Act relating to national security (Security Act)

This is an unofficial translation of the Norwegian version of the Act and is provided for information purposes only. Legal authenticity remains with the Norwegian version as published in Norsk Lovtidend. In the event of any inconsistency, the Norwegian version shall prevail.

The translation is provided by the Ministry of Justice and Public Security

Chapter 1. Purpose and scope

Section 1-1.*Purpose*

The act is intended to help

a) protect Norway's sovereignty, territorial integrity and democratic system of government, and other national security interests

b) prevent, detect and counter activities which present a threat to security

c) ensure that security measures are implemented in accordance with the fundamental legal principles and values of a democratic society.

Section 1-2.*Application of the act*

The act applies to governmental, county and municipal bodies.

The act applies to suppliers of goods or services in connection with classified procurements pursuant to Chapter 9.

In the case of undertakings situated on Svalbard, on Jan Mayen or in a dependency, the act applies with the scope and subject to any local adjustments decided by the King.

The King in Council may issue regulations on the scope of the act, and may wholly or partly exempt specified undertakings or certain types of information, information systems, objects and infrastructure.

Section 1-3.*Decision that the act shall apply to other undertakings*

Within its area of responsibility, a ministry shall decide that the act shall apply wholly or partly to undertakings which

a) handle classified information

b) control information, information systems, objects or infrastructure which are of vital importance to fundamental national functions

c) engage in activities which are of vital importance to fundamental national functions.

The undertakings shall be given prior notice of any decision pursuant to the first paragraph.

The National Security Authority may on its own initiative propose to a ministry that the ministry make a decision pursuant to the first paragraph. If the ministry does not make a decision in accordance with the recommendation of the National Security Authority, the National Security Authority may submit the matter to the ministry which has overall responsibility for protective security work in the civilian sector or the ministry which has overall responsibility for protective security work in the defence sector for a final decision.

The National Security Authority shall make a decision pursuant to the first paragraph with respect to undertakings which do not fall within the area of responsibility of any ministry. The ministry is the body of appeal.

Section 1-4.*Application of the act to the Storting (the Norwegian parliament), parliamentary bodies, the Government and the courts*

The act applies to the Storting and parliamentary bodies to the extent decided by the Storting.

Provisions laid down in and pursuant to Chapter 8 do not apply to members of parliament, government ministers or Supreme Court judges.

The act applies to the courts subject to the special rules set out in provisions on security clearance and authorisation in and pursuant to the Courts of Justice Act and the Criminal Procedure Act. The King may issue further special rules.

Section 1-5.*Definitions*

In this act, the following terms shall have the following meanings:

1. national security interests: Norway's sovereignty, territorial integrity and democratic system of government, and general political security interests related to

a) the activities, security and freedom of action of the highest state bodies

b) defence, security and contingency preparedness

c) relations with other states and international organisations

d) economic stability and freedom of action

e) fundamental societal functions and the basic security of the population

2. fundamental national functions: services, production and other types of activity which are of such importance that a complete or partial loss of the function would have consequences for the State's ability to protect national security interests

3. protective security work: planning, facilitation, implementation and checking of protective measures targeting activities which present a threat to security and the consequences of such activities

4. activities which present a threat to security: intentional acts which may directly or indirectly harm national security interests

5. associates: persons who are close family members or who have some other close relationship which may affect whether a person is suitable for security clearance.

Chapter 2. Responsibility and authority related to protective security work

Section 2-1.*Ministerial responsibility and authority related to protective security work*

The ministries are responsible for protective security work in their areas of responsibility, and shall

a) identify and maintain an overview of fundamental national functions

b) identify and maintain an overview of undertakings of material importance to fundamental national functions

c) make decisions pursuant to section 1-3 first paragraph

d) notify overviews to the National Security Authority pursuant to paragraphs a) and b), as well as decisions pursuant to paragraph c).

The King in Council may issue regulations on ministerial responsibility and authority related to protective security work.

Section 2-2.*The National Security Authority's responsibility for protective security work*

The National Security Authority has cross-sectoral responsibility for ensuring that undertakings perform protective security work in accordance with the act.

The National Security Authority has overall responsibility for controlling the state of security in all sectors, and shall ensure that the undertakings comply with their duties under the act. Among other things, the National Security Authority shall

a) ensure supervision of undertakings' compliance with requirements related to protective security work

b) prepare and maintain basic criteria for inspections

c) obtain and assess information relevant to protective security work

d) provide information, advice and guidance on protective security work and required measures

e) maintain an overview of functions and undertakings identified by the ministries pursuant to section 2-1

f) maintain an overview of undertakings in respect of which a decision has been made pursuant to section 1-3

g) facilitate the exchange of information pursuant to section 2-3

h) help develop security measures and adopt requirements related to protective security work.

The National Security Authority is the national competent authority in relation to other countries and international organisations.

To the extent necessary to perform tasks specified in or pursuant to the act, the National Security Authority shall be granted unhindered access to critical national information, critical national information systems, critical national objects or critical national infrastructure.

The King may issue regulations on the National Security Authority's responsibility for protective security work.

Section 2-3.*Exchange of threat assessments and other security information*

The National Security Authority shall arrange for undertakings to which the act applies to be granted access to information about threat assessments and other information which is relevant to the undertakings' protective security work.

The National Security Authority shall in consultation with sector authorities and other relevant authorities ensure the establishment of necessary forums for the exchange of information and experience.

The King may issue regulations on the exchange of threat assessments and other security information.

Section 2-4.*Response function and warning system for digital infrastructure*

The King will appoint an authority to operate a national response function for serious cyberattacks and a national warning system for digital infrastructure.

When necessary for the performance of tasks pursuant to the first paragraph, this authority may process personal data in the form of

a) metadata on ICT traffic to and from undertakings which are connected to the national warning system for digital infrastructure

b) information which is required for analysis of triggered alarms in the warning system

c) IP addresses received from national and international partners

d) logs and infected hardware when necessary to assist an undertaking in its handling of serious cyberattacks and the undertaking consents to this.

When strictly necessary for the performance of tasks pursuant to the first paragraph, other personal data than specified in the second paragraph may also be processed.

The processing of personal data and interference with the right to privacy shall not be more extensive than necessary to achieve the purpose.

The King may issue regulations on the national response function and the national warning system for digital infrastructure.

Section 2-5.*Decisions in response to a risk of harm to national security interests*

The King in Council may make necessary decisions to prevent activities which present a threat to security or other planned or ongoing activities which may present a not insignificant risk of a threat to national security interests. Such a decision may be made without regard to the restrictions in section 35 of the Public Administration Act, and regardless of whether an activity is permitted under another act or decision.

Before a decision is made, advisory opinions should be obtained from relevant bodies with expertise in the relevant specialist area.

A decision pursuant to the first paragraph constitutes a special ground for enforcement pursuant to Chapter 13 of the Enforcement Act.

The King in Council may issue regulations specifying which decisions may be made pursuant to the first paragraph.

Chapter 3. Supervision

Section 3-1.*Supervision of undertakings*

The National Security Authority supervises undertakings which are covered by the act.

The ministry may decide that authorities with sectoral responsibility which supervise the protection of information, information systems, objects or infrastructure shall supervise undertakings which are covered by the act. The National Security Authority shall nevertheless conduct supervision when required pursuant to international obligations or for other imperative reasons.

The National Security Authority shall supervise ministries and authorities with supervisory responsibility pursuant to the second paragraph.

The King may issue regulations on the granting of supervisory responsibility and the division of responsibility between the National Security Authority and relevant authorities with sectoral responsibility.

Section 3-2.*Cooperation between the National Security Authority and other authorities with supervisory responsibility*

The National Security Authority and authorities with supervisory responsibility pursuant to section 3-1, second paragraph, shall enter into a cooperation agreement. Wherever possible, the conduct of supervision shall be coordinated with other supervisory authorities.

The National Security Authority shall prepare and develop basic criteria for inspections pursuant to the act, and facilitate joint training of supervisory personnel.

The National Security Authority may, if necessary, participate in the preparation and conduct of supervision performed by authorities with supervisory responsibility. Authorities with supervisory responsibility may request such assistance from the National Security Authority.

Authorities with supervisory responsibility shall notify the National Security Authority of planned supervision, provide an account of completed supervision and provide information on any non-conformances and instructions issued.

The King may issue regulations on cooperation and the exchange of information between the National Security Authority and authorities with supervisory responsibility.

Section 3-3.*General supervision principles*

Supervision pursuant to section 3-1 shall not unnecessarily disrupt the ordinary operations of supervision subjects.

Information gathered by the supervisory authority may only be used in connection with supervision and protective security work.

Section 3-4.*Site access rights and duty to give notice of on-site inspections*

The supervisory authority may demand access to undertakings' information, information systems, objects and infrastructure. Undertakings shall make relevant personnel available during supervision to the extent necessary.

Written notice shall be given of on-site inspections. Supervision may nevertheless be performed without notice if necessary for security-related reasons.

The King may issue regulations on on-site inspections.

Section 3-5.*The supervisory authority's processing of personal data*

The supervisory authority may process personal data if necessary to perform its tasks.

The processing of personal data must not constitute a disproportionate interference with the right to privacy.

If possible, personal data shall be processed using the information systems of the undertaking, without such data being copied or transferred to the supervisory authority. The supervisory authority may nevertheless demand a copy of personal data if necessary to document whether provisions of the act have been breached.

The King may issue regulations on the supervisory authority's processing of personal data.

Section 3-6.*Instructions*

The supervisory authority may instruct an undertaking to implement measures which are necessary to achieve the purpose of the act. Instructions to implement specific measures may only be issued if the costs inflicted on the undertaking appear reasonable relative to what the measure may achieve.

If authorities with supervisory responsibility do not perform supervision in accordance with requirements specified in or pursuant to the act, the National Security Authority may issue instructions to perform such supervision.

Instructions pursuant to the first and second paragraphs may be appealed. The provisions of Chapter VI of the Public Administration Act apply to the right of appeal of independent natural or legal persons.

Chapter 4. General requirements concerning protective security work

Section 4-1.*Security management*

Responsibility for protective security work rests with the head of an undertaking. Protective security work shall be incorporated into the undertaking's management system. The undertaking's state of security shall be checked regularly.

The undertaking shall ensure that employees, suppliers and contractors have an adequate understanding of risks and security. Chapter 9 applies to suppliers in classified procurements.

The King may issue regulations on security management.

Section 4-2.*Risk assessment*

Undertakings shall conduct regular risk assessments. The assessment shall form the basis for implementation of protective security measures.

As part of the assessment, each undertaking shall identify other undertakings on which it is dependent for its proper functioning.

The assessment shall be reviewed regularly, and be revised if necessary.

The supervisory authority shall on request provide advice and guidance on the assessment.

The King may issue regulations on the conduct of risk assessments.

Section 4-3.*Duty to implement security measures and exercises*

Undertakings shall implement such protective security measures as are required to ensure an appropriate level of security and reduce the risk associated with activities which present a threat to security. Such measures may be implemented in conjunction with other protective security measures taken by each undertaking, provided that the requirements of this act are met.

The cost of a security measure shall be reasonably proportionate to what the measure may achieve.

The undertaking shall conduct regular exercises to evaluate the effect of implemented security measures.

The King may issue regulations on the duties of undertakings covered by the act, and on exercises.

Section 4-4.*Documentation requirement*

Undertakings shall document their assessments of risks and implemented and planned security measures.

The King may issue regulations on documentation requirements.

Section 4-5.*Duty to give notice*

An undertaking shall notify the National Security Authority and other authorities tasked with performing supervision pursuant to section 3-1, second paragraph, immediately if

a) it is affected by activities which present a threat to security

b) it has a reasonable suspicion that activities which present a threat to security have affected or may affect the undertaking or other undertakings

c) serious breaches of security requirements pursuant to Chapters 5, 6 or 7 have occurred .

The undertaking shall notify the supervisory authority irrespective of any duty of secrecy if it gains knowledge of a planned or ongoing activity which may present a not insignificant risk of a threat to national security interests. The supervisory authority shall notify the National Security Authority without undue delay and forward the notification to the responsible ministry for assessment of a decision pursuant to section 2-5.

The King may issue regulations on the duty to give notice pursuant to the second paragraph.

Chapter 5. Information security

Section 5-1.*Critical national information*

Information is nationally critical if national security interests may be harmed if the information becomes known to unauthorised persons, is lost, is altered or becomes unavailable.

Section 5-2.*Protection of critical national information*

Undertakings shall ensure an appropriate level of security in relation to critical national information, so that the information

a) does not become known to unauthorised persons

b) is not lost or altered

c) is available when there is an official need-to-know.

The King may issue regulations on the identification and protection of critical national information. In special cases, such regulations may grant exemptions from security requirements specified in or pursuant to this act.

Section 5-3.*Classified information*

An undertaking which produces information shall classify and mark the information if national security interests may be harmed if the information becomes known to unauthorised persons. The following security classification levels shall be used:

a) TOP SECRET if critical adverse consequences could result

b) SECRET if serious adverse consequences could result

c) CONFIDENTIAL if adverse consequences could result

d) RESTRICTED if adverse consequences could result to some extent.

Security classification shall not be used to a greater extent or for longer than necessary. Unless otherwise provided, the security classification shall cease to apply after 30 years.

The King may issue regulations on security classification and protection of information received or provided pursuant to a mutually binding agreement with a foreign state or international organisation.

Section 5-4.*Access to and duty of secrecy in respect of classified information*

Classified information shall only be released to persons who have an official need-to-know and are authorised to have access to such information.

All persons who have access to classified information as part of their work or service for an undertaking covered by the act have a duty of secrecy in respect of the content of such information. The duty of secrecy continues to apply after such work or service has concluded.

Section 5-5.*Technical surveillance countermeasures*

The National Security Authority may inspect premises, buildings and other objects which an undertaking controls either alone or together with other parties to determine whether unauthorised persons could gain access to classified information through wiretapping, physical observation or signal interception.

Information gathered during such an inspection may only be used for the purpose of the inspection. The information shall be erased when it is no longer needed. Knowledge and experience acquired by the National Security Authority through the inspection may be

used in the further development of the National Security Authority's general security work.

The National Security Authority shall issue a report to the undertaking on the results of the inspection. The report shall only contain information which may help to improve the undertaking's security.

The King may issue regulations on technical surveillance countermeasures, and regulations authorising the performance of such inspections by parties other than the National Security Authority.

Section 5-6.*Cryptosecurity*

Cryptosystems which are to be used to protect classified information must be approved by the National Security Authority.

The National Security Authority is the national administrator of cryptomaterials and a supplier of cryptosecurity services to undertakings. The National Security Authority may approve other suppliers of cryptosecurity services.

The National Security Authority shall approve encryption algorithms used in equipment intended for export.

The King may issue regulations on cryptosecurity.

Chapter 6. Information system security

Section 6-1.*Critical national information systems*

An information system is nationally critical if it handles critical national information or if it is itself of vital importance to fundamental national functions.

The King may issue regulations on the identification of critical national information systems.

Section 6-2.*Protection of critical national information systems*

Undertakings shall ensure an appropriate level of security for critical national information systems, so that

a) the information systems function as intended

b) unauthorised persons do not gain access to information processed by the systems

c) information processed by the systems is not altered or lost

d) information processed by the systems is available to persons with an official need-to-know.

The King may issue regulations on the identification and protection of critical national information systems. In special cases, such regulations may grant exemptions from security requirements specified in or pursuant to this act.

Section 6-3.*Approval of critical national information systems*

Critical national information systems shall be approved by an approval authority. Information systems which are to process classified information shall be approved before being used.

The King may issue regulations on approval of critical national information systems, the appointment of approval authorities and requirements applicable to suppliers.

Section 6-4.*Monitoring of critical national information systems*

Undertakings shall continuously monitor their critical national information systems to prevent, detect and counter incidents which may harm national security interests. Incidents relevant to such security work shall be registered.

The sending of information to, from and within critical national information systems shall be registered, stored and analysed to the extent necessary for the purpose of the monitoring.

Information systems which process personal data shall only be monitored using the methods and to the extent necessary for the purpose of the monitoring.

Information pursuant to the first and second paragraphs may be stored for up to five years. Stored personal data may only be used to the extent necessary for the purpose of the monitoring.

Where multiple undertakings are linked with the same information system, they may agree that one of the undertakings shall conduct monitoring pursuant to the first and second paragraphs on behalf of all of the undertakings. The undertaking which conducts the monitoring shall ensure that the information security requirements in section 5-2 are followed.

The undertaking shall ensure that authorised users of monitored information systems are informed of the purpose of the processing of the personal data and what monitoring measures have been implemented. They shall also be informed if the personal data is released and, if so, to whom.

The King may issue regulations on monitoring of critical national information systems, including provisions specifying

a) which types of information may or must be registered, stored and analysed in connection with the monitoring

b) who shall have access to information which is registered and stored in connection with the monitoring

c) how access is to be granted to registered or stored information

d) that information pursuant to the first and second paragraphs shall be subject to different storage period than five years.

Section 6-5.*Penetration testing of critical national information systems*

An undertaking may ask the National Security Authority to attempt to penetrate its critical national information systems. The purpose must be to check whether security measures are adequate. The undertakings' employees must be informed that such a check may be performed.

If the check entails the processing of personal data, this shall not be more extensive than necessary for the purpose.

Information to which the check provides access may only be used for the purpose of the check. When the information is no longer required, it shall be erased. Knowledge and experience acquired by the National Security Authority through the penetration testing may be used in the further development of the National Security Authority's general security work.

The National Security Authority shall issue a report to the undertaking on the results of the check. The report shall only contain information which may help to improve the undertaking's security.

The King may issue regulations on the penetration of critical national information systems, and regulations authorising the performance of such checks by parties other than the National Security Authority.

Section 6-6.*Communication and content monitoring of information systems*

An undertaking may ask the National Security Authority to check whether its information systems process classified information beyond the scope permitted by the system's security approval. The undertakings' employees must be informed that such a check may be performed.

The National Security Authority may perform the check by intercepting and reading information which is processed by or sent between information systems.

The check shall not encompass private communications or communications with undertakings which are not covered by the act. If the check nevertheless intercepts such communications, the check shall be stopped immediately, and information to which the check has secured access shall be erased.

All persons who have access to information as specified in the third paragraph in connection with work or service for the National Security Authority have a duty of secrecy in respect of the content of such information.

The National Security Authority shall notify the management of the undertaking of the methods to be used in the check and the National Security Authority's assessment of the risk that the check may intercept communications as specified in the third paragraph. If the management of the undertaking concludes that the objective of information system security cannot justify the methods and the risk, the check shall not be performed.

Information to which the check provides access may only be used for the purpose of the check. When the information is no longer required, it shall be erased. Knowledge and experience acquired by the National Security Authority through the check may be used in the further development of the National Security Authority's general security work.

The National Security Authority shall issue a report to the undertaking on the results of the check. The report shall only contain information which may help to improve the undertaking's security.

The King may issue regulations on communication and content monitoring of information systems, and regulations authorising the performance of such checks by parties other than the National Security Authority.

Chapter 7. Object and infrastructure security

Section 7-1.*Critical national objects and infrastructure*

Objects and infrastructure are nationally critical if fundamental national functions may be harmed if their functionality is reduced or they are subjected to vandalism, damage or unlawful seizure.

Ministries shall designate, classify and maintain an overview of critical national objects and infrastructure in their areas of responsibility. All identified and classified objects and infrastructure shall be notified to the National Security Authority together with a specification of the classification category.

The National Security Authority shall identify, classify and maintain an overview of critical national objects and infrastructure which do not fall within the area of responsibility of any ministry.

Undertakings which control objects or infrastructure identified pursuant to the second or third paragraph shall be notified of such identification.

Decisions on identification and classification which affect an independent natural or legal person may be appealed. The ministry is the body of appeal in respect of decisions made by the National Security Authority.

The National Security Authority may on its own initiative propose to a ministry that the ministry make a decision pursuant to the second paragraph. If the ministry does not make a decision in accordance with the proposal of the National Security Authority, the National Security Authority may submit the matter to the ministry which has overall responsibility for protective security work in the civilian sector or the ministry which has overall responsibility for protective security work in the defence sector for a final decision.

The King may issue regulations on the identification of objects and infrastructure, and regulations on notification of the National Security Authority.

Section 7-2.*Classification of critical national objects and infrastructure*

Critical national objects and infrastructure shall be classified if fundamental national functions may be harmed if their functionality is reduced or they are subjected to vandalism, damage or unlawful seizure. The following classification categories shall be used:

a) HIGHLY CRITICAL if critical adverse consequences could result

b) CRITICAL if serious adverse consequences could result

c) IMPORTANT if adverse consequences could result.

The classification shall be based on a damage potential assessment, and the fundamental national functions supported by the object or infrastructure and the consequences of reduced functionality shall be specified. The reasons for the classification shall be included in the overviews of critical national objects and infrastructure prepared by the ministries and the National Security Authority.

If part of an object or item of infrastructure has a higher classification than the rest of the object or item of infrastructure, that part shall be defined as an independent object or item of infrastructure.

The King may issue regulations on the classification of critical national objects and infrastructure.

Section 7-3.*Protection of objects and infrastructure*

Undertakings shall implement necessary security measures to maintain an appropriate level of security. Such security measures may include

a) physical, electronic, human or organisational barriers,

b) systems designed to detect and give warnings about activities or incidents,

c) systems and procedures designed to clarify activities and incidents and the background to them,

d) monitoring of undesirable activities and undesirable incidents, or

e) a combination of the measures specified in a) to d).

Undertakings shall conduct a risk assessment to determine what measures are needed to protect the object or infrastructure.

Protection of objects and infrastructure may also include a requirement for access clearance pursuant to section 8-3.

The King may issue regulations on the protection of objects and infrastructure at each classification level, and regulations on the use of security forces.

Section 7-4. *Testing of security measures*

An undertaking may ask the National Security Authority to attempt to overcome established security measures in order to gain access to critical national objects or infrastructure. The purpose must be to check whether security measures are adequate. The undertakings' employees must be informed that such a check may be performed.

