GÜN + PARTNERS
AVUKATLIK BÜROSU

Developments for Local Storage in Turkey

1. Introduction and Executive Summary

The National Cyber Security Strategy and Action Plan (2020-2023) was published by the Ministry of Transport and Infrastructure on December 29, 2020. It was emphasized for critical infrastructures that issues such as keeping domestically produced data within the country will play a key role in studies to be carried out to protect such infrastructures and to increase their strength.

On the other hand, the Presidential Circular on Information and Communication Security Measures No. 2019/12 (the "Circular") entered into force after being published in the Official Gazette on July 6, 2019 with respect to local storage requirements. With the Circular, it was aimed to mitigate and neutralize serious security risks that may be encountered in the digitalization process of information, and to ensure the security of especially critical types of data. One of the most important matters regulated by Circular is the requirement to securely store critical information and data such as population, health and communication records and genetic and biometric data domestically within Turkey. This is not considered as a data transfer restriction but is mostly interpreted as a requirement of keeping a back-up of the relevant data in Turkey (local storage requirement) for accessibility.

Even though the Circular addresses to public institutions and organizations and enterprises providing critical infrastructure services, it will affect private law legal entities serving these institutions and enterprises. Therefore, local storage requirement under the Circular is indirectly applied to suppliers and business partners of public institutions and organizations and of enterprises providing critical infrastructure services. For instance, in accordance with Article 3 of the Circular, data of any public institution or organization shall not be stored in cloud storing services except for the relevant institution's own private systems or local service providers controlled by the relevant institution. In this context, it can be concluded that, in accordance with the Circular, private entities which provide services to any public institution shall have a domestic server in terms of cloud services that they can offer to such institutions. Additionally, in

accordance with Article 6 of the Circular, local applications shall be preferred for use for social media and communication.

Besides, there are also discussions about applicability and nature of the Circular. The Circular and the Information and Communication Security Guide ("Guide") prepared by the Digital Transformation Office ("DTO") to detail implementation of measures specified in the Circular may also be considered just as a guideline in terms of security standards and argued that it may not be binding.

It is also discussed that within the framework of the National Cyber Security Strategy and Action Plan (2020-2023), additional regulations may be brought to the agenda for keeping data within the country and for restriction upon data transfers. On the other hand, there are also rumors that Personal Data Protection Authority is working about Article 9 of the Law on Protection of Personal Data which restricts cross-border transfer of personal data under more severe conditions compared to General Data Protection Regulation in Europe. It may also be possible that the respective Authority can introduce new mechanisms and alternatives for cross-border transfer such as binding corporate rules which is not regulated under Turkish law but provided as an option for data controllers by the Authority based on its powers.

In addition to legislation regarding local storage of data in some specific sectors, the obligation under the Circular for specific data categories shows that a special protection is aimed in general. It is wondered in which direction developments regarding data transfer, localization and data residency will evolve in Turkey.

2. Developments in Information Security: Information and Communication Security Guide

The Circular states that the Guide involving various security levels to be implemented in public institutions and organizations and enterprises providing critical infrastructure services will be prepared and published under the coordination of the DTO. In this context, the Guide was approved on 24.07.2020 and published on the DTO's website.

The Guide is an extensive guideline consisting of detailed actions and measures to be taken to provide security of the data as well as the Guide also includes several annexes and detailed guidance/templates which the companies may use during their compliance work. On the other hand, in accordance with feedbacks we receive from the practitioners in data and information security sectors, most of the issues mentioned in the Guide are generally related to known technical issues and administrative measures. Still, it is recommended that the institutions and operators within the scope as well as third parties providing services to such institutions and operators – which are indirectly in the scope - should consider time schedule foreseen under the Guide and arrange their internal processes in parallel with the Guide as much as possible.

The enterprises are required to determine equipment and assets within their organization and perform the criticality rating and gap analysis within 6 months from the publication date of the Guide to follow the time schedule foreseen under the Guide. Following the relevant analysis, a roadmap for compliance, which will include steps to be followed to comply with the Guide, should also be prepared in the first 6 months. This period expired on 31.01.2021 in terms of public institutions and organizations and enterprises providing critical infrastructure services.

