# Government Decree
## on information security in central government
## (681/2010)

### Chapter 1
### General provisions

#### Section 1
*Scope of application*

This Decree contains provisions on the general information security requirements applicable to the handling of documents by central government authorities, on the grounds for classifying documents, and on the information security requirements corresponding to the classification and applicable to the handling of documents.

#### Section 2
*Relationship to other legislation*

(1) The Act on the Openness of Government Activities (621/1999) contains provisions on the publicity of official documents, on the consideration of a request for access to such documents, and on the general obligations related to good practice on information management. Section 6 of the Act on International Information Security Obligations (588/2004) contains provisions on the secrecy obligation applicable to documents classified in accordance with international information security obligations.

(2) Subject to international information security obligations, this Decree shall apply to the handling of a document received from an authority of another country or from an international institution.

#### Section 3
*Definitions*

For the purposes of this Decree

(1) *central government authority* means a State administrative authority, another government agency or body, a court of law or another authority for administration of justice;

(2) *information security* means administrative, technical and other measures and arrangements to comply with secrecy obligations and restrictions on use related to information, as well as to ensure access to information and its integrity and availability;

(3) *secret document* means a document which is referred to in section 5(1) of the Act on the Openness of Government Activities and which, according to the Act or another act, shall be kept secret;

(4) *handling of a document* means receiving, preparing, recording, viewing, modifying, providing, copying, transferring, delivering, destroying, keeping or filing a document or any measure directed at a document by means of electronic data processing, sound or image reproduction equipment or other devices, or by other means;

(5)*international information security obligation* means an obligation which relates to the handling of secret documents, is based on an international treaty or statute and is binding on Finland;

(6)*sensitive personal data* means personal data under section 11 of the Personal Data Act (523/1999);

(7)*biometric data* means data which are used for identifying natural persons and individualise them on the basis of their physiological features or behaviour.

## Chapter 2
## **General information security requirements**

### Section 4
### *Basis for planning information security*

A central government authority shall ensure that its planning of information security pursuant to good practice on information management is based on inquiries and assessments conducted by it regarding documents in its possession and the significance of their contents, that the planning is conducted with account of the requirement to ensure good publicity and secrecy structures in information systems, and that the information security measures are geared with consideration of the significance and purpose of use of the information to be protected, of the threats against the documents and the information systems, and of the costs for the information security measures.

### Section 5
### *Implementing information security at basic level*

(1) In order to implement informationsecurity, a central government authority shall ensure that

(1) any informationsecurity risks connected with the activities of the central government authority are identified;

(2) thecentral government authority has sufficient expertise for ensuring informationsecurity, and the related duties and responsibility are defined;

(3) the duties and responsibilities related to the handling of documents are defined;

(4) access to and availability of information in different situations are safeguarded, and procedures are created to overcome exceptional situations;

(5) the secrecy and other protection of documents and the information contained therein are safeguarded by granting access to documents only to those who need secret information or personal data recorded in a personal data file for performing their work duties;

(6) unauthorised modification and other unauthorised or inappropriate processing of information is prevented by access rights management, access monitoring, and appropriate and sufficient security arrangements concerning information networks, information systems and information services;

(7) thepremises for data processing and storage of documents are sufficiently monitored and protected;

(8) the reliability of personnel and other persons performing tasks related to the handling of documents is ensured, if necessary, by means of a security clearance procedure and other means available by virtue of law;

(9) the personnel and other persons performing tasks related to the handling of documents are provided with instructions and training for the appropriate handling of documents and the information contained therein;

(10) compliance with given instructions is monitored, and the need to revise the instructions is assessed regularly.

(2) Section 26(2) of the Act on the Openness of Government Activities contains provisions on the obligation of central government authorities to ensure the protection of secret information when access to such information is provided for the performance of a commission. Moreover, section 32(2) of the Personal Data Act contains provisions on providing access to personal data recorded in personal data files.

Section 6
*Consideration of different handling stages*

Information security measures shall be planned and implemented so that they cover all stages of handling a document, ranging from the preparation or reception of the document to the filing or destruction thereof, including the provision and transfer of the document and the supervision of the handling. In the planning, compliance with data processing obligations shall be ensured also when data processing tasks are carried out on commission of central government authorities.