If the check entails the processing of personal data, the check shall not be more extensive than necessary for the purpose.

Information to which the check provides access may only be used for the purpose of the check. When the information is no longer required, it shall be erased. Knowledge and experience acquired by the National Security Authority through the check may be used in the further development of the National Security Authority's general security work.

The National Security Authority shall issue a report to the undertaking on the results of the check. The report shall only contain information which may help to improve the undertaking's security.

The King may issue regulations on the testing of security measures related to critical national objects and infrastructure, and regulations authorising the performance of such testing by parties other than the National Security Authority.

Section 7-5. *Prohibition against accessing locations and areas*

In the interests of defence, security and contingency preparedness, the King may issue regulations on or make individual decisions providing that persons may not

a) access or stay in the vicinity of military areas

b) access or stay in the vicinity of specified locations or areas

c) observe military exercises or tests, military operations or other military activity.

Chapter 8. Personnel security

Section 8-1.*Requirement for security clearance, access clearance and authorisation*

Persons who are to have access to classified information shall be authorised in accordance with section 8-9. The same applies to persons who are to have access to critical national objects and infrastructure in respect of which a decision has been made pursuant to section 8-3.

Persons who are to be authorised for access to information with a classification of CONFIDENTIAL or above must hold a valid security clearance. Persons who are to be authorised for access to critical national objects and infrastructure in respect of which a decision has been made pursuant to section 8-3 must hold valid access clearance.

The King may issue regulations on the processing of clearance cases and the validity period of clearances.

Section 8-2.*Security clearance*

Persons shall require security clearance if they are to have access to information with a classification of CONFIDENTIAL or above pursuant to section 5-3.

The same applies to persons who may gain access to such information through their work. However, security clearance shall not be undertaken if the risk that such persons may gain access to such information can be eliminated through other, simpler security measures.

The King may issue regulations on the relationship between national security classification levels and the security classification levels used by NATO, other countries or international organisations.

Section 8-3.*Access clearance*

Within its area of responsibility, a ministry may decide that access clearance is required for access to all or parts of critical national objects or infrastructure. The National Security Authority may make such decisions with respect to undertakings which do not fall within the area of responsibility of any ministry.

No decision requiring access clearance shall be made if other suitable security measures can be implemented.

A decision requiring access clearance which affects an independent natural or legal person may be appealed.

Persons may be granted access clearance if they are to have access to objects or infrastructure classified pursuant to section 7-2. The ministry may decide that persons holding a particular level of security clearance shall also be cleared for access to a specified critical national object or specified critical national infrastructure.

The King may issue regulations on decisions requiring access clearance and the relationship between access clearance and security clearance.

Section 8-4.*Clearance decisions*

A person may only be cleared if there are no reasonable grounds for doubting the persons suitability related to security. Clearance decisions are made by the clearance authority.

In the assessment of suitability related to security, emphasis shall be given to circumstances relevant to the person's reliability, loyalty and judgment in connection with the processing of classified information and access to critical national objects and infrastructure. The assessment shall be based on vetting.

The clearance authority shall ensure that clearance cases are elucidated as well as possible. If there is doubt about whether a person is suitable for security clearance, the clearance authority shall conduct a security interview with the person.

Emphasis may be given to information related to the following circumstances:

a) espionage, planning or committing acts of terrorism, sabotage, assassinations or similar acts, and attempts to engage in such activities

b) criminal acts or preparing for or inciting criminal acts

c) circumstances which may cause the person, or that person's associates, to be subjected to threats against their life, health, freedom or honour, such that the person may be coerced into acting contrary to national security interests

d) falsification or incorrect or non-presentation of factual circumstances which the person had to understand to be relevant to their security clearance

e) abuse of alcohol or other intoxicants

f) any illness that on medical grounds temporarily or permanently may reduce reliability, loyalty or judgment

g) compromise of critical national information or breach of security provisions

h) refusal or failure by the person to provide personal data

i) failure to notify the authorisation authority of personal circumstances relevant to security

j) refusal to make a pledge of secrecy, a statement confirming a desire not to be bound by a pledge of secrecy or refusal or failure to participate in a security interview

k) financial circumstances which might tempt the person to act contrary to national security interests

l) connections with organisations which have an unlawful purpose and which may threaten the democratic social order or which regard violence and terrorism as acceptable instruments

m) inability to perform satisfactory vetting

n) ties with other countries

o) other circumstances which may give reason to fear that a person may act contrary to national security interests.

In the assessment of whether a person is suitable for security clearance, no emphasis shall be given to political engagement and other lawful social participation, such as membership of, sympathising with or activities on behalf of lawful political parties or organisations.

Emphasis may only be given to information about associated persons if it is relevant from a security perspective.

The King may issue regulations on clearance and the conduct of security interviews.

Section 8-5.*Conduct of vetting*

The National Security Authority shall vet all persons requiring clearance.

The person requiring clearance must have consented to vetting. Such consent shall include re-vetting pursuant to the third paragraph. Vetting shall be conducted at the request of the clearance authority unless the National Security Authority has decided otherwise.

The clearance authority shall wherever necessary request re-vetting within the validity period of a clearance.

Vetting shall cover information provided by the person requiring clearance. The person shall have a duty to provide complete information on circumstances which may be relevant in the assessment of whether the person is suitable for security clearance. A clearance case may be closed without a substantive decision if a person fails to respond to enquiries by the clearance authority.

If the person requires security clearance at the security classification level SECRET or higher, or is to be cleared for access to objects or infrastructure classified as HIGHLY CRITICAL, and in other special cases, vetting may be conducted in respect of associated persons.

Vetting shall also cover other information in the possession of the clearance authority, and information from relevant registers. It may also cover information from other sources, such as public authorities, places of service, workplaces and other references.

