Dr. Mehmet Bedii KAYA

The Presidency of Turkey – The Decree on Information and Communication Security Measures (2019/12)

www.mbkaya.com

THE PRESIDENCY OF TURKEY - THE DECREE ON INFORMATION AND COMMUNICATION SECURITY MEASURES (2019/12)

Unofficial translation by Dr. Mehmet Bedii Kaya

DISCLAIMER: This document is an unofficial translation of the Decree on Information and Communication Security Measures (2019/12) issued on 6 July 2019 by the Presidency of Turkey. The text in this document is not the official translation and is provided for information purposes only. While care has been taken to ensure accuracy, the translator does not guarantee that the translation is free from error or omission. Use of the text is at the user's own risk.

Official Journal Date: 06.07.2019

Official Journal No: 30823

DECREE

The Presidency

Subject: Information and Communication Security Measures

DECREE

2019/12

The transfer of data to digital environments, the facilitation of access to information, the digitalization of infrastructures, and widespread use of information management systems brings about serious security risks. The following measures have been deemed appropriate in order to diminish and neutralize security risks encountered, in particular, for ensuring the security of critical data that may jeopardize national security or deteriorate public order, especially when its confidentiality, integrity or accessibility is compromised.

(1) Critical information and data such as population, health and communication records and genetic and biometric data shall be securely stored domestically.

(2) Critical data in public institutions and organizations shall be kept in a secure network in an offline and physically secure medium, access to the devices to be used in such network shall be controlled and the logs shall be preserved under precautions against alteration.

(3) Data of public institutions and organizations shall not be stored in cloud storage services except for the institutions' own private systems or local service providers controlled by the institutions.

(4) Aside from mobile applications developed by institutions authorized under the legislation for encoded or encrypted communication, classified data-sharing communication shall not be conducted through mobile applications.

(5) Classified data-sharing communication shall not be conducted on social media.

(6) The use of national social media and communications applications shall be preferred.

(7) Dissemination security (TEMPEST) or similar security measures shall be taken by public institutions and organizations where classified information is processed.

(8) No mobile devices and devices capable of transfer shall be present in the rooms/environments where critical data, document and document exist and/or interviews are conducted.

(9) Data, files and documents containing classified or institutional private information shall not be kept on devices (laptop, mobile device, external memory, etc.) which are not institutionally authorized or are used personally.

(10) Portable devices (laptop, mobile devices, external memory/disc, CD/DVD, etc.) including those personally used, which's sources are uncertain shall not be connected to the institutional systems. The devices which store classified information shall only be taken out of the organization provided that the data contained in the devices are encrypted at hardware and software level, and any devices used for this purpose shall be recorded.

(11) The development of domestic and national encryption systems shall be encouraged, and it shall be ensured that classified communications are conducted through these systems.

(12) The manufacturer and/or suppliers shall be required to undertake a commitment to the extent possible that any software or hardware to be acquired by public institutions and organizations does

not contain any feature unsuitable for the intended use or any back door (a security vulnerability, which allows access to a system without the user's knowledge/permission).

(13) Respective measures shall be taken for the safe development of software. Acquired or developed software shall be subject to security testing before use.

(14) Institutions and organizations shall take the necessary measures regarding cyber threat notifications.

(15) The access authorization of staff, including senior executives, to the systems shall be conducted through taking into account the actual works actually performed and the respective needs.

(16) It shall be ensured that industrial control system are kept offline, and the necessary security measures (firewall, end-to-end tunneling methods, authorization, identification mechanisms, etc.) shall be taken in cases when such systems are required to be open to the Internet.

(17) Security investigation or archive investigation shall be conducted in accordance with the relevant regulation for senior executives of institutions and organizations of strategic importance in terms of directly affecting national security and for the staff to be employed in critical infrastructure, facilities and projects.

(18) The settings of public e-mail systems shall be configured to be secure; email services shall be hosted in our country and under the control of the institution, and communication between servers shall be conducted in encrypted form.

(19) No corporate communication shall be made from non-corporate and personal e-mail addresses, and corporate e-mails shall not be used for personal purposes (private communication, private social media account, etc.).

(20) The operators authorized to provide communication services shall be obliged to establish an Internet exchange point in Turkey. Necessary measures shall be taken in order to prevent domestic communication traffic data, which should be exchanged domestically, to be transmitted out of the country.

(21) The data in the regions where the critical institutions are located shall not be carried over radio-link or similar methods, but shall be carried over fiber-optic cables. In critical data communication, radio-link communication shall not be used; however, where it is inevitable, the data shall be encrypted by using devices with national encryption systems.

In order to diminish and neutralize security risks encountered, in particular, for ensuring the security of critical data that may jeopardize national security or deteriorate public order, especially when its confidentiality, integrity or accessibility is compromised, and in accordance with national and international standards as well as information security criteria, “Information and Communication Security Guide” shall be prepared under the coordination of the Turkish Presidency Digital Transformation Office with the necessary contribution by the relevant public institutions and organizations to be implemented in public institutions and organizations and entities providing services as critical infrastructures, and published at the www.cbddo.gov.tr address. The Guide will be updated in line with the needs, developing technology, changing circumstances and modifications in the National Cyber Security Strategy and action plans.

All public institutions and organizations and entities providing services as critical infrastructures when establishing new information systems shall comply with the procedures and principles stated in the Guide. Existing information technology infrastructures with due consideration of security level priorities shall be gradually aligned with these principles in accordance with the plan to be included in the Guide following its publication. During compliance projects and newly established information systems, the current update version published at the specified address shall be taken into consideration.

Aside from the duties and activities carried out within the scope of ensuring national security and protection of confidentiality, institutions and organization shall establish an audit mechanism for the implementation of the Guidelines and shall supervise the implementation at least once a year. The results of the audit, and any corrective and preventive actions, shall be submitted to the Digital Transformation Office in accordance with the principles and procedures specified in the Guidelines.

For your information and consideration.

5 July 2019

Recep Tayyip ERDOĞAN

PRESIDENT