JULY 2019

New Presidential Decree on Information and Communication Security Measures

Digitalizing of information and information storages, facilitating access to information, common usage of information management systems would create security risks. In order to reduce those security risks and ensure the safety of critical data in Turkey, the Presidential Decree on Information and Communication Security Measures No. 2019/12 (the "Decree") was published in the Official Gazette on July 6, 2019.

The Decree consists of 21 Articles to provide measures on information and communication security including requirements for the domestic localization of data and limitations on the use of cloud services. Although the scope of application is not stated explicitly, it primarily concerns public institutions and organizations. Also, private organizations that provide services in electronic communications, transportation, banking and finance, or energy sectors, should take identified measures into account.

According to the Decree, critical data means "*information that could threaten national security or disrupt public order when its' privacy, integrity or accessibility is compromised*". Information relating to population, health, communication records and genetic, biometric data are deemed critical data.

The following major measures must be taken to ensure security of such critical data:

- Critical data shall be stored domestically in a secure manner.
- Critical data in public institutions and organizations shall be kept in a secure environment closed to the internet access, and the devices used in that secure environment shall be strictly controlled.
- The data of the public institutions and organizations shall not be stored in a cloud service.
- Confidential data shall not be shared or communicated through mobile applications or social media except for national mobile applications developed by authorized institutions for coded and encrypted communication.
- National social media applications shall be preferred.
- No mobile devices or devices for data transfer shall be allowed in environments where confidential data and documents are located or where interviews are conducted.
- The safety measures shall be determined for transfer of confidential data processed by public institutions and organizations.

- The development of national crypto systems will be encouraged, and they shall be used for communication on confidential data.
- Manufacturer and suppliers shall be required to undertake a commitment that any software or hardware to be acquired by public institutions and organizations do not contain any feature unsuitable for their intended use or any back-door.
- The security measures on development of software shall be determined. The security tests shall be completed before the usage of those software.
- The public institutions and organizations shall take necessary security measures against cyber threat.
- Security investigation shall be completed before the recruitment of personnel working on critical infrastructure, project and institutions.
- The settings of public institutions' e-mail systems shall be configurated securely and the servers shall be kept domestically. The communication between servers shall be made in cryptical way.
- Corporate e-mail addresses shall not be used for personal communication, likewise it is prohibited to use personal e-mail address in corporate communication.
- The operators authorized to provide communication services shall be liable to establish an internet exchange point in Turkey. Measures shall be taken to prevent the cross-border transmission of domestic communication traffic which needs to be exchanged domestically.

Besides all of those contemplated measures, the Presidency's Digital Transformation Office (the "Office") will prepare and publish Guidelines on Information and Communication Security (the "Guidelines") in light of the national and international standards on information security. The Guidelines will be updated in line with changing essentials, conditions, developing technology and National Cyber Security Strategy.

All public institutions and organizations and private organizations that provide critical infrastructure services will be obliged to

1. comply with the rules and procedures in the Guidelines,
2. review and revise their existing information systems in accordance with the Guidelines,
3. set up internal mechanisms to review and examine for compliance with the Guidelines,
4. examine compliance internally at least once a year,
5. report the examination results and corrective actions to the Office.

Even though the Decree compels public institutions to be compliant with contemplated security measures, private companies operating critical infrastructure services to store data outside Turkey or use global cloud services will also be affected by this new regulatory basis once the Guidelines on the application of the measures are published.

CONTACT US

Polat İş Merkezi No: 29 Offices: 28 - 29
Mecidiyeköy, Istanbul, Turkey
+ 90 (212) 215 30 00
info@gurulkan.com
www.gurulkan.com