Act of 20 March 1998 No. 10 relating to Protective Security Services (the Security Act)

Chapter 1. General provisions

Section 1. ***The purpose of the Act***

The purpose of this Act is to:

a) take steps enabling the effective countering of threats to the independence and security of the realm and other vital national security interests,
b) safeguard the constitutional rights of individuals,
c) assure trust in and simplify the basic system for overseeing protective security services.

Section 2. ***The general scope of the Act***

This Act applies to administrative agencies. In terms of this Act, an administrative agency means any agency of the state or a municipality. In doubtful cases the King may decide whether an agency is to be regarded as an administrative agency. The King may also decide that an administrative agency shall wholly or partly be exempt from this Act when there are special reasons for so doing, and may in such cases lay down special rules instead.

This Act also applies to any legal person who is not an administrative agency and who is a supplier of goods or services to an administrative agency in connection with a classified procurement.

The King may decide that this Act shall wholly or partly also apply to any other legal person, including individuals, associations, foundations, companies, and private and public business enterprises,

a) who owns or otherwise controls or supervises a sensitive object, or
b) who is granted access to classified information by an administrative agency.

This Act applies to courts of law along with the special rules ensuing from the provisions regarding security clearance and authorization laid down in and pursuant to the Courts of Justice Act and the Criminal Procedure Act. The King may lay down further special rules.

This Act does not apply to the Storting, the Office of the Auditor General, the Storting's Ombudsman for Public Administration and other agencies of the Storting.

This Act applies to Svalbard and Jan Mayen insofar as the King so decides.

Section 3. *Definitions*

For the purposes of this Act, the following definitions shall apply:

1. Protective security services: the planning, preparation, implementation and overseeing of protective security measures which seek to eliminate or reduce risk resulting from an activity that poses a threat to security.
2. Activity that poses a threat to security: preparation for, attempt at and implementation of espionage, sabotage or acts of terrorism, and complicity in such activity.
3. Espionage: gathering of information by covert means for intelligence purposes
4. Sabotage: the intentional destruction, paralysis or operational shutdown of equipment, materiel, installations or activity, or the intentional neutralization of persons, carried out by or for a foreign state, organization or group.
5. Acts of terrorism: the unlawful use of, or threat to make use of, power or violence against persons or property, in an attempt to put pressure on the country's authorities or population or society at large in order to achieve political, religious or ideological goals.

6. Enterprise: an administrative agency or other legal person to whom this Act applies, cf. section 2
7. Information: any type of information in material or intangible form.
8. Sensitive information: information which shall be marked with a security classification pursuant to the provisions of section 11 of this Act.
9. Classified information: information which is marked with a security classification pursuant to the provisions of section 11 of this Act.
10. Information system: an organized collection of peripheral equipment, software, hardware and communication networks that link them together.
11. Monitoring: eavesdropping or deciphering of electronic signals that are communicated within or between information systems.
12. Sensitive object: property that must be protected against activity that poses a threat to security in the interests of the security of the realm or of allies or other vital national security interests.
13. Procurement authority: an administrative agency which intends to procure, or has procured, goods or services from a legal person who is not an administrative agency.
14. Classified procurement: procurement, undertaken by a procurement authority, which entails that the supplier of the goods or service will be given access to sensitive information or a sensitive object, or which entails that the procurement must be classified for other reasons.
15. Vetting: gathering of relevant information for the assessment of security clearance.
16. Security clearance: a decision, made by the clearing authority and based on vetting, regarding the presumed suitability of a person for a given security classification.
17. Authorization: decision, made by the person responsible for granting authorization, to the effect that a person, subject to prior security clearance (except for access to information classified as RESTRICTED), assessment of his or her knowledge of security provisions, official needs and submission of a written pledge of secrecy, shall be granted access to information with a specified classification.

Chapter 2. General provisions regarding responsibility for and performance of protective security services

Section 4. *Overall responsibility*

The Ministry has the overall responsibility for protective security services. This does not limit the responsibility and duties of individuals pursuant to the provisions laid down in or pursuant to this Act.

The executive functions of the Ministry shall be carried out by the National Security Authority.

Section 5. *Duties of individual enterprises*

Each enterprise has a duty to implement protective security services pursuant to the provisions laid down in or pursuant to this Act.

