Translation from Finnish
Legally binding only in Finnish and Swedish
Ministry of Finance, Finland

Government Decree on Security Classification of Documents in Central Government

(1101/2019)

By decision of the Government, the following is enacted under section 18, subsection 4 of the Act on Information Management in Public Administration (906/2019) and section 8, subsection 2 of the Act on International Information Security Obligations (588/2004):

Section 1
Scope of application

This Decree lays down provisions on the security classification of the documents referred to in section 18, subsection 1 of the Act on Information Management in Public Administration (906/2019), hereinafter *the Information Management Act*, the markings to be made in documents to be classified and the information security measures related to the handling of classified documents in central government authorities.

Provisions on public access to official documents and the consideration of a request for access to a document are laid down in the Act on the Openness of Government Activities (621/1999).

Provisions on the secrecy obligation of a document classified in accordance with international information security obligations and the implementation of international information security obligations are laid down in the Act on International Information Security Obligations (588/2004). Subject to international information security obligations as provided in the said Act, this Decree applies to the handling of a document that has been received from an authority of another country or from an international institution and that is to be classified.

Section 2
Definitions

In this Decree:
1) *central government authorities* means authorities operating in government agencies and public bodies, courts of law and committees established to handle appeals;
2) *handling of a document* means the receipt, preparation, recording, viewing, modification, disclosure, copying, transferring, delivering, destruction, storage and filing of a document and other measures directed at a document;
3) *a terminal device* means an information system or a part thereof usually used by one person for electronic data processing related to performing his or her work tasks or to other tasks of a central government authority.

In addition to what is separately provided in this Decree on the copying of a document or on a copy of a document, the provisions on a document apply to a copy of a document.

Section 3
Security classification and security classification marking

Documents referred to in section 18, subsection 1 of the Information Management Act that are to be classified are divided into the following security classification levels:
1) documents at security classification level I, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can cause exceptionally grave prejudice to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act;
2) documents at security classification level II, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can cause significant prejudice to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act;
3) documents at security classification level III, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can cause prejudice to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act;
4) documents at security classification level IV, where the unauthorised disclosure or unauthorised use of the secret information contained in the document can be disadvantageous to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.

The security classification levels referred to above in subsection 1 are marked in documents as follows: documents at security classification level I are marked ERITTÄIN SALAINEN; documents at security classification level II are marked SALAINEN; documents at security classification level III are marked LUOTTAMUKSELLINEN; and documents at security classification level IV are marked KÄYTTÖ RAJOITETTU. In addition to the said markings, the markings TL I; TL II; TL III; and TL IV may be used.

By derogation from subsection 2, the security classification level is marked in Swedish in documents prepared in the Swedish language or translated into Swedish. The

marking may also be made in other cases if the authority deems it necessary. Documents at security classification level I are marked YTTERST HEMLIG; documents at security classification level II are marked HEMLIG; documents at security classification level III are marked KONFIDENTIELL; and documents at security classification level IV are marked BEGRÄNSAD TILLGÅNG.

The security classification level of a document shall also be indicated in the information on the document in the case register referred to in section 25 of the Information Management Act and in another information pool generally used by an authority for information management.

The marking may be made on a separate document to be attached to the document if it is not technically feasible to make markings on a document or to modify the marking or if the handling requirements corresponding to the security classification level are needed only for a certain short period.

Section 4

Equivalence of security classification in fulfilling international information security obligations

Subject to international information security obligations, the equivalent of the security classification marking ERITTÄIN SALAINEN or YTTERST HEMLIG is the marking TOP SECRET in English or a corresponding marking in another language; the equivalent of the marking SALAINEN or HEMLIG is SECRET or a corresponding marking in another language; the equivalent of the marking LUOTTAMUKSELLINEN or KONFIDENTIELL is CONFIDENTIAL or a corresponding marking in another language; and the equivalent of the marking KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG is RESTRICTED or a corresponding marking in another language.

Section 5

Removal or modification of a marking related to a security classification level

If there are no longer legal grounds for the security classification of a document or if it is necessary to modify the security classification level, an appropriate marking of the removal or modification of the marking referred to in section 3 shall be made on the document on which the original marking was made and in the information on the document referred to in section 3, subsection 4. The appropriateness of the marking shall be checked at the latest when providing a third party access to the document.

If the document has been received from another authority, the marking related to a security classification level may be removed or modified only by permission of the authority that prepared the document or by permission of the authority in charge of the handling of the matter in its entirety unless it is clear that there are no longer grounds for the use of a security classification level.

Section 6

Preconditions for granting access to a classified document

A central government authority shall ensure in advance that the protection of a classified document is duly organised if the authority grants access to a classified document to a party other than a central government authority. The requirement does not apply to disclosing information on the contents of a document based on a party's right of access to information.

Provisions on the obligation of an authority to ensure the secrecy and protection of information when disclosing secret information for the performance of a commissioned task are laid down in section 26, subsection 3 of the Act on the Openness of Government Activities.

Section 7
Multi-tier protection

The information management entity shall take measures to prevent, preclude and contain any actions compromising the protection of the information system, the telecommunications arrangement and the security area referred to in section 9 used for the handling of classified documents, measures to detect and trace any actions compromising the protection, and measures to restore, without delay, the security level that existed prior to the action that caused the protection to be compromised.

Section 8
Handling rights and lists thereof

The right to handle a classified document may be granted only to persons who, due to their work duties or a need connected to attending to other duties of central government authorities, need to obtain information on a document or otherwise to handle it and who have been informed of the instructions and procedures related to the protection of classified information and who are aware of the obligations related to the handling of documents.