Section 7
*Compliance with classification criteriaand*

*corresponding information security requirements*

(1) If a central government authority has decided to classify its documents for information security, the classification shall comply with the criteria laid down in Chapter 3.

(2) The central government authority shall ensure that the classified documents prepared or received by it are handled in compliance with the requirements laid down in Chapter 4. However, notwithstanding the provisions above, the central government authority may, in its own activities, apply information security requirements exceeding the requirements of Chapter 4.

## Chapter 3
## **Classification of documents**

### Section 8
### *Classification criteria*

(1)Secret documents or the information contained therein may be classified according to the information security requirements to be complied with in handling them. The classification may also be conducted by applying the information security requirements only to those documents or those stages of handling of a document in respect of which special measures are needed because of the interest to be protected. The classification shall not be extended to documents or parts of documents in respect of which compliance with the handling requirements is not necessary because of the interest to be protected.

(2) Documents other than secret documents may only be classified in cases referred to in section 9(2).

### Section 9
### *Protection levels indicating handling requirements*

(1) The following protection levels are used for the classification of secret documents:

(1) protection level I, if unauthorised disclosure or unauthorised use of the secret information contained in the document could cause particularly grave prejudice to a public interest referred to in a secrecy provision;

(2) protection level II, if unauthorised disclosure or unauthorised use of the secret information contained in the document could cause significant prejudice to a public interest referred to in a secrecy provision;

(3) protection level III, if unauthorised disclosure or unauthorised use of the secret information contained in the document could cause prejudice to a public or private interest referred to in a secrecy provision;

(4) protection level IV, if unauthorised disclosure or unauthorised use of the secret information contained in the document could be disadvantageous to a public or private interest referred to in a secrecy provision.

(2) Also a document which is not stipulated as secret may be classified at the protection level referred to in subsection 1(4) above if provision of access to the document has been left to the discretion of the central government authority by law or if the information contained in the document may, according to law, be used or provided only for a certain purpose, and if unauthorised disclosure of the information could be disadvantageous to a public or private interest or weaken the ability of the central government authority to perform its functions.

Section 10
*General provisions on protectionlevel markings*

(1) A protection level marking may be supplemented with information about the secrecy of the document, taking, however, into account the provisions of section 25 of the Act on the Openness of Government Activities. The section lays down provisions on the secrecy marking obligation.

(2) The markings under this Decree may be made on a separate document to be attached to the secret document if it is not technically feasible to make them on the secret document or to modify markings existing on it, or if the handling requirements corresponding to the protection level are needed only for a certain short period.

(3) A protection level marking shall be made on the document clearly and correctly, and the classification shall be maintained only as long as necessary for protecting the interest in question. When grounds for the classification of the document no longer exist on the basis of an act or this Decree or when the classification needs to be modified, an appropriate marking indicating the removal or modification of the classification shall be made on the document on which the original protection level marking was made. The necessity of the marking and the protection level required by it shall be reviewed at the latest when the central government authority is considering to provide access to the document to external parties.

(4) If a document classified at protection levels I–III has been received from another central government authority, its protection level marking shall not be modified without notifying the originating authority thereof.

Section 11
*Special provisions on security classification markings*

(1) If unauthorised disclosure or unauthorised use of a document or the secret information contained therein could cause prejudice to international relations, State security, defence or other public interests in the manner referred to in section 24(1)(2) and section 24(1)(7–10) of the Act on the Openness of Government Activities, the protection level marking on the secret document may be supplemented or replaced with a specific security classification marking.

(2) The security classification shall be marked as follows:

(1) documents classified at protection level I shall be marked "ERITTÄIN SALAINEN" (top secret);

(2) documents classified at protection level II shall be marked "SALAINEN" (secret);

(3) documents classified at protection level III shall be marked "LUOTTAMUKSELLINEN" (confidential);

(4) documents classified at protection level IV shall be marked "KÄYTTÖ RAJOITETTU" (restricted).

(3) Security classification markings shall not be used in cases other than those under subsection 1, unless they are necessary for compliance with international information security obligations, or unless the document is otherwise related to international cooperation.

(4) Security classification markings shall be made in Swedish on documents written or translated in Swedish. Markings in Swedish may also be made in other cases if the central government authority considers it necessary. The Finnish and Swedish security classification markings correspond to each other as follows: "ERITTÄIN SALAINEN" – "YTTERST HEMLIG", "SALAINEN" – "HEMLIG", "LUOTTAMUKSELLINEN" – "KONFIDENTIELL", and "KÄYTTÖ RAJOITETTU" – "BEGRÄNSAD TILLGÅNG".

Section 12
*Equivalence of security classifications in fulfilment of international information security obligations*

Subject to international information securityobligations, the equivalent of the security classification marking "ERITTÄIN SALAINEN" under international information securityobligations is ”TOP SECRET” or an equivalent expression in another language; the equivalent of the marking "SALAINEN" is "SECRET" or an equivalent expression in another language; the equivalent of the marking "LUOTTAMUKSELLINEN" is "CONFIDENTIAL" or an equivalent expression in another language; and the equivalent of the marking "KÄYTTÖ RAJOITETTU" is "RESTRICTED" or an equivalent expression in another language.

## Chapter 4
## **Handling requirements applicable to classified documents**

Section 13
*Handlingrights and lists thereof*

(1) Access to a document classified at protection levels I–III may only be provided to persons who, because of their work duties, have a need to obtain information from the document or to handle it otherwise and who are aware of the obligations related to the handling of the document. The same applies to a document which is classified at protection level IV, contains sensitive personal data or biometric data and is recorded in a personal data file.

(2) Subject to international information securityobligations, a central government authority shall maintain a list of the work duties entitling employees to handle documents classified at protection level I or II, or documents classified at protection level III or IV and stored in personal data files. The central government authority may also maintain a list of persons entitled to handle the documents referred to above.

(3) The central government authority shall ensure that any person who is no longer responsible for work duties entitling him or her to handle classified documents returns the documents or destroys them in an appropriate manner.

(4) Separate provisions shall be issued regarding the conduct of personnel security clearances and regarding other measures to verify the reliability of personnel.

## Section 14
*Security requirements concerning premises for storage and handling of documents*

A central government authority shall ensure that

(1) the premises used for storing or otherwise handling classified documents are protected by means of appropriate locks, access control and other measures to prevent unauthorised access to the premises and the documents kept therein;

(2) it is possible to identify all persons who are provided access to premises used for storing or otherwise handling documents classified at protection level I or II;

(3) all documents classified at protection level I or II are kept in a safe, locked cabinet, vault or room which prevents unauthorised access to the information contained in the documents;

(4) it is possible to identify persons who are provided access to archives, data processing centres or other premises relevant to the maintenance of information systems or the functioning of telecommunications and used for storing or otherwise handling documents classified at protection level III, or of documents classified at protection level IV and stored in nationwide personal data registers.

## Section 15
*Handling of documents outside central government authorities' premises*

Subject to a permission, commission or instruction given by acentral government authority, its classified documents shall not be stored or otherwise handled outside its premises.

## Section 16
*Preparation, recording and modification of electronic documents*

(1) A central government authority may permit electronic recording of a document classified at protection level I or II onto a data medium or another device which

(1) is not connected with an information network, if the document is recorded with strong encryption or with other strong protection; or

(2) is only connected with an information network of the central government authority which connects the device used for recording and storing the document with other devices in the same specially monitored room possessed by the central government authority, if the information network connecting the devices has no connection with other information networks and the handling of the document is otherwise strongly protected.

(2) The central government authority may permit electronic recording of a document classified at protection level II onto a data medium or another device connected with its information network if the use of the information network is restricted, the document is recorded with strong encryption or with other strong protection, and the central government authority has ensured also otherwise that the information network and the data processing in their entirety fulfil the requirements of the high level of information security applied normally.

(3) The central government authority may permit recording of a document classified at protection level III onto a device connected with its information network if the use of the information network is restricted and the document is recorded with encryption or with other protection so that the information network and the data processing in their entirety fulfil the requirements of the increased level of information security applied normally. The same applies to a document which is classified at protection level IV, contains sensitive personal data or biometric data and is recorded in a personal data file.

(4) In preparing a document classified at protection levels I–III in electronic format and in modifying the document it shall be ensured that the disadvantage caused by diffuse radiation can be reduced sufficiently. If the device is connected with an information network, the information network shall also fulfil the criteria under subsection 1(2) or subsection 2 or 3.