The enterprise shall

a) draw up internal instructions in order to safeguard security,
b) ensure that persons employed or engaged in the enterprise receive adequate training in security issues, and
c) regularly check the state of security in the enterprise.

The responsibility rests with the head of the enterprise. If executive functions are delegated internally in the enterprise, this shall be done in writing.

All persons employed or engaged in the enterprise are responsible for observing security considerations in their work or assignments for the enterprise, and have a duty to assist the protective security services.

Further provisions will be laid down by the National Security Authority.

Section 6. *General provisions regarding the performance of protective security services*

When the performance of protective security services in accordance with or pursuant to this Act is left to the discretion of the person responsible, the means and methods used shall involve no more interference than appears to be necessary in relation to the security risk in question and other circumstances.

When performing protective security services, particular consideration shall be shown for the constitutional rights of individuals.

Section 7. *Cooperation*

The King will lay down provisions regarding national, regional and local cooperation on protective security services.

Chapter 3. The National Security Authority

Section 8. *General functions*

The National Security Authority shall coordinate protective security measures and oversee the state of security. The National Security Authority is also the executive body in relation to other countries and international organizations.

Section 9. *Further provisions as to functions*

The National Security Authority shall

a. collect and evaluate information of significance for the implementation of protective security services,
b. seek to enter into international cooperation, including cooperation with analagous services of other countries and organizations, when this serves Norwegian interests,
c. supervise the state of security in enterprises, including checking whether the duties of individuals laid down in or pursuant to this Act are fulfilled, and if necessary giving orders for improvements,
d. contribute towards the development of security measures, including initiating research and development in areas of significance for protective security services,
e. provide information, advice and guidance to enterprises, and
f. otherwise carry out the functions that follow from the provisions laid down in and pursuant to this Act.

The King may make further provisions regarding the National Security Authority's performance of its functions.

Section 10. *The National Security Authority's right of access*

Insofar as is necessary for implementing the supervisory functions laid down in or pursuant to this Act, the National Security Authority shall be given unhampered access to any area where there is sensitive information or a sensitive object, if the area is owned, used or otherwise controlled by an enterprise.

Chapter 4. Information security

Section 11. *Security classification*

When information must be protected for security reasons, one of the following security classifications shall be used:

a. TOP SECRET shall be used if it might have absolutely decisive adverse consequences for the security of Norway or its allies, its relationship with foreign powers or other vital national security interests if the information were to become known to unauthorized persons.
b. SECRET shall be used if it could seriously harm the security of Norway or its allies, its relationship with foreign powers or other vital national security interests if the information were to become known to unauthorized persons.
c. CONFIDENTIAL shall be used if it could harm the security of Norway or its allies, its relationship with foreign powers or other vital national security interests if the information were to become known to unauthorized persons.
d. RESTRICTED shall be used if it could to any extent entail adverse consequences for the security of Norway or its allies, its relationship with foreign powers or other vital national security interests if the information were to become known to unauthorized persons.

The person who issues or otherwise produces sensitive information shall ensure that the information is marked with the appropriate security classification. Security classification shall not be carried out to a greater extent than is strictly necessary, and the security classification used shall be no higher than necessary.

Security classification shall not be made effective for longer than is strictly necessary, and the classification shall cease to apply after not more than 30 years. Further rules regarding downgrading of classification and declassification will be prescribed by the King. For special cases, the King may make exceptions from the 30-year rule set out in the first sentence.

Provided that there is reciprocity, the King may make an agreement with a foreign state or international organization concerning the security classification of information received that is so classified by the state or international organization in question, and concerning the obligation to take steps to secure such information.

Section 12. *Duty to protect classified information*

Any person who gains access to classified information in the course of his or her work, assignment or office for an enterprise has a duty to prevent unauthorized persons from gaining knowledge of such information. The duty of secrecy also applies after the person in question has completed the work, assignment or term of office. Classified information shall only be released to persons who have an official need to have access to it. However, the duty of secrecy shall not preclude classified information from being given to other persons when this is specially authorized by statute or general regulations laid down by the King.

The King will make further rules regarding the handling of classified information, including registration, storage, transmission and destruction. The King may also make rules regarding the duty to take steps to ensure that classified information is correct, complete and accessible.

Section 13. Security-related approval of information systems

Before sensitive information is processed, stored or transmitted in an information system, the National Security Authority, or the person authorized by the National Security Authority, shall approve the system for the security classification concerned.

The National Security Authority is the certifying authority for information systems that are to handle sensitive information.

The National Security Authority may authorize other enterprises to perform services for securing information systems that are to handle sensitive information.

The National Security Authority will lay down further regulations regarding the security-related approval of information systems.

Section 14. *Cryptosecurity*

Only cryptosystems that have been approved by the National Security Authority are allowed to be used to protect sensitive information.

The National Security Authority is the national administrator of cryptomaterial and supplier of cryptosecurity services to enterprises. However, the National Security Authority may approve other suppliers of cryptosecurity services. The latter shall sign a special agreement to this effect with the National Security Authority.

The National Security Authority shall approve cryptoalgorithms that are used in equipment intended for export.

Further provisions will be laid down by the National Security Authority.

Section 15. *Monitoring and penetration of information systems*

An enterprise may allow the National Security Authority to check, by monitoring, whether information systems in the enterprise concerned store, process or transmit sensitive information without being authorized to do so. The employees of the enterprise are to be informed of such checking in advance. In no event shall monitoring cover private communications or communications that are transmitted to or from persons other than enterprises.

An enterprise may allow the National Security Authority to attempt and, as the case may be, to effect the penetration of information systems that store, process or transmit sensitive information, in order to check the resistance of the systems. The employees of the enterprise are to be informed of such checking in advance.

Information of which the National Security Authority gains knowledge in connection with checking pursuant to the first and second paragraphs shall be destroyed when it is no longer of significance for such checking.

The King will make further provisions, including provisions regarding notice and implementation of monitoring and penetration and regarding storage and destruction of information.

Section 16. *Technical security inspections*

The National Security Authority, or the person authorized by the National Security Authority, may carry out inspections of premises, buildings or other objects that are owned, used or otherwise controlled by an enterprise, with a view to ascertaining whether unauthorized persons with or without technical aids can gain access to sensitive information by means of visual surveillance/snooping*, eavesdropping or deciphering of electronic signals.

The King will make further regulations regarding the implementation of technical security inspections.

Chapter 5. Object security

Section 17. *Duty to protect sensitive objects*

The enterprise concerned has a duty to identify sensitive objects which the enterprise owns or otherwise controls or supervises, and to take the necessary protective security measures to protect sensitive objects from activities that pose a threat to security.

The King will make further provisions regarding the duty to protect sensitive objects. The King may also decide that security clearance is required pursuant to the provisions of Chapter 6 for any person who might gain access to a sensitive object.

Section 18. *Protection of foreign objects in Norway*

Provided there is reciprocity, the King may enter into an agreement with a foreign state or international organization concerning the duty to take steps to protect foreign objects in Norway that are deemed to be sensitive by the state or organization concerned.

Chapter 6. Security of personnel

Section 19. *When security clearance and authorization shall be carried out*

Any person who might gain access to sensitive information shall undergo prior security clearance and receive authorization as necessary.

Special security clearance is given for the following national security classifications, and if relevant, for corresponding security classifications in NATO or another international organization:

a. CONFIDENTIAL (if relevant, NATO CONFIDENTIAL/equivalent)
b. SECRET (if relevant, NATO SECRET/equivalent)
c. TOP SECRET (if relevant, COSMIC TOP SECRET/equivalent).

Access to information classified as RESTRICTED does not require security clearance, but the person concerned shall be authorized.

Section 20. *Vetting of personnel*

Vetting of personnel shall be carried out at the request of the person responsible for authorization, unless otherwise decided by the National Security Authority.

No vetting shall take place unless the person who is undergoing security clearance has been notified of and consented to such vetting being carried out. Vetting shall always cover information provided by the person concerned himself/herself. The latter has a duty to provide complete information regarding matters that might presumably be of significance for evaluating his/her suitability with respect to security pursuant to section 21.

In the case of security clearance for SECRET/equivalent or higher security classifications, and in other special cases, persons who have close family ties to the person concerned may be vetted.

