GURULKAN ÇAKIR

Obligations of Non-resident Data Controllers under Turkish Law

Introduction

The codification of personal data protection in Turkish law is relatively a recent development, dating only back to 2016. The long-awaited law on Protection of Personal Data ("Code") which is largely based on the EU Directive 95/46/EC came into effect and a new era started for all entities and persons collecting personal data in Turkey.

Following the enactment of the Code, a number of secondary regulations have been put into force in an integrative approach to form an effective data protection regime. Furthermore, Turkish Data Protection Authority ("TDPA") has published several guidelines to shed light on diverse issues concerning personal data protection.

As is the case with the GDPR of European Union, Turkish Data Protection Law has an extra-territorial reach in certain circumstances, impacting data controllers domiciled outside of Turkish jurisdiction if their data processing activities are related to Turkey or targeted data subjects are resident in Turkey.

This article aims to elucidate noteworthy obligations on non-resident data controllers under Turkish personal data protection regime.

Obligation to Register

In principle, all data controllers, including non-residents, must register with the Data Controllers Registry ("Registry") before they commence processing personal data. In this framework, the following information is required for registration:

- Identity and address details of the data controller and the representative of data controller,
- The purposes for which personal data may be processed,
- Data subject groups and data categories,
- Receiver and receiver groups to which personal data can be transferred,
- Data categories projected to be transferred to foreign countries,
- Date of registration and date of termination of registration,
- Precautions taken with regard to personal data security, and
- Maximum retention period required for the purpose for which the personal data is processed.

All of the above information contained in the Registry is accessible to public. The data controller is responsible for the completeness, accuracy and up-to-dateness of legal information maintained in the Registry. In this context, the data controller must notify the Registry of any change in the registered information within 7 days after the date of change.

That said, TDPA, with its decision No. 2018/32, has provided exemption for certain data controllers. In this scope, non-resident data controllers which process personal data through non-automatic means (on condition that the processing is part of a data-filing system) are exempt from the registration obligation. However, such data controllers who are not under obligation to register in the first place must register with the Registry within 30 days if and when they start processing personal data through automatic means.

Another noteworthy aspect of registration obligation has its source from the TDPA's decision No. 2018/88 which sets forth certain deadlines for data controllers to register with the Registry. According to the said decision, non-resident data controllers

already collecting personal data from data subjects in Turkey must register with the Registry until September 30, 2019.

Data controllers violating the registration or notification obligations may be subject to an administrative penalty ranging from TRY 20.000 to TRY 1.000.000

Obligation to Appoint a Local Representative

Non-resident data controllers must appoint a representative through whom the communication between the data controller, TDPA and data subjects will be conducted. The representative can be a real person or a legal entity but must in any case be resident in Turkey.

The appointment of the representative must be made by a written resolution to be issued by the competent decision-making body or person(s) of the non-resident data controller. A certified copy of such resolution will then be submitted to TDPA by the representative at the time of application for registration.

The appointment decision must also empower the representative with the following;

- To accept and receive notifications and/or correspondence sent by TDPA,
- To relay TDPA requests to the data controller and to relay the respective responses of the data controller to TDPA
- To relay requests of data subjects to the data controller and to relay the respective responses of the data controller to the concerning data subjects, and
- To conduct transactions relating to the Registry.

The representative must at the time of registration declare a real person whose contact details will be recorded in the Registry for communication purposes.

The registration transactions are carried out by the representative through the online data controllers information system called "VERBIS".

Obligation to Create a Personal Data Inventory

Along with the registration, data controllers must create and maintain a Personal Data Processing Inventory ("Inventory"). The Inventory should include the following;

- purpose of personal data processing,
- legal cause of data processing
- data categories,
- maximum retention periods required for the actualisation of the purpose of personal data processing,
- types of personal data to be transferred abroad, and
- precautions taken for the security of personal data.