## Section 17
*Copying of documents*

(1) A document classified at protection level I shall not be copied without the authorisation of the authority which prepared it. All copies of documents classified at protection level I or II shall be listed. In electronic copying of a document onto a data medium, account shall also be taken of the provisions in section 16 concerning the conditions for electronic recording of documents.

(2) A copy of a classified document shall be provided with the same marking as the original document, unless the classification already otherwise becomes apparent in the copy. A central government authority may decide that a document classified at protection level III or IV need not be marked if it is not provided to external parties

and if the persons handling the document in the central government authority are aware of the requirements to be complied with in the handling.

Section 18
*Deliveryof documents*

(1) A document classified at protection level I or II shall be packed appropriately for delivery and be delivered to the recipient either in person or in another safe manner approved by the central government authority.

(2) The delivery and reception of a document classified at protection level I or II shall be registered.

Section 19
*Transfer of documents in information networks*

(1) A document classified at protection level I or II shall not be transferred in information networks. However, such a document may be transferred in an information network of the central government authority which connects the device used for recording and storing the document with other devices in the same specially monitored room possessed by the central government authority if the information network connecting the devices has no connection with other information networks and the handling of the document is otherwise strongly protected.

(2) A document classified at protection level II may also be transferred in an information network of the central government authority if the use of the information network is restricted, the document is recorded with strong encryption or with other strong protection and the central government authority has ensured also otherwise that the information network and the data processing in their entirety fulfil the requirements of the high level of information security applied normally.

(3) The central government authority may permit transfer of a document classified at protection level III in its information network if the use of the information network is restricted and the central government authority has ensured that the information network and the data processing in their entirety fulfil the requirements of the increased level of information security applied normally. The same applies to transfer in an information network of sensitive personal data or biometric data classified at protection level IV and recorded in a nationwide personal data file. Other documents classified at protection level IV may be transferred in a manner determined by the central government authority.

Section 20
*Registration of handling*

(1) The handling of documents classified at protection levels I–III and of documents classified at protection level IV, containing sensitive personal data or biometric data and recorded in a personal data file shall be registered in an electronic log, an information system, a case management system, a manual register or a document.

(2) The provision in subsection 1 shall not apply to draft versions which are available only to the person who prepared them.

Section 21
*Filing and destruction*

(1) The Archives Act (831/1994) contains provisions on the filing of classified documents.

(2) A copy of a document classified at protection level I or II which is no longer needed shall be destroyed, unless it is returned to the authority which prepared the document. The copy may be destroyed only by a person to whom the central government authority has assigned this task. However, draft versions of documents may be destroyed by the person who prepared them.

(3) A document in paper format shall be destroyed in the manner corresponding to its protection level. A document recorded electronically onto a device or a data medium or in an information system shall be destroyed in a similar manner, ensuring that the temporary files generated during the use of the information system are deleted sufficiently often, unless they are deleted automatically from the information system.

Chapter 5
**Entry into force**

Section 22
*Entry into force*

(1) This Decree shall enter into force on 1 October 2010.

(2) This Decree shall repeal Chapters 2 and 3 of the Decree on the Openness of Government Activities and on Good Practice in Information Management (1030/1999) of 12 November 1999.

Section 23
*Transitional provisions*

(1) Documents classified before the entry into force of the Decree shall be handled pursuant to the requirements laid down in the Decree for the corresponding protection level, unless it is obvious that the grounds for classification based on the Decree have ceased to exist.

(2) The provisions of section 10(3) on markings indicating modification or removal of classification shall apply to a classification made before the entry into force of the Decree only if the classified document is provided to an external party.

(3) The data processing by a central government authority shall be brought in compliance with the requirements for informationsecurity at basic level under section 5 of the Decree within three years from the entry into force of the Decree.

(4) A central government authority shall bring the handling of classified documents in compliance with the requirements laid down in Chapter 4 of the Decree within five years from its decision to classify its documents.

(5) The premises used by the central government authority upon the entry into force of the Decree shall fulfil the premises security requirements laid down in the Decree within five years from the entry into force of the Decree. The same applies to premises put into use before two years have passed since the entry into force of the Decree.