No information shall be gathered, registered or passed on which concerns political engagement as specified in section 8-4, fifth paragraph.

The controller of relevant registers has a duty to release records information irrespective of any duty of secrecy. Records information shall be notified in writing. No payment may be demanded in respect of such register information.

The controller of relevant registers shall facilitate digital transfer of records information to the National Security Authority.

Information received by the clearance authority in connection with vetting shall not be used for purposes other than assessment of whether the person is suitable for security clearance. However, the clearance authority may release information to the authorisation authority if necessary for security monitoring of the person.

The King may issue regulations on

a) vetting of associates

b) re-vetting

c) which registers are relevant in the context of vetting

d) the procedure for records checks abroad

e) the release of information in connection with corresponding vetting conducted by the authorities in other countries

f) the archiving, storage, despatch and digital transfer of vetting information.

Section 8-6.*Application of clearance on terms*

In special cases, clearance on terms may be granted, for example restriction to one specific position.

The King may issue regulations on the application of conditions for clearance.

Section 8-7.*Clearance of persons holding foreign citizenship*

A person holding foreign citizenship may be granted clearance following an individual overall assessment, provided that there are no reasonable grounds for doubting that the person is suitable for security clearance. In addition to the circumstances specified in section 8-4, the assessment shall emphasise the security-related significance of the home state, the person's ties with the home state and ties with Norway.

When conducting clearance of a person holding foreign citizenship, special consideration shall be given to whether risk may be reduced through the application of conditions, for example position clearance.

The King may issue regulations on clearance of persons holding foreign citizenship.

Section 8-8.*Revocation, downgrading or suspension of clearance*

If the clearance authority receives information giving grounds for doubting whether a cleared person is suitable for security clearance, the clearance authority shall consider revoking or downgrading the clearance, or suspend the clearance and implement further investigations. The authorisation authority shall be notified immediately of any decision to revoke, restrict or suspend a clearance. The clearance authority shall give the National Security Authority notice of the decision, which shall include a statement of reasons.

Section 8-9.*Authorisation*

The head of the undertaking constitutes the authorisation authority, and is responsible for security-related management and control of authorised persons.

An authorisation interview shall be held before authorisation is granted. Authorisation may only be granted if the authorisation authority is not in possession of information giving reasonable grounds for doubting whether a person is suitable for access to classified information or critical national objects and infrastructure.

The National Security Authority may require the undertaking to keep the National Security Authority informed of persons authorised.

The King may issue regulations on authorisation, the duties of the authorisation authority and the duty of the undertaking to keep the National Security Authority informed of the identities of authorised persons.

Section 8-10.*Downgrading, suspension and revocation of authorisation*

If the authorisation authority receives information giving reasonable grounds for doubting an authorised persons suitability related to security, the authorisation authority shall assess whether the authorisation should be maintained, revoked, downgraded or suspended. The authorisation authority shall notify the clearance authority of the decision.

An authorisation shall lapse if

a) the person leaves the position to which the authorisation relates

b) the need for authorisation is no longer present

c) the person no longer holds adequate clearance.

Section 8-11.*Duty to give notice of circumstances which may affect suitability related to security*

A cleared and authorised person shall immediately notify the authorisation authority of circumstances which may be relevant to whether the person is suitable for access to classified information or critical national objects and infrastructure.

Section 8-12.*Release of information to the Police Security Service*

In clearance cases where persons have ties with other states, the National Security Authority shall at the request of the Police Security Service provide information about persons' clearance status, ties with other states, place of service or which undertaking has requested clearance.

Information may only be released pursuant to the first paragraph when the Police Security Service states this to be necessary for performance of the service's tasks pursuant to section 17 b and section 17 c (1) of the Police Act.

The King may issue regulations on the release of information to the Police Security Service in clearance cases.

Section 8-13.*Reasons for and notice of decisions in clearance cases*

Any person who has been assessed for clearance is entitled to know the outcome of the assessment. If it is decided that the person should not be granted the desired clearance, the clearance authority shall on its own initiative notify the person of the outcome and the reasons for it. The clearance authority shall also give notice of the right to appeal the decision.

The statement of reasons shall not include information which may reveal circumstances

a) which are relevant to national security interests

b) which are relevant for the protection of sources

c) of which the person should not gain knowledge in the interests of their health

d) which concern the person's associates and of which the person should not gain knowledge

e) which concern technical installations, production methods, business analyses and calculations, and business secrets otherwise, provided that these are such that third parties could exploit them in a commercial context.

The clearance authority shall prepare an internal statement of reasons which specifies all relevant circumstances.

Chapters IV and V of the Public Administration Act does not apply to clearance or authorisation decisions.

Section 8-14.*Disclosure in clearance cases*

Once a clearance decision has been made, the person who has been assessed for clearance is entitled to examine the case documents.

The person is not entitled to disclosure of all or parts of documents which contain information as specified in section 8-13, second paragraph. Nor is the person entitled to disclosure of documents prepared as part of the internal case preparations of the clearance authority or the body of appeal. The exception in the second paragraph does not apply to factual information or summaries or other processed forms of factual information.

A person entitled to disclosure shall be provided with copies of the documents if he or she so requests.

The King may issue regulations on disclosure in clearance cases.

Section 8-15.*Despatch to a specifically appointed lawyer*

A person who has received a statement of reasons pursuant to section 8-13, first paragraph, from which information as specified in section 8-13, second paragraph, has been omitted, or who has had a request for disclosure pursuant to section 8-14, second paragraph, first sentence, refused is entitled to the assistance of a specifically appointed lawyer.

