 or assistance to the police pursuant to section 10-7 cf. the Police Act section 27 a.

Section 4-9 *Ban on industrial espionage*

The Norwegian Intelligence Service shall not collect or assist in collecting, process or disclose information in order to give companies or other commercial entities or sectors a competitive advantage.

Chapter 5. Basic conditions for collecting and disclosing information

Section 5-1 *Basic conditions for target discovery*

The Norwegian Intelligence Service may instigate target discovery when there is just cause to investigate whether collection could provide information relevant for intelligence purposes.

Section 5-2 *Basic conditions for targeted collection*

The Norwegian Intelligence Service may instigate targeted collection when specific grounds give cause to investigate whether collection could provide information relevant for intelligence purposes.

Section 5-3 *Basic conditions for collecting and querying in raw data in bulk*

The Norwegian Intelligence Service may collect raw data in bulk when it is necessary to do so in order to access a relevant and adequate information basis.

Querying in raw data in bulk shall satisfy the basic target discovery or targeted collection conditions and be logged for control purposes. A query shall not be carried out if it would constitute a disproportionate interference against the individual.

Querying in raw data based on a search term linked to a person located in Norway may only be conducted if strictly necessary in order to perform a task set forth in section 3-1. Sentence 1 does not apply if the person in question is a foreigner or a stateless person acting on behalf of a foreign state or state-like actor.

Section 5-4 *Proportionality*

Collection and disclosure of information shall not take place if it would constitute a disproportionate interference against the individual. When making this assessment, it should be considered whether a less intrusive measure could fulfil the purpose satisfactorily, what the

impact of the intrusion will be on the person affected by it, the significance of the case and circumstances in general.

Chapter 6. Methods of information collection that could entail interference against persons

Section 6-1 *General conditions*

For intelligence purposes, the Norwegian Intelligence Service may use methods of information collection in accordance with the provisions set forth in this chapter, provided that the basic conditions set out in chapter 5 are met and the collection is not in contravention of other provisions of the Act.

The methods may be used covertly against persons subject to or otherwise affected by them.

Their use shall be terminated if the statutory conditions are no longer present.

Section 6-2 *Open sources*

The Norwegian Intelligence Service may collect openly available information. Information is not openly available when access to it requires active covert action or the bypassing of passwords or similar protection mechanisms.

Section 6-3 *Human intelligence*

The Norwegian Intelligence Service may collect information through systematic interaction with persons in physical space or cyberspace. The Service may find, verify, cultivate, recruit, train and run sources for the purpose of collecting information which is not openly available or to facilitate such collection.

Section 6-4 *Systematic observation*

The Norwegian Intelligence Service may conduct systematic observation in public locations where intelligence targets are likely to be present. The same applies to private locations closed to the public, provided that the observer is located on the outside. Observational aids, recordings and other documentation may be used.

Systematic observation refers to planned visual observations in physical space of a natural person or group of persons, a property, a legal person, an area or another intelligence target.

Section 6-5 *Technical tracking*

The Norwegian Intelligence Service may position technical direction-finding equipment in physical space on or near an intelligence target in order to map the target's position and movements.

Section 6-6 *Searches etc.*

The Norwegian Intelligence Service may search a residence, room or other storage unit in order to find information or items. The Service may take possession of intelligence-related items discovered during the search. Searches of locations that by their nature are not accessible to everyone may only be conducted if strictly necessary.

The Norwegian Intelligence Service may take possession of intelligence-related items from persons.

Section 6-7 *Bugging and imagery surveillance*

The Norwegian Intelligence Service may collect sound and imagery from cameras or microphones located on or near a place where an intelligence target can reasonably be expected to be present. Such collection may not be conducted in locations that by their nature are not accessible to everyone, unless strictly necessary.

Section 6-8 *Other technical collection*

The Norwegian Intelligence Service may collect information using technical sensors or other technical methods not regulated by sections 6-5, 6-7, 6-9 or 6-10, including imagery surveillance of persons from space-based or airborne sensors.

Such collection may not take place in locations that are not by their nature accessible to everyone, unless strictly necessary.

Section 6-9 *Mid-point collection*

The Norwegian Intelligence Service may collect electronic communication in transit and map communication infrastructure. Provisions for facilitated collection of electronic communication being transported across the Norwegian border are set forth in chapters 7 and 8.

Section 6-10 *End-point collection*

The Norwegian Intelligence Service may observe and collect electronic information that is not openly available in computer systems or similar systems or services possessed by or expected to be used by intelligence targets.

If there is reason to believe that the collection will include information which is not intended for communication, the collection shall not be carried out unless strictly necessary.

Section 6-11 *Preparatory measures*

The Norwegian Intelligence Service may take any preparatory measures required to employ methods pursuant to this chapter, including bypassing or circumventing real and technical obstacles, installing, searching or taking possession of technical devices and software and seizing control of, modifying or deploying electronic or other technical equipment.

Section 6-12 *Decision to employ a collection method*

The Director of the Norwegian Intelligence Service may decide to use methods pursuant to this chapter unless the decision is to be made by the Ministry pursuant to section 2-5.

The decision shall not be given for longer than necessary and not for more than one year at a time. The decision shall be reconsidered as soon as possible should the preconditions for the decision change significantly.

Section 6-13 *Decision requirements*

A decision pursuant to section 6-12 shall be in writing and state

(a) the mission to which the collection is linked
(b) what or who the collection applies to
(c) the factual and legal basis for the collection
(d) the duration of the decision.

In matters of urgency, a decision may be made orally. If so, it shall be put into writing as soon as possible.

Chapter 7. Facilitated collection of cross-border electronic communication

Section 7-1 *General conditions and scope*

The Norwegian Intelligence Service may, for intelligence purposes, collect electronic communication being transported across the Norwegian border provided that the basic conditions pursuant to chapter 5 are met, the provisions of chapters 7 and 8 are being obeyed and the collection does not contravene other provisions of the Act.

The provisions of chapters 7 and 8 only apply when it is necessary for providers pursuant to section 7-2 to facilitate the collection.

Section 7-2 *Electronic communications providers' obligation to facilitate*

Providers covered by section 1-5 of the Electronic Communications Act and providers of internet-based communications or messaging services available to the public shall mirror and make available to the Norwegian Intelligence Service selected communication streams and otherwise facilitate selection, filtering, testing, collection, storage and queries as described in this chapter, for instance by

(a) providing information on signal environments, data formats, technical devices and methods
(b) allowing the Service to install equipment and establish a temporary or permanent presence in order to operate equipment in locations controlled by the provider
(c) assisting in the technical operation and maintenance of established solutions
(d) helping to enable the Service to conduct test collection and test analyses of network and service traffic
(e) ensuring access to communication without obstacles such as link encryption or equivalent encryption controlled by the provider
(f) contributing to secure solutions.

Such facilitation shall not reduce the quality of electronic communication services for the users. Any additional expenses incurred by the provider as a result of such facilitation will be covered by the State.

The Ministry may issue regulations in respect of the obligation to facilitate pursuant to subsection 1 and principles for calculating additional expenses pursuant to subsection 2.

Section 7-3 *Facilitation decision*

The facilitation decision is made by the Director of the Norwegian Intelligence Service. As far as possible, the provider shall be given the opportunity to comment before the decision is made. The decision may apply for a period of up to three years at a time.

The provider may appeal the decision to the Ministry. The term of appeal is three weeks from the time when the decision was communicated to the provider. On the provider's request,

the Ministry may decide that the decision should not be initiated until the appeal has been settled.

Facilitation decisions shall be communicated to the EOS Committee and the Norwegian Communications Authority. Upon request, the Norwegian Communications Authority is entitled to information from the Norwegian Intelligence Service regarding technical and operational solutions used to fulfil the obligation to facilitate.

The Ministry may issue regulations in respect of facilitation decisions pursuant to subsection 1 and the handling of appeals pursuant to subsection 2.

Section 7-4 *Duty of confidentiality*

Anyone subject to an obligation to facilitate pursuant to section 7-2 is required to maintain confidentiality as to the Norwegian Intelligence Service's access, technical and operational solutions and other matters linked to the facilitation. The duty of confidentiality similarly applies to anyone who carries out work or offers services to someone with an obligation to facilitate, or who assists in facilitation in any other way. The duty of confidentiality continues to apply after a person has completed their work or service.

The duty of confidentiality does not hinder the provision of information to the EOS Committee or the Norwegian Communications Authority.

Section 7-5 *Test collection and test analyses*

The Norwegian Intelligence Service may conduct test collection and test analyses of traffic and networks covered by this chapter. Test collection and test analyses shall be used exclusively to enable selection, filtering, storage, queries, reprocessing, understanding the signal environment and recognising services and data formats, as well as other technical support.

Test collection is conducted by extracting unfiltered communication from one or more communication streams. One extraction shall not exceed 30 seconds. No more than one extraction may be conducted per hour.

Extracts shall be stored in a short-term storage location to be held separate from data stored pursuant to sections 7-7 and 7-9.

Extracts shall not be stored longer than necessary and shall be deleted after 14 days at the latest. Technical parameters and processed analyses of test data that cannot be linked to an individual may be stored for as long as necessary for the purposes set forth in subsection 1 sentence 2.

Test collection, test analyses and other technical support shall only be carried out by technical experts with special training who do not have intelligence analysis as one of their tasks. There shall always be two experts present when setting up and analysing extracts pursuant to subsection 2.

Section 7-6 *Selection and filtering*

The Norwegian Intelligence Service shall, through selection and filtering, seek to prevent storage pursuant to section 7-7 of metadata regarding communication between senders and recipients who are both located in Norway, unless one of them is covered by section 4-2 subsection 1.

Section 7-7 *Collection and storage of metadata in bulk*

Following selection and filtering pursuant to section 7-6, the Norwegian Intelligence Service may collect and store metadata in bulk on electronic communications being transported across the Norwegian border. Metadata refers to data which describes other data or which contains additional information linked to data, including data which describes the contents' format, the sender and recipient or the communication's size, position, timestamp or duration.

In order to prevent storage of content data, the Norwegian Intelligence Service shall establish and maintain a list of which types of metadata may be stored. The list shall be made available to the EOS Committee and the Norwegian Communications Authority.

Stored metadata shall be deleted after 18 months at the latest.

In respect of technical analysis, troubleshooting and updating of stored metadata for the purpose of enabling queries, section 7-5 subsection 5 sentence 1 shall apply correspondingly.

Section 7-8 *Queries in stored metadata*

The Norwegian Intelligence Service may, within the scope of the court's decision pursuant to chapter 8, conduct queries in metadata stored in accordance with section 7-7. Queries shall be based on search terms.

Queries in stored metadata may only be conducted by Norwegian Intelligence Service personnel who are assessed as capable of doing so and who are appointed by the Service's Director. The personnel shall have completed special training. An individual may only conduct queries in accordance with query privileges adapted to that individual's task portfolio.

Section 7-9 *Targeted collection and storage of content data*

The Norwegian Intelligence Service may, within the scope of the court's decision pursuant to chapter 8, conduct targeted collection and storage of content data and affiliated metadata from electronic communications being transported across the Norwegian border. Content data is data which is not metadata.

Section 7-10 *Internal control and activity logs*

The Norwegian Intelligence Service shall take systematic measures to ensure that activity pursuant to this chapter is conducted in compliance with the Act.

All queries shall be verifiable at a later date through activity logs. Logs shall be kept for ten years and be available for inspection by the EOS Committee at all times.

Section 7-11 *Continuous control*

The EOS Committee shall conduct continuous control of the Norwegian Intelligence Service's compliance with the provisions contained in this chapter, for instance that queries are only conducted in accordance with the court's decisions and that the short-term storage and test data are used exclusively for technical support.

The EOS Committee shall have unhindered access to all information, internal guidelines and procedures, locales, equipment, software, filter updates, activity logs, etc. being used in activity pursuant to this chapter.

The Norwegian Intelligence Service shall facilitate control through technical solutions.

Section 7-12 *Petition to cease and delete*

If the EOS Committee believes that activity pursuant to this chapter is being conducted in contravention of the Act, the Committee may submit a petition to Oslo District Court demanding that illegal activity cease and that illegally collected information is deleted. Prior to submitting the petition, the Norwegian Intelligence Service shall be notified of the Committee's views and given the opportunity to comply with them.

The rules of chapter 8 apply correspondingly insofar as they are appropriate.

Section 7-13 *Ban on disclosing surplus information*

The Norwegian Intelligence Service shall not disclose surplus information from collection pursuant to this chapter. Such information does not trigger the obligation to prevent or inform pursuant to other legislation.

Surplus information as mentioned in subsection 1 can nonetheless be disclosed to the extent necessary in order to prevent grave danger to someone's life, health or freedom, or to prevent someone from being falsely accused or convicted of a criminal offence. The EOS Committee shall be notified of any information disclosure.

Information that is not surplus information may be disclosed provided that the conditions set forth in chapter 10 are met.

Section 7-14 *Prohibition against use as evidence in criminal proceedings*

Information obtained through collection pursuant to this chapter may not be used for sentencing purposes or for imposing other criminal sanctions. Sentence 1 does not apply to cases that involve violations of section 131 of the Penal Code.

Section 7-15 *Information security*

The Norwegian Intelligence Service is obliged to prevent unauthorised persons from gaining access to information being stored and processed pursuant to the provisions of this chapter. The Service shall take security measures pursuant to sections 9-9 and 11-5 to ensure that the information is only available to those who have legal access to it.

Chapter 8. Judicial review of facilitated collection of cross-border electronic communications

Section 8-1 *Order authorising facilitated collection*

By order, the court may grant the Norwegian Intelligence Service authorisation to conduct queries pursuant to section 7-8 and to collect and store pursuant to section 7-9. The order may specify conditions. Grounds shall be given for the order. The court may reverse the order.

The court's decision shall be made as soon as possible. The individual who the decision is directed at or who is otherwise affected by it shall not be given the opportunity to express his/her opinion nor be notified of the order.

The order shall be communicated to the Norwegian Intelligence Service. The Service shall make the court order and the petition available to the EOS Committee.

Section 8-2 *Petition requirements*

The petition for authorisation pursuant to section 8-1 shall be submitted to Oslo District Court by the Director of the Norwegian Intelligence Service, or by another person so authorised by the Director. The petition shall be in writing and state

a) the mission to which the query or collection is linked
b) the factual and legal basis for the query or collection
c) the query terms or query term categories that will be used if the petition applies to queries in stored metadata pursuant to section 7-8
d) what or who the collection is directed at if the petition applies to targeted collection and storage of content data pursuant to section 7-9
e) the proposed duration of the authorisation cf. section 8-6.

Section 8-3 *Oral hearings*

The court may decide to conduct oral hearings. The Norwegian Intelligence Service shall be represented by the Director of the Service or by another person so authorised by the Director. The Service may also be represented by civil servants or anyone else who can substantiate the case.

The court meetings shall be held in camera.

Section 8-4. *Matters to be reviewed by the court*

The court shall review whether the conditions pursuant to this Act are met. This includes whether or not

a) the query or collection is within the scope of the Norwegian Intelligence Service's tasks pursuant to chapter 3
b) any of the bans in sections 4-1, 4-8, 4-9 or 9-4 hinder the query or collection
c) the basic conditions pursuant to chapter 5 are met.

Section 8-5 *Special advocate*

Upon receiving a petition as mentioned in section 8-2, the court shall appoint an advocate to safeguard the rights of individuals and the interests of society in the case at hand. The appointment of an advocate can be waived if the court finds it unobjectionable. The advocate shall be appointed from a special group of advocates who have the appropriate security clearance and may not be represented by another advocate or person acting on his/her behalf. The advocate shall be remunerated by the State.

The advocate shall be informed of the petition and any other information presented to the court, but does not have right of access to information beyond this. The advocate shall not communicate with anyone affected by the case.

The advocate is entitled to express his/her opinion before the court makes its decision. The advocate shall be notified of court hearings and has a right to attend them.

The Ministry may issue regulations in respect of the appointment of advocate pursuant to subsection 1.

Section 8-6 *Duration*

The court's authorisation pursuant to section 8-1 shall not be given for longer than necessary. If it applies to target discovery pursuant to section 7-8, authorisation may not exceed

one year. If it applies to targeted collection pursuant to sections 7-8 or 7-9, authorisation may not exceed six months.

The Norwegian Intelligence Service shall terminate ongoing queries pursuant to section 7-8 and collection and storage pursuant to section 7-9 if the statutory conditions are no longer present.

Section 8-7 *Information security*

The court's order shall be classified according to and in pursuance of the provisions of the Security Act.

The court shall ensure that information and documents with the highest level of classification can be handled in pursuance of the provisions of the Security Act during written or oral hearings. The court shall make provisions to enable special advocates that have been appointed under section 8-5 to access classified information at the court's premises.

The Ministry may issue regulations in respect of the court's access to case law in matters under this chapter.

Section 8-8 *Duty of confidentiality*

Judges and anyone else who carry out work or offer services to the courts have a duty of confidentiality in respect of petitions, court hearings, court orders and any other information to which they gain access in cases under this chapter. The duty of confidentiality continues to apply after a person has completed their work or service.

The duty of confidentiality does not hinder the provision of information to the EOS Committee.

Section 8-9 *Appeals*

The Norwegian Intelligence Service and the special advocate may appeal the court's decision.

The provisions of the Criminal Procedure Act chapter 26 apply correspondingly insofar as they are appropriate. Section 8-7 applies correspondingly for the court of appeal.

Section 8-10 *Matters of urgency*

If delay entails a great risk that information essential to the execution of the Norwegian Intelligence Service's tasks pursuant to chapter 3 could be lost, orders from the Service's Director may take the place of a court order. The Service shall immediately, and no later than 24 hours after the collection started, present the case before the court.

The court will by order decide whether to allow the query or collection cf. section 8-1. If the court finds that the query or collection was unlawful, the court shall notify the EOS Committee accordingly. The court may instruct the Norwegian Intelligence Service to delete the collected information.

Chapter 9. Processing of personal data following collection

Section 9-1 *Relationship to the Personal Data Act*

This chapter applies to the Norwegian Intelligence Service's processing of personal data for intelligence purposes when personal data is processed wholly or partly by automated means or in a non-automated manner and is recorded in or will be recorded in a database.

The processing of personal data for purposes other than intelligence purposes is subject to the provisions of the Personal Data Act, with the exceptions set out in section 2-7 subsection 1 and any special protective regulations pursuant to section 11-4 subsection 3.

Section 9-2 *Basis for processing*

The Norwegian Intelligence Service may process personal data when it is necessary to do so for intelligence purposes.

Section 9-3 *Exceptions to the collection of personal data*

With the exception of section 9-4, the provisions of this chapter do not apply to processing in the form of collection. Processing in the form of collection is regulated by chapters 3 to 8.

Section 9-4 *Ban on discrimination*

The Norwegian Intelligence Service shall not process personal data exclusively based on known information about a person's ethnicity or national background, political, religious or philosophical conviction, language, political activity, union affiliation, health-related issues or sex life or sexual orientation.

Section 9-*5 Processing of confidential communication with persons in certain occupations*

The Norwegian Intelligence Service shall not process confidential communication with persons in certain occupations as mentioned in the Criminal Procedure Act section 119 and the Dispute Act section 22-5 when the person in question or the person confiding in him/her is residing in Norway or is a Norwegian citizen.

If it is strictly necessary that the rationale for justifying the protection of the confidential communication yield to national security interests, such confidential communication can nevertheless be processed.

The decision to process confidential communication pursuant to subsection 2 shall be made by the Director of the Norwegian Intelligence Service. The decision shall be in writing and describe the factual and legal basis for the processing. The decision shall be communicated to the EOS Committee.

Section 9-6 *Processing of information which could identify a source*

The Norwegian Intelligence Service shall not process information confided to someone in their journalistic work and which could reveal the source of the information, if the person who confided or the person to whom the information was confided is residing in Norway, is a Norwegian citizen, or is on assignment for a business in Norway that is subject to section 2 of the Media Liability Act. The ban also applies if the person is no longer residing in Norway or working for the business, but was so at the time the information was given.

If it is strictly necessary that the rationale for justifying the protection of sources yield to national security interests, information mentioned in subsection 1 can nonetheless be processed.

The decision to process information pursuant to subsection 2 shall be made by the Ministry after the matter has been submitted pursuant to section 2-5. The decision shall be in writing and describe the factual and legal basis for the processing. The decision shall be communicated to the EOS Committee.

Section 9-7 *Correct and updated personal data*

The Norwegian Intelligence Service shall, to the extent possible, make sure that personal data that is being processed and that is not raw data in bulk is correct and updated. Incorrect personal data shall be corrected or deleted without undue delay. The Service shall, to the extent possible, make sure that the error does not negatively affect the person the personal data applies to.

If non-verified personal data is disclosed pursuant to chapter 10, this shall be communicated to the recipient.

Section 9-8 *Deletion*

Personal data shall be deleted when it is no longer needed for the processing purpose.

Raw data in bulk shall be deleted after 15 years at the latest, from the date it was stored, unless there are important considerations that justify suspending deletion. The decision to suspend deletion is made by the Director of the Norwegian Intelligence Service for no more than 5 years at a time. Metadata that has been collected and stored in bulk pursuant to section 7-7 shall nevertheless be deleted after 18 months at the latest cf. section 7-7 subsection 3.

Deletion of personal data from operational systems and databases that are available to intelligence production does not preclude the data from being stored in pursuance of other legislation.

Section 9-9 *Information security*

The Norwegian Intelligence Service shall safeguard confidentiality, integrity and availability through systematic measures when processing personal data. The measures shall be prepared in accordance with the provisions of the Security Act.

Access to personal data shall be limited to those who need access for the processing purpose.

Section 9-10 *Data protection officer*

The Norwegian Intelligence Service shall have at least one data protection officer.

The data protection officer shall contribute to compliance with this Act through training, guidance, direction and internal control. The data protection officer shall be able to receive notifications from Norwegian Intelligence Service employees concerning violations and discrepancies linked to the processing of personal data.

Chapter 10. National and international collaboration and information exchange

Section 10-1 *National and international collaboration*

The Norwegian Intelligence Service shall collaborate with other Norwegian authorities in respect of cross-border threats, counteracting and handling of serious incidents in cyberspace and other prioritised areas.

The Norwegian Intelligence Service shall establish and maintain intelligence collaboration with other countries, defence alliances to which Norway is signatory and other international organisations. Matters as mentioned in section 2-5 shall be submitted to the Ministry for decision.

Section 10-2 *Disclosure of intelligence information as part of national collaboration*

The Norwegian Intelligence Service may disclose intelligence information to other Norwegian authorities provided that

(a) disclosure takes place for intelligence purposes or is necessary in order to promote the tasks of the recipient body, or prevent activity from being conducted in an improper manner
(b) disclosure of information which the Norwegian Intelligence Service has received from a third party is disclosed with the permission of that party
(c) disclosure of personal data is in accordance with chapter 9
(d) disclosure is proportionate pursuant to section 5-4
(e) disclosure is justifiable given the quality of the information, who the recipient of the information is and how the recipient intends to use it
(f) it is expected that the disclosed information will be handled properly from a security perspective.

Disclosure with a view to collection or other measures by the recipient on behalf of the Norwegian Intelligence Service may only take place if the Service itself lawfully could have carried out the collection or the measure.

Disclosure shall be verifiable.

This section does not apply to disclosure of information to the EOS Committee and other inspection and supervisory authorities.

Section 10-3 *Disclosure of intelligence information as part of international collaboration*

The Norwegian Intelligence Service may disclose intelligence information to other states' authorities or international organisations provided that

(a) the conditions under section 10-2 are met
(b) the disclosure is under national control and in Norway's interest
(c) a condition is imposed that the information may not be used as a basis for collection against persons in Norway, with the exception of persons covered by section 4-2 subsection 1 and it is in Norway's interest that the recipient body collects information on them.

The Norwegian Intelligence Service shall not disclose intelligence information if there is a real risk that the information could contribute to a person being subjected to torture or other cruel, inhuman or degrading treatment or punishment.

Section 10-4 *Disclosure of surplus information*

The Norwegian Intelligence Service may disclose surplus information to other Norwegian authorities provided that the conditions under section 10-2 are met.

Surplus information originating from collection under chapter 7 is regulated by section 7-13.

Surplus information that is confidential communication under section 9-5 or source information under section 9-6 may not be disclosed.

Section 10-5 *Disclosure of information to the Norwegian Intelligence Service from Norwegian authorities*

Notwithstanding statutory duty of confidentiality, Norwegian authorities may disclose information to the Norwegian Intelligence Service if this is considered necessary for prevention and security purposes within the scope of the Service's tasks under chapter 3. Sentence 1 does not apply to duty of confidentiality as mentioned in the Criminal Procedure Act section 119 and the Dispute Act section 22-5 or the duty to maintain secrecy under the Criminal Procedure Act section 216 i.

Section 10-6 *Dissemination of information on behalf of Norwegian authorities*

The Norwegian Intelligence Service may disseminate information to and from other states' authorities on behalf of other Norwegian authorities provided that

(a) the Norwegian authority has requested the Norwegian Intelligence Service to disseminate the information
(b) the recipient is informed that the dissemination is made on behalf of the Norwegian authority
(c) the Norwegian Intelligence Service does not alter the information, add its own information or request the recipient to act in a certain way in the light of the information.

The recipient shall be informed that dissemination to a third party is contingent upon consent from the Norwegian authority, and whether such consent already has been granted.

Disclosure shall be verifiable.

Section 10-7 *Assistance to the police*

The Norwegian Intelligence Service may assist the police in pursuance of the Police Act section 27 a. Assistance may not be in the form of queries or collection pursuant to chapter 7.

Chapter 11. Concluding provisions

Section 11-1 *Relationship to the Public Administration Act*

With the exception of sections 13 to 13 f concerning duty of secrecy, the Public Administration Act shall not apply to case processing pertaining to the execution of the Norwegian Intelligence Service's tasks under this Act.

Section 11-2 *Duty of confidentiality*

Anyone who performs work or services for the Norwegian Intelligence Service shall maintain lifelong silence about any information to which he/she becomes aware in performing

his/her work or service, if it could harm national security interests if the information were to become known to unauthorised persons.

Employees at the Norwegian Intelligence Service shall maintain lifelong silence about their employment or that of anyone else.

The duty of confidentiality under subsection 1 also applies to anyone who becomes acquainted with classified information under section 2-4 subsection 3.

Information as mentioned in subsections 1 to 3 may not be utilised in any activity outside the Norwegian Intelligence Service.

The duty of confidentiality does not prevent information from being disclosed in pursuance of the provisions of this Act or in pursuance of the provisions of other legislation, or from being shared with other individuals at the Norwegian Intelligence Service in accordance with applicable rules for authorisation and the need-to-know principle.

Section 11-3 *Citizenship and security clearance requirements*

Military personnel and civilian employees at the Norwegian Intelligence Service shall be Norwegian citizens and have TOP SECRET security clearance.

For positions with a lower need for security clearance, the Director of the Norwegian Intelligence Service may determine that personnel can have SECRET security clearance.

Section 11-4 *Protecting intelligence operations, etc.*

The Norwegian Intelligence Service may utilise cover structures and incorrect, false or misleading identities, documents and data, as well as seize control of, modify or deploy electronic equipment in order to protect its operations.

Provisions in other legislation regarding the duty to provide information do not apply to information concerning compensation that the Norwegian Intelligence Service gives to sources and persons working under contract who are not employed by the Service. Such compensation or payments shall not be classified as taxable income on the part of the recipient nor be included in the basis for calculating or reducing social benefits, etc.

The King in Council may prescribe provisions that disregard other legislation, for instance the requirement to report information to public records, to the extent necessary in order to protect the Norwegian Intelligence Service's employees, sources, capabilities, methods or operations from public exposure or from being compromised vis-à-vis other states.

Section 11-5 *Archives, information systems and intelligence databases*

The Norwegian Intelligence Service's archives, information systems and intelligence databases shall be satisfactorily secured and inaccessible to anyone other than the Service's authorised personnel who need access in order to perform their duties and individuals who are tasked with performing control and supervision of the Norwegian Intelligence Service.

Section 11-6 *Emergency preparedness*

The Norwegian Intelligence Service shall prepare and maintain emergency preparedness plans, including deliberate measures to secure that the Service's information and systems do not fall under the control of unauthorised persons in the event of a crisis or armed conflict, in accordance with the National Preparedness System and the Norwegian Armed Forces' operational plans.

Section 11-7 *Complaint and notification*

Anyone may submit a complaint to the EOS Committee pursuant to the Act relating to oversight of intelligence, surveillance and security services. The Norwegian Intelligence Service is not obligated to notify a person who has been the subject of information collection that could constitute a human rights interference.

Section 11-8 *Penalty*

Any person who fails to comply with the facilitation decision under section 7-3 or who violates the duty of confidentiality under section 7-4 is liable to a penalty of a fine or imprisonment for a term not exceeding six months.

Chapter 12. Entry into force and amendments to other legislation

Section 12-1 *Entry into force*

The Act enters into force on the date determined by the King. Its various provisions may enter into force at different times.

Section 12-2 *Repeal*

The Act of 20 March 1998 no. 11 relating to the Norwegian Intelligence Service is repealed from the date this Act enters into force.

Section 12-3 *Amendments to other Acts*

From the date this Act enters into force, the following amendments to other Acts shall be made:

1. The following amendments shall be made to the Act of 4 July 2003 no. 83 relating to electronic communication:

Section 2-8 new subsection 4 shall read:
Provisions regarding facilitation for the purpose of collecting electronic communications transported across the Norwegian border is laid down in chapter 7 of the Act relating to the Norwegian Intelligence Service.

Section 6-2 a subsection 1 new third sentence shall read:
The Norwegian Intelligence Service may, in exceptional cases and for a short period of time, use frequencies allocated to others for identity capture when this is strictly necessary in order to collect information about a person who falls within the scope of section 4-2 subsection 1 of the Act relating to Norwegian Intelligence Service.

Section 6-2 a subsection 2 shall read:
The Police, *Norwegian Intelligence Service* 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. The Authority determines, in consultation

with the Police, *Norwegian Intelligence Service* or National Security Authority, on whether and if so when the rights holder shall be informed.

Section 6-2 a subsection 3 third sentence shall read:
The Armed Forces may only be awarded licenses for exercises within the Armed Forces' permanent training areas. *The Norwegian Intelligence Service is exempt from this provision.*

2. In the Act of 19 May 2006 no. 16 relating to the right of access to documents held by public authorities and public undertakings (Freedom of Information Act) section 2 subsection 4 new fourth sentence shall read:
This Act does not apply to documents processed by the Norwegian Intelligence Service under the Norwegian Intelligence Act.

The current fourth sentence becomes a new fifth sentence.