Otherwise vetting shall cover information in the possession of the clearance authority concerned and searching of relevant public registers, cf. fifth paragraph, first sentence. The person responsible for the register has a duty to disclose information from the register notwithstanding the duty of secrecy. Information from the register shall be communicated in writing. Vetting may also cover other sources, including statements from places where the person being vetted has served or worked, public authorities or references that have been provided or are supplementary. Information for the purpose of vetting shall be provided to the clearance authority free of charge.

The King will decide which registers are relevant for vetting. The King will also lay down provisions regarding the procedure for inspection of registers abroad and regarding the disclosure of

information in connection with similar vetting by the authorities of other countries. Under no circumstances shall information regarding political involvement covered by section 21, second paragraph, be collected, registered or transmitted to other persons.

Information provided to the clearance authority in connection with vetting shall not be used for purposes other than the evaluation of security clearance. Such information may however be communicated to the person responsible for authorization if this is deemed to be necessary for the security-related management and control of the person concerned.

Section 21. *Basis of assessment for security clearance*

Security clearance shall only be given or maintained if there is no reasonable doubt as to the suitability of the person concerned with respect to security. When making a decision regarding such suitability, importance shall only be attached to matters that are relevant to evaluating the reliability, loyalty and sound judgement of the person concerned in relation to the handling of sensitive information. Importance may be attached to information regarding the following matters:

a: Espionage, planning or implementation of sabotage, an assassination or the like, or an attempt to carry out such activity.
b. Criminal acts or preparations for or the encouragement of such acts.
c. Factors that may lead to the person concerned himself or herself or persons who have close family ties with the person concerned being subjected to threats entailing a risk to life, limb, freedom or honour along with a risk of possible pressure on the person concerned to take action that is contrary to security interests.
d. Falsification or misrepresentation of or failure to present facts which the person concerned must have understood are of significance for the security clearance.
e. Abuse of alcohol or other intoxicants.
f. Any illness which may be deemed on medical grounds to be liable to result in the temporary or permanent impairment of reliability, loyalty or sound judgement.
g. Compromise of sensitive information, breach of specified security provisions, refusal to provide personal information regarding himself or herself, failure to keep the person responsible for authorization currently informed about personal matters of significance for security, refusal to take a pledge of secrecy, expression of a wish not to be bound by a pledge of secrecy or refusal to participate in a security interview.
h. Financial matters that may induce disloyalty.
i. Connection with domestic or foreign organizations which have illicit objectives, which may threaten the democratic social order or which consider violence or acts of terrorism to be acceptable means.
j. Lack of opportunity to carry out satisfactory vetting.
k. Other matters which may give reason to fear that the person concerned might act contrary to security interests.

Political involvement, including membership of, sympathy with or active support of lawful political parties or organizations or other lawful social involvement, shall not be of significance for the assessment of a person's suitability with respect to security.

Decisions regarding clearance shall be based on a case-by-case overall evaluation of the available information. The clearance authority shall seek to clarify unclear matters, if appropriate by conducting a security interview.

Negative information regarding closely related persons, cf. section 20, third paragraph, shall only be taken into consideration if it is assumed that the circumstances of the closely related person might affect the suitability of the person being vetted with respect to security.

Section 22. *Security clearance of foreign nationals*

Foreign nationals shall normally not be given security clearance. However, if there is a special need to give foreign nationals access to sensitive information, clearance may be given. In such cases, security clearance shall only be given after the opinion of the National Security Authority has been obtained.

Further rules regarding the security clearance of foreign nationals will be laid down by the King.

Section 23. *The clearance authority and the authorization authority*

Each individual ministry is the clearance authority for personnel within its sphere of authority. In special cases, the ministry may delegate clearance authority to subordinate enterprises which have an extensive need for clearance.

In connection with classified procurement effected by the ministry concerned or a subordinate agency or institution, the ministry is the clearance authority for personnel employed or engaged under contract by the supplier. The ministry may delegate the authority to the procurement authority to which clearance authority has been delegated pursuant to the first paragraph, second sentence.

The King will decide who shall be the clearance authority for other enterprises, including emergency preparedness personnel in county municipalities, municipalities and agencies or enterprises which are linked to them in connection with emergency preparedness.