The lawyer shall be granted access to factual case information and the parts of the statement of reasons which are unknown to the person who has been assessed for clearance, but not to documents prepared for the purposes of the internal preparation of the case by the clearance authority or the body of appeal.

The lawyer shall advise the person assessed for clearance on whether he or she should appeal.

The ministry appoints lawyers, who shall require security clearance at the highest level.

The King may issue regulations on entitlement to the assistance of a lawyer, the appointment of lawyers and the information to which such lawyers may have access.

Section 8-16.*Clearance authorities and central register of clearance decisions*

The King will appoint one clearance authority for the defence sector and one for civilian sectors. The intelligence and security services will clear their own personnel.

When special reasons so indicate, the King may appoint clearance authorities other than those specified in the first paragraph.

The King may issue regulations on the establishment of a central register of clearance decisions.

Section 8-17.*Appeals related to clearance decisions*

A decision concerning clearance, clearance on terms or determination of the earliest date for re-opening a clearance case may be appealed by the person to whom the decision relates. The same applies to refusal to provide a statement of reasons and refusal of a disclosure request.

The appeal shall be submitted to the clearance authority. The National Security Authority is the body of appeal. The ministry is the body of appeal in respect of clearance decisions made by the National Security Authority at first instance.

The appeal deadline is three weeks from the date on which the recipient receives the notice of decision. The appeal deadline is interrupted by any appeal against refusal to provide a statement of reasons or refusal of a disclosure request. A new appeal deadline relating to the clearance decision starts on the date the body of appeal's decision is received or the recipient is otherwise notified of it. In cases where a lawyer has reviewed the case pursuant to section 8-15, a new appeal deadline runs as of the date on which the recipient receives the lawyer's advice.

Chapter VI of the Public Administration Act applies in clearance cases unless otherwise provided in or pursuant to this act.

Chapter 9. Classified procurements, etc.

Section 9-1.*Classified procurements*

A classified procurement is a procurement where the supplier of the good or service may gain access to or produces classified information, see section 5-3, or may gain access to a critical national object or infrastructure, see section 7-1.

Section 9-2.*Security agreements with suppliers*

A classified procurement may only be implemented if the undertaking's agreement with the supplier includes a security agreement. If a foreign supplier or its personnel have to be cleared or granted access to classified information, the National Security Authority shall approve the supplier before the agreement is entered into.

The security agreement shall clarify and specify the parties' duties and responsibilities pursuant to the act. The security agreement shall always specify the security classification level of the procurement, see sections 5-3 and 7-2, specified for each part of the assignment, and how the supplier is to comply with the requirements of the act which apply to the procurement.

Unless otherwise provided in the security agreement, the supplier must cover the cost of compliance with requirements which follow from the provisions of the act.

The King may issue regulations on the content of a security agreement and on exceptions to the requirement for a security agreement.

Section 9-3.*Facility security clearance*

Before a supplier may be granted access to information with a classification of CONFIDENTIAL or higher, the supplier must hold valid clearance for the specified security classification level. The supplier shall also be cleared if necessary for other reasons.

A facility security clearance shall only be issued if there are no reasonable grounds for doubting that the supplier is suitable for security clearance. In the assessment, emphasis shall only be given to circumstances which may affect the supplier's ability and willingness to perform protective security work pursuant to the act. The assessment basis shall include vetting of persons who are members of the supplier's board and management.

The supplier shall provide the clearance authority with all information which may be relevant to the facility security clearance.

The supplier shall notify the clearance authority as soon as possible of changes to its board or management, changes to its ownership structure, the relocation of offices and equipment, the commencement of debt settlement proceedings, any bankruptcy petition and other circumstances which may affect the assessment as to whether the supplier is suitable for security clearance. If a security risk arises which cannot be eliminated through protective security measures, the clearance authority may rescind the facility security clearance. Classified information or critical national objects or infrastructure may

not be transferred to a new owner or be included in the administration of the estate in connection with debt settlement proceedings or bankruptcy unless the clearance authority has consented to this.

The provisions of Chapter 8 otherwise apply insofar as they are relevant.

The King will appoint a clearance authority for facility security clearance. The King may issue regulations on requirements related to facility security clearance and the duration of the clearance.

Section 9-4.*Duty to give notice and authority to make decisions in connection with procurements for use in critical national information systems, objects and infrastructure*

In the context of procurements for use in a critical national information system, object or infrastructure, the undertaking shall assess whether the procurement may present a not insignificant risk that the information system, object or infrastructure may be affected by or be used in activities which present a threat to security. The duty to conduct such an assessment does not apply if it is obvious that the procurement does not present any such risk.

The undertaking shall notify the ministry if the assessment shows that the procurement presents a risk as specified in the first paragraph. Undertakings which are not subject to any ministry shall notify the National Security Authority. The duty to give notice applies irrespective of any duty of secrecy. The duty does not apply if the undertaking itself implements measures which eliminate the risk or render it insignificant.

The ministry which is notified pursuant to the second paragraph may ask relevant bodies to comment on the risk associated with the procurement and the supplier's reliability in security terms.

If a procurement for use in a critical national information system, object or infrastructure may present a not insignificant risk as specified in the first paragraph, the King in Council may decide that the procurement shall not be implemented, or that it shall be subject to conditions. This applies even if an agreement has been entered into in relation to the procurement. If no decision is made pursuant to the first sentence, the ministry shall notify the undertaking accordingly. A decision pursuant to the first sentence constitutes a special ground for enforcement pursuant to Chapter 13 of the Enforcement Act.

The King in Council may issue regulations on the duty to give notice and on authority to make decisions.