A central government authority shall keep a list of persons who have the right to handle documents at security classification level I, II or III. The list shall state the person's task on which the need to handle classified information is based.

A central government authority shall ensure that any person who no longer performs tasks on which the right to handle classified information is based returns the documents or destroys them in an appropriate manner.

Section 9

Security areas

The information management entity shall determine the following physically protected *security areas* to protect the handling of classified documents and the information systems in the manner referred to in section 10:
1) *administrative areas* that have a visibly defined perimeter and where only persons authorised by a central government authority have been granted unescorted access;
2) *secured areas* that have a visibly defined and protected perimeter through which all entry and exit is controlled by means of a pass or personal recognition system and where unescorted access is granted only to persons whose reliability has been ensured and who are specifically authorised to enter the area.

Section 10
Protecting the handling of documents and information systems with security areas

Classified documents shall, inside and outside security areas, be handled so that access to classified information is protected from unauthorised individuals.

A document at security classification level I may be stored or otherwise handled only inside secured areas.

Documents at security classification levels II–IV may be handled inside and outside security areas, however, so that:
1) information pools containing documents at security classification level II or III and information systems used in the handling of these documents shall be placed in a secured area;
2) documents in paper form at security classification levels II and III shall be stored in a secured area;

3) information pools containing documents at security classification level IV and information systems used in the handling of these documents shall be placed in a security area;
4) documents in paper form at security classification level IV shall be stored in a security area.

Notwithstanding the provisions of subsection 3, paragraphs 1 and 3 on the placing of information systems in security areas, documents at security classification levels II–IV may also be handled inside and outside administrative areas referred to in section 9, paragraph 1 with a terminal device and a telecommunications arrangement that meet the requirements of sections 11 and 12. The terminal device used for handling a document at security classification level II shall, however, be stored in a secured area. If documents in electronic format at security classification level III or IV are stored in a terminal device outside a secured area, they shall be protected with an encryption solution that is sufficiently secure for the security classification level. The information security of the terminal device shall be ensured.

Section 11
Requirements concerning information systems and telecommunications arrangements

The information systems and telecommunications arrangements used for handling classified documents shall be implemented so that:
1) taking into account the security classification level of the documents handled therein, they are separated in a sufficiently reliable manner from the information systems and telecommunications arrangements at a lower security level;
2) protection is provided against electronic messages that compromise information security, and the protection and the related measures are guaranteed throughout the life-cycles of the information system and telecommunications arrangement;

3) the information system users are provided only with the information, rights or authorisations that are necessary to perform the tasks;
4) their integrity is ensured in a sufficient manner;
5) persons using them, as well as equipment and information systems are identified in a sufficiently reliable manner;
6) only the necessary functionalities to meet the operational requirements are implemented;
7) the encryption solutions used are adequately secure, taking into account the security classification level of the documents handled in the information system or telecommunications arrangement.

When handling documents at security classification level I–III by electronic means, it shall be ensured that the risks related to electromagnetic emanations and electronic intelligence gathering have been sufficiently reduced. The information security measures implemented to reduce the risks shall be commensurate with the risk of exploitation of the information and the security classification level.

Section 12
Transfer of a document in an information network

Provisions on the transfer of secret data in a public information network are laid down in section 14 of the Information Management Act.

Classified documents may be transferred only in encrypted form in other than a public information network outside the security areas of authorities or via an information system or telecommunications arrangement at a lower security level than the said security classification level. If the transfer of classified documents takes place in a security area in other than a public information network and sufficient

protection of the information can be implemented by physical protection measures, unencrypted transfer or encryption at a lower security level may be used.

Section 13
Carriage of a document

Classified documents may be carried outside security areas by protecting the electronic data carriers with adequate encryption.

An unencrypted document at security classification level I–III shall be appropriately packaged and carried to the recipient under continuous control. The said document may also be carried to a recipient in another safe manner approved by a central government authority whereby the confidentiality and integrity are ensured in a manner that is adequate for the said security classification level.

Section 14
Monitoring of the handling of a document

In order to monitor the handling of classified documents, a central government authority shall implement the following measures:
1) the handling of a document at security classification level I–III shall be registered in an electronic log, an information system, a case register or a document;
2) the transmission and receipt of a document at security classification level I–III shall be registered;
3) an authorisation of the authority that has prepared the document shall be acquired for the copying of documents at security classification levels I and II;
4) a list shall be maintained of the copies of the documents at security classification levels I and II and of persons handling them.

Provisions on the registration of documents in the case register are laid down in section 25 of the Information Management Act.

Section 15
Destruction of a document

A classified document which is no longer required shall be destroyed in such a way that recreation and reconstruction of the information in whole or in part is prevented in a manner that is sufficiently reliable for the said security classification level.

If the document has been prepared by another authority, the authority that prepared the document shall be notified of the destruction of the document at security classification levels I and II that is no longer required unless it is returned to the authority that prepared the document. Documents at security classification levels I and II may be destroyed only by a person assigned to this task by an authority. Any draft versions of a document may be destroyed by the person who prepared them.

Section 16
Entry into force and transitional provisions

This Decree enters into force on 1 January 2020.

The need for a marking related to security classification in accordance with section 3 with regard to filed documents or documents stored in a central government authority shall be assessed if the central government authority takes up a document for other handling.

If a central government authority has not made a classification decision in accordance with section 7 of the Government Decree on Information Security in Central Government (681/2010), it shall bring the handling of classified documents

into conformity with the handling requirements provided in sections 6–15 of this Decree within three years from the entry into force of the Decree.