After the six-month period, required and essential data security measures for equipment and assets which were rated the most critical (1st level measures) shall be implemented within 12 months at latest after criticality rating and gap analysis (within 18 months at latest from the publication of the Guide), such measures for equipment and assets which were rated the second most critical (2nd level measures) shall be implemented within 15 months at latest after criticality rating and gap analysis (within 21 months at latest from the publication of the Guide) and such measures for equipment and assets which were rated the third most (the least) critical (3rd level measures) shall be implemented within 18 months at latest after criticality rating and gap analysis (within 24 months at latest from the publication of the Guide). There are detailed provisions in the Guide regarding the measures and their implementation.

In addition to the Circular, there are also provisions in the Guide that refers to domestic storage and data transfer. For instance, while the obligation under the Circular 'not to store data of public institutions and organizations in cloud storing services except for the institutions' own private systems or local service providers controlled by the institutions' can also be interpreted as a restriction for cross-border data transfer, the Guide also mentions a requirement 'to ensure critical data to be stored domestically and not to be hosted abroad' in terms of using cloud services. This is a provision that may have consequences for suppliers providing services to public institutions and organizations. Additionally, for operators, it is emphasized that measures should be taken to keep the domestic communication traffic within the borders of the country, to prevent this traffic and subscriber records from transferring outside Turkey and re-directing to Turkey and to keep the traffic within the country during accessing the servers to ensure the security of the cloud environment.

The Circular also stipulates that institutions and organizations should establish control mechanisms for the implementation of the Guide and audit the application at least once a year. The results of the audit and any corrective and preventive actions shall be reported to the DTO in accordance with the principles and procedures specified in the Guide. However, although the Guide states that audit activities will be carried out according to the Information and Communication Security Audit Guide to be published on the DTO's website, the respective audit guide has not been published yet. Audit guide is also expected to be published.

3. Sanctions in Case of Breach to the Requirements

The Circular states that the information systems to be newly established in all public institutions and organizations and enterprises providing critical infrastructure services must be compliant with the Guide. In addition, for the DTO, in case of any vulnerabilities arising from failing to comply with the respective measures, sanctions under the current legislation may also be applied. The Circular and the Guide do not specifically stipulate any sanction as this is not expected from legal point of view.

In terms of public servants working in public institutions and organizations, it is obvious that the Constitution of the Republic of Turkey and Public Servants Law numbered 657 will be applicable. In this context, public servants and officials may have liabilities towards both to the state and to individuals. This may affect the public institutions and organizations' arranging their internal processes and their expectations from suppliers to undertake for the services to be provided to public institutions and organizations.

In terms of enterprises providing critical infrastructure services, sanctions regarding information security can be applied within the scope of the legislation they are subject to. Therefore, the regulatory and supervisory authorities may conduct some changes in their secondary legislation by considering the Circular and the Guide for information security issues. In addition, sanctions for compliance with the Circular and the Guide can also be regulated separately in general. It should also be underlined that in case of an audit that can be carried out by the regulatory and supervisory authorities responsible for regulation and supervision of the relevant critical sector or by the DTO, when any breach to the Circular and the Guide is detected, the administrative sanctions about the information security under the respective regulations and other relevant legislation related to the respective sector may also apply.

Additionally, the Circular states that the Guide can be updated by considering needs, developing technology, changing circumstances and modifications in the National Cyber Security Strategy and action plans.

In terms of some critical sectors, the matters regulated under the Circular and the Guide are not unprecedented. For instance, there are legal sanctions applicable to electronic communication operators under Electronic Communication Law numbered 5809, Information and Communication Technologies Authority's Administrative Sanctions Regulation and Regulation on the Principles and Procedures of Coded or Encrypted Communication in the Electronic Communication Service of Public Institutions and Organizations and Real Persons and Legal Entities. The relevant regulations and other secondary legislation of the Information Communication and Technologies Authority require the data security measures to be taken in parallel or similar to the

Circular and the Guide. From this point of view, the current practices of electronic communication enterprises are generally in compliance with measures stipulated under the Circular and the Guide. Nevertheless, it will be useful to follow up the developments. For instance, the Regulation on Processing of Personal Data and Protection of Their Confidentiality in Electronic Communication Sector was amended as to come into force on June 4, 2021. Contrary to the former regulation, the new regulation does not prevent the cross-border transfer of personal data in principle and allows such transfer with explicit consent. The Circular states that operators authorized to provide communication services shall establish an internet exchange point in Turkey and shall take necessary measures to prevent the export of the domestic communication traffic which should be exchanged domestically. This provision is considered as a regulation restricting the cross-border transfer beyond the domestic storage obligation for critical data. On the other hand, although the new Regulation on Processing of Personal Data and Protection of Their Confidentiality in Electronic Communication Sector states that it is essential not to take traffic and location data abroad for national security reasons, the situations where even traffic and location data may be transferred abroad are not ignored. For situations where traffic and location data are transferred to third parties, the cross-border transfer of such data is also allowed provided that the subscribers are informed about the name of countries in which the respective third-party recipient resides, and they explicitly consent to such transfer. It is beyond doubt that electronic communication operators are subject to the Circular and the Guide. In this framework, it should be followed closely how the Circular and the Guide will be implemented together with the Regulation on Processing of Personal Data and Protection of Their Confidentiality in Electronic Communication Sector for such operators.

In the finance sector which is also determined as a critical sector, both Regulation on the Internal Systems and Interior Capital Adequacy Assessment Process of the Banks and the Regulation on Information Systems of Banks and Electronic Banking Services issued by the Banking Regulation and Supervision Agency as well as the Communiqué on the Management and Audit of Information Systems of Financial Leasing, Factoring and Financing Companies

may also apply in case for situations where the respective enterprises do not provide a security level required by the Circular and the Guide. In terms of energy, transportation and water management sectors which are other critical sectors, it will be useful indeed to arrange information security processes in accordance with the Circular and the Guide for the authorized private entities providing services in these sectors under supervision of the respective Ministries and regulatory and supervisory authorities. General regulations about security of information and data as well as infrastructure in these sectors can constitute legal ground o sanctions against the respective enterprises in case of any breach to the Circular and the Guide.

Finally, although there are some doubts about whether the Circular and the Guide are fully implemented by public institutions, the Ministries are aware of the issue and public institutions take some measures to ensure their suppliers to comply with the relevant requirements. For instance, there are circumstances that private legal entities which are not directly subject to the Circular can undertake contractual obligations that they guarantee compliance with such within the scope of services they provide to public institutions and organizations. As we observe that it become a common practice, undertaking such a compliance in tender processes may cause serious damages of private persons and companies as it may result in ban from tenders when they do not comply with the Circular and the Guide during public procurement of their goods and services even if they are not an enterprise providing critical infrastructure services.

Conclusion

It is highly controversial in practice and doctrine whether the Circular and the Guide is binding upon private legal persons. Generally, circulars are regulations that toward the sub-administrative units or the governed ones and express how the superior legal rule can be interpreted or how the superior legal rule should be applied by the administration. As stated in various precedents of High Administrative Court, it is more appropriate that circulars do not introduce a new obligation to the legal environment, do explain existing rules, and most importantly, do not violate the subjective rights and interests of the respective persons.

Any wide implementation of the Circular and the Guide in a way that requires data localization or restricts data transfer may lead to various discussions within this framework. To exemplify, although cross-border transfer is possible on certain conditions or with the explicit consent of the data subject in any case under the Law on Protection of Personal Data which is a law and superior legal legislation piece within hierarchy of norms, the restrictions on opportunities provided by the respective law through implementation of the Circular or the Guide may bring into question the validity of the Circular and the Guide as well as lawfulness of any sanction which can be applied with this respect.

Special thanks to Tayfun Yıldız for his contributions.