The security clearance of foreign nationals may only be granted by the ministry concerned. Security clearance for COSMIC TOP SECRET or its equivalent may only be granted by the National Security Authority.

Authorization may be granted if the person responsible for granting authorization has no information that casts doubt on whether the person in question is reliable from the point of view of security. Authorization is normally given by the head of the enterprise. Authorization shall not be given before notice of security clearance has been received, except in such cases as are described in section 19, third paragraph, and a security interview has been held. The National Security Authority will issue further rules regarding authorization and regarding who is responsible for granting authorization.

Section 24. *Cessation, revocation, downgrading and suspension of security clearance and authorization*

Personnel who have been granted security clearance and authorization shall keep the person responsible for granting authorization informed of matters that are likely to be of significance for the suitability of the person concerned with respect to security.

Should information emerge that casts doubt on a security-cleared person's suitability with respect to security, the clearance authority shall consider revoking or downgrading the clearance, or suspending the clearance and initiating further investigations to clarify the matter.

If a decision is made to revoke, downgrade or suspend a security clearance, notice thereof stating the grounds for the decision shall be sent to the National Security Authority. The person responsible for granting authorization shall be notified immediately.

Authorization automatically ceases to have effect

a. when the person resigns from the position covered by the authorization

b. when, for other reasons, there is no longer a need for authorization, or
c. when the person concerned no longer has sufficient security clearance.

If the person responsible for granting authorization receives information that gives reason to doubt whether an authorized person may still be considered suitable in terms of security, consideration shall be given to revoking, reducing or suspending authorization. The subsequent decision shall be reported to the competent clearance authority.

The National Security Authority will determine the general term of validity for security clearances.

Section 25. *Grounds and appeal*

Chapters IV to VI of the Public Administration Act do not apply to decisions regarding security clearance or authorization.

Any person who has been evaluated for a security clearance is entitled to be informed of the result. In the case of negative decisions, the person concerned shall as a matter of course be notified of the result. Notification of a negative decision shall include information concerning the person's right to request the grounds for the decision and concerning the right of appeal.

The request for the grounds for the decision regarding security clearance shall be sent to the clearance authority. The clearance authority shall obtain the opinion of the National Security Authority before the grounds may be given. Grounds shall be given, unless this is precluded by due consideration for the protection of privacy or sources or for the protection of sensitive information.

Appeals against decisions regarding security clearance shall be sent to the competent clearance authority. The National Security Authority is the appeals body. The Ministry is the appeals body for clearance decisions made by the National Security Authority at first instance.

Section 26. *Supplementary provisions*

The King will prescribe regulations regarding the establishment of a central register for clearance decisions.

The National Security Authority will lay down supplementary provisions regarding personnel security, including

a. security clearance of specified categories of personnel, such as national servicemen in the Defence Forces,
b. archiving, storage and forwarding of documents in cases concerning clearance and vetting, and
c. conduct of security interviews.

Chapter 7. Classified procurement

Section 27. *Entry into a security agreement*

In the case of classified procurement, a security agreement shall be entered into between the procurement authority and the supplier. The security agreement shall have been entered into before the supplier may be given access to sensitive information. Security agreements may only be entered into with foreign suppliers subject to the approval of the National Security Authority. The National Security Authority may decide that a security agreement shall also be entered into if the supplier might gain access to a sensitive object or if it is necessary for other reasons to classify the procurement.

The security agreement shall determine further details regarding responsibility and duties pursuant to the provisions laid down in and pursuant to this Act, including

a. the security classification of the procurement, specified for the individual parts of the assignment,

b. the implementation in practice of investigations regarding the supplier and other screening of the latter in order to evaluate the security situation and check that the supplier is in compliance with the security provisions and other duties pursuant to this Act, and
c. consequences in the event of a breach of the security agreement.

Any expenses or requirements the supplier might have in order to fulfil the provisions laid down in or pursuant to this Act and the security agreement entered into are of no concern to the procuring authority and the National Security Authority, unless otherwise explicitly agreed in the security agreement.

Section 28. *Supplier clearance*

Before a supplier may be given access to sensitive information which is classified CONFIDENTIAL or higher, or if it is deemed necessary for other reasons, the supplier shall have a valid supplier clearance for the specified security classification. The supplier clearance applies to an individual assignment. The National Security Authority is the clearance authority.

No supplier clearance shall be given if there is a reasonable doubt as to the suitability of the supplier with respect to security. When making a decision regarding suitability with respect to security, importance shall only be attached to factors that are relevant to an evaluation of the supplier's ability and willingness to implement protective security services pursuant to the provisions laid down in or pursuant to this Act. The evaluation shall also comprise the vetting of persons in the Board of Directors and management of the supplier.

The supplier shall provide all information that is likely to be of importance in deciding the question of clearance.

The supplier shall without undue delay notify the National Security Authority of any changes in the Board of Directors or management, changes in the ownership structure, relocation of premises and equipment, institution of debt settlement proceedings or presentation of a bankruptcy petition and other matters that may be of significance for the suitability of the supplier with respect to security. If such matters are deemed to represent a security risk and the risk cannot be eliminated by implementing protective security services, the National Security Authority may revoke the supplier clearance. Sensitive information or objects may not be transferred to a new owner or form part of the administration of an estate in connection with debt settlement or bankruptcy proceedings unless the National Security Authority has consented thereto.

In all other respects, the provisions of Chapter 6, including the provisions regarding grounds and appeal, shall apply insofar as they are appropriate.

Section 29. *Supplementary provisions, etc.*

The King may lay down supplementary provisions regarding classified procurement, and lay down special rules for the implementation of international classified procurement.

Chapter 8. Control and supervisory arrangements. Penal provisions

Section 30. *Control and supervisory arrangements*

Protective security services pursuant to this Act are subject to the control and supervision of the Storting's Committee for the Scrutiny of Intelligence, Surveillance and Security Services, in accordance with the provisions laid down in and pursuant to Act of 3 February 1995 No. 7 relating to the scrutiny of intelligence, surveillance and security services.

The King may establish special arrangements for the control and supervision of the National Security Authority and the protective security services of other enterprises, for the purpose of ensuring that their activities are carried out within the framework of statutes, administrative or military directives and non-statutory law currently in force, or to ensure that the rule of law and other considerations are safeguarded.

Section 31. *Penalties*

Any person who wilfully or negligently contravenes provisions laid down in or pursuant to sections 5, 10, 12, second paragraph, 13, first and fourth paragraphs, 14, first, third and fourth paragraphs, and 17 of this Act, or contravenes orders issued by the National Security Authority pursuant to section 9, first paragraph, litra c of this Act, shall be liable to fines or imprisonment for a term not exceeding six months, unless the offence is covered by a more stringent penal provision. An accomplice shall be liable to the same penalty.

Any person who wilfully or through gross negligence contravenes section 11, second paragraph, first sentence, of this Act, shall be liable to fines or imprisonment for a term not exceeding one year, unless the offence is covered by a more stringent penal provision.

Chapter 9. Commencement of the Act and amendments to other Acts

Section 32. *Commencement*

This Act shall enter into force from the date decided by the King.

Section 33. *Amendments to other Acts*

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

1. Act of 13 August 1915 No. 5 relating to courts of justice (the Courts of Justice Act).

Section 12, third paragraph, first sentence, shall read:

In cases where information is provided which pursuant to the Security Act may only be made known to persons who are specially authorized, only judges who are authorized for the level of protection in question shall participate.

Section 21, third paragraph, first sentence, shall read.

In cases where information will be provided which pursuant to the Security Act can only be made known to persons who are specially authorized, only judges who are authorized for the level of protection in question shall participate.

Section 91, second paragraph, first sentence, shall read:

Jurors and lay judges who are to participate in a case in which information will be provided which pursuant to the Security Act can only be made known to persons who are specially authorized shall be passed over if they cannot be authorized for the level of protection in question.

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

Section 102, second paragraph, shall read:

The King will prescribe further rules concerning how the court shall proceed to appoint an official defence counsel in cases in which information will be given that pursuant to the Security Act can only be made known to persons who are specially authorized.

Section 141, second paragraph, shall read:

The King will prescribe further rules concerning how the court shall proceed to appoint experts in cases in which information will be given that pursuant to the Security Act can only be made known to persons who are specially authorized.