Obligation to Adopt a Storage & Neutralisation Policy

Data controllers must draw up a written personal data storage and neutralisation policy ("Policy") in accordance with the Inventory. The Policy should include and indicate the following:

- Purpose of drawing up the Policy,
- Data storage mediums,
- Definitions of legal and technical terms,
- Legal, technical or other grounds necessitating the storage and neutralisation of personal data,
- Technical and administrative measures taken to secure personal data and to prevent illegal processing and access to personal data,
- Technical and administrative measures taken to ensure lawful neutralisation of personal data,
- Titles, departments and job descriptions of persons involved in the storage and neutralisation process,
- A chart demonstrating the storage and neutralisation periods,
- Periodic neutralisation periods, and
- Information relating to changes and updates in the Policy,

Nevertheless, the mere fact that a personal data storage and neutralisation policy has been created does not mean that the personal data is stored, erased, destructed or anonymised in practice. The data controller should genuinely implement the

Policy in its daily operations to maintain the compliance with the law.

Obligation to Ensure Data Security

Data controllers' primary duty is to prevent unlawful processing of personal data and unlawful access to personal data. Therefore, the data controller must take all necessary technical and administrative measures to ensure the appropriate level of security in terms of protection of personal data.

The delegation of some authorities to data representative or data processor does not transfer this obligation in any case whatsoever. Data controller cannot disclose personal data to third persons in contravention of the Law.

In case of failure to fulfil the obligation to ensure data security, data controllers may be subject to an administrative fine ranging from TRY 15.000 to TRY 1.000.000.

Obligation to Notify TDPA and Data Subjects

If the processed personal data is accessed by third persons illegally, the data controller must notify the relevant breach to TDPA and concerning data subjects as soon as possible. TDPA may announce the incident on its website or through other media if deemed necessary.

According to TDPA's decision No. 2019/10, the expression "*as soon as possible*" shall be interpreted as 72 hours for the purpose of clarifying the ambiguities and setting forth the applicable standards. This means that the data controller must notify TDPA of the personal data breach immediately but in any case, not later than 72 hours after having become aware of the incident.

Moreover, the data controller shall serve a notice within a reasonable time in relation to the respective breach to data subjects who are affected from such data breach. The data controller is obliged to reach the data subjects directly if their contact details are available, or otherwise, through other means.

If the data controller fails to serve such notification within 72 hours without any solid grounds, then reasons for such delay need to be clarified and notified to TDPA via further notice.

Obligation to Inform Data Subjects

Informing data subjects is not only an obligation on the data controller, but an indispensable right of data subjects whose personal data is processed.

When collecting personal data, the data controller must inform data subjects of the following;

- Identity of the data controller and, its representative, if any
- Purposes for which personal data will be processed,
- If the collected personal data is to be transferred, the purpose of transfer and the recipient groups to whom the personal data will be transferred,
- Method and legal cause for collection of personal data,
- Rights of data subjects

This exercise of this duty is not contingent upon information requests of data subjects. Even if the explicit consent of data subject has been taken or other circumstances enabling data controller to process personal data without consent have arisen, the data controller must at all times fulfil this obligation.

In case of failure to fulfil the obligation to inform, data controllers may be subject to an administrative fine ranging from TRY 5.000 to TRY 100.000.

Obligation to Respond to Requests of Data Subjects

The data controller must respond to requests made by data subjects free of charge and within 30 days at the latest. The response must indicate the result of the request as well as the legal justification if the request has been declined.

Conclusion

Even if a data controller does not have a presence in Turkey, it will still have to understand the impact of Turkish data protection

regulations if it processes Turkish residents' personal data. Therefore, complying with data protection regulations should be a concern not only for domestic data controllers, but for non-resident data controllers as well, since failing to fulfil data protection obligations may cause severe administrative fines as well as other punitive sanctions.

GURULKAN ÇAKIR

GURULKAN ÇAKIR AVUKATLIK ORTAKLIĞI

Polat İş Merkezi, Offices 28-29
Mecidiyeköy 34387
Istanbul, TURKEY

T +90 212 215 30 00
M info@gurulkan.com
W www.gurulkan.com