Chapter 10. Restrictions on ownership

Section 10-1.*Duty to notify in connection with acquisition of an undertaking*

Any person who wishes to acquire a qualified ownership interest in an undertaking which is subject to the act, see section 1-3, shall notify the ministry accordingly. In cases where the undertaking does not fall within the area of responsibility of any ministry, such notice shall be given to the National Security Authority.

A qualified ownership interest exists if the acquisition will, overall, give the acquirer, either directly or indirectly,

a) at least one-third of the share capital, participating interests or votes in the undertaking

b) the right to own at least one-third of the share capital or participating interests, or

c) significant influence over the management of the company otherwise.

Shares which are owned or taken over by the shareholder's associates have the same status as the shareholder's own shares; see section 2-5 of the Securities Trading Act. The same applies to participating interests which are owned or taken over by associates of the owner of the participating interests.

The King may issue regulations on the duty to notify.

Section 10-2.*Processing of notice of acquisition of undertaking*

The ministry or the National Security Authority which receives a notice pursuant to section 10-1 shall make a decision on the notice as soon as possible.

Any person who receives a notice pursuant to section 10-1 may ask relevant bodies to comment on the potential risks associated with the acquisition and the acquirer's reliability in security terms.

Within 60 working days, the ministry or the National Security Authority shall notify the party which has given notice that the acquisition has been approved or that the matter will be considered by the King in Council pursuant to section 10-3. The period shall be calculated as of the date on which the ministry or the National Security Authority received such notice. If the ministry or the National Security Authority submits a written request for further information within 50 working days, the period shall be suspended until the acquirer's reply is received.

The King may issue regulations on processing of the notice by ministries and the National Security Authority.

Section 10-3.*Decision to prohibit acquisition of an undertaking*

If an acquisition pursuant to section 10-1 may present a not insignificant risk of a threat to national security interests, the King in Council may decide that the acquisition shall not be implemented, or that implementation shall be subject to conditions. This applies even

if an agreement has been entered into in relation to the acquisition. If no decision is made pursuant to the first sentence, the ministry shall notify the acquirer accordingly.

A decision pursuant to the first sentence constitutes a special ground for enforcement pursuant to Chapter 13 of the Enforcement Act.

The King may issue regulations on the prohibition of acquisition of an undertaking.

Chapter 11. Special oversight arrangements. Coercive fines, fines and legal penalties

Section 11-1.*Special oversight arrangements*

Protective security work pursuant to the act is subject to the control and supervision of the Parliamentary Intelligence Oversight Committee in accordance with provisions laid down in and pursuant to the Intelligence Services Oversight Act.

Section 11-2.*Coercive fines*

In the event of contravention of provisions laid down in or pursuant to sections 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, section 9-2, first paragraph, section 9-4, first paragraph, first sentence, or section 9-4, second paragraph, first or second sentence, the supervisory authority may impose a coercive fine, which shall accrue until the matter has been rectified. The same applies to instructions issued pursuant to section 3-6.

A decision on a coercive fine may be appealed to the ministry.

A decision pursuant to the first paragraph constitutes a special ground for enforcement pursuant to Chapter 13 of the Enforcement Act.

The King may issue regulations on coercive fines.

Section 11-3.*Fines*

The supervisory authority may impose a fine on an undertaking if the undertaking or any person acting on its behalf intentionally or negligently

a) contravenes provisions laid down in or pursuant to sections 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, 9-2, first paragraph, 9-4, first paragraph, first sentence, or section 9-4, second paragraph, first or second sentence

b) contravenes instructions issued pursuant to section 3-6

c) provides incorrect or incomplete information to the supervisory authority pursuant to sections 3-4 or 4-5

d) contributes to contraventions as specified in a to c.

When setting the size of the fine, particular emphasis shall be given to the grossness of the contravention, the duration of the contravention, demonstrated culpability and the turnover of the undertaking. A decision to impose a fine constitutes a special ground for enforcement pursuant to Chapter 13 of the Enforcement Act.

The power to impose a fine shall be subject to a five-year limitation period. The limitation period shall be interrupted if the supervisory authority notifies the undertaking that it is suspected of contravention of the act or a decision made pursuant to the act.

A decision to impose a fine may be appealed til the ministry.

The King may issue regulations on fines.

Section 11-4.*Legal penalties*

A penalty of a fine or imprisonment for a term not exceeding six months, or both, shall be applied to any person who intentionally or negligently contravenes provisions laid down in or pursuant to section 3-4, 4-3 or section 5-2, section 5-3, first paragraph, sections 6-2, 6-3 or 7-3, section 9-2, first paragraph, section 9-4, first paragraph, first sentence, or section 9-4, second paragraph, first or second sentence, or who contravenes instructions issued by the supervisory authority pursuant to section 3-6, unless the matter is covered by a stricter penal provision.

A penalty of a fine or imprisonment for a term not exceeding one year, or both, shall be applied to any person who intentionally or with gross negligence breaches a duty of secrecy pursuant to section 5-4, second paragraph, or section 6-6, fifth paragraph, unless the matter is covered by a stricter penal provision.

A penalty of a fine or imprisonment for a term not exceeding one year, or both, shall be applied to any person who contravenes a prohibition issued pursuant to section 7-5, unless the matter is covered by a stricter penal provision.

The same penalties shall be imposed in respect of attempted contraventions as specified in the first to third paragraphs.

Chapter 12. Entry into force and amendment of other acts

Section 12-1.*Entry into force*

The act shall enter into force on the date decided by the King.[1] The King may provide that difference provisions shall enter into force on different dates.

1 As of 1 January 2019 in accordance with res. 20 December 2018 No. 2052.

Section 12-2.*Repeal*

As of the date the present act enters into force, the Act of 20 March 1998 No. 10 relating to Protective Security Services shall be repealed.