Turkey - Data Transfers

TABLE OF CONTENTS

May 2018

1. THE LAW

The Data Protection Law No. 6698 of 2016 ('the Law') was enacted fairly recently, only being published on 7 April 2016.

Prior to the publication of the Law, the data protection regime in Turkey was established in a piecemeal way, through the combination of a provision of the Constitution and various other legislative measures, such as provisions of the Criminal Code Law No. 5237, 2004 relating to illegal access and transfer of personal data. As per this previous data protection regime, obtaining the consent of the data subject was sufficient grounds for the processing and/or transfer of personal data, with no further restrictions imposed on transfer of such data abroad.

The Law has changed this system, by introducing detailed provisions relating to all forms of data processing and transfer activities. Following the publication of the Law, the transfer of data within Turkey and to third parties abroad became subject to these new provisions, and data

Turkey and to third parties abroad became subject to these new provisions, and data controllers have bene forced to amend their approach.

As the Personal Data Protection Board ('the Board') only started operating in January 2017, there are still no ancillary regulations or Board decisions regarding the issues of the transfer of personal data, although the Board has issued some detailed secondary legislation including the Regulation on Data Controllers' Registry, the Regulation on Deletion, Destruction and Anonymization of Personal Data, Communiqué on Principles and Procedures Related to Information Requirements and the Communiqué on Applications to Data Controllers in late 2017 and early 2018. This has left some uncertainty regarding key areas and issues relating to transfer that should be addressed by the Board.

2. KEY DEFINITIONS | BASIC CONCEPTS

The Law is heavily modelled on the Data Protection Directive (95/46/EC), and as such uses similar definitions.

Personal data: All kinds of information belonging to a real person, whose identity is identified or is identifiable.

Data processing: The Law does not provide an exhaustive list of functions that can be considered processing, instead providing examples of such functions, including disclosure and transfer of personal data.

Data subject: A person whose personal data is being processed.

Data controller: A real or legal person, determining the objectives and tools of processing of personal data and responsible for the establishment and management of data recording system.

Data processor: A real or legal entity, processing personal data, relying on the authority, granted by data controller, in the name of data controller.

Personal data of a special nature: Personal data relating to race, ethnicity, political views, philosophical belief, religious denomination or other beliefs, clothing and attire, membership in associations, charities or trade unions, health, sex life, convictions, security measures and biometric and

genetic data.

As per the Law, personal data can only be processed following the explicit consent of the data sub-

ject. However, the Law also lists situations that are exceptions to the rule of obtaining explicit consent. It should be noted that this primary rule and the exceptions also apply to the transfer of personal data. The Law defines these exceptions as, situations where the data transfer is:

- clearly mandated by law;
- for a person who is unable to express their explicit consent due to a situation of impossibility, the processing is required for the safeguarding of their or a third person's life or physical wellbeing;
- directly related to the formation or execution of an agreement to which the data subject is a party;
- required for the data controller to satisfy their legal obligation;
- regarding data that has been made public by the data subject;
- mandatory for the establishment, use or protection of a right; or
- on the condition that it does not harm the data subject's fundamental rights and freedoms, mandatory for the legitimate interests of the data controller.

The Law also contains exceptions relating to personal data of a special nature. These exceptions are far more limited and allow for transfer without obtaining consent only when such transfer is clearly mandated by law. However, it should be noted that these exceptions do not apply personal data relating to health or sex life, with transfer of such personal data only possible upon obtaining the explicit consent of the data subject.

3. SCOPE OF APPLICATION

The Law applies to data controllers, thus making data controllers liable for the activities of processing and transfer of personal data under their control. Furthermore, where data controllers utilise the services of third party data processors, the Law dictates they remain jointly liable for establishing all of the technical and administrative measures required to ensure the safeguarding of the personal data and to prevent any unlawful access or processing of said data.

The Law contains a provision that identifies the areas of exception that are exempt from such provisions, including:

- use of personal data by real persons within the scope of activities relating to either themselves or their family members living in the same house, on the condition that the data is not provided to third parties and data security requirements are followed;

data is not provided to third parties and data security requirements are followed;

- processing of personal data for official statistics or, on the condition that the data is made anonymous, used for purposes such as research, planning or statistics;
- on the condition that such use is not contrary to national defence and security, public safety and order, economic security, the right to privacy and personal rights, and, on the condition that it does not constitute a crime, processing for the purposes of art, history, literature or scientific pursuits or processing within the scope of the freedom of speech;
- processing within the scope of the preventive, protective and intelligence activities of the public bodies and institutions that have been authorised by law to safeguard national defence, security, public safety and order or economic security; or
- processing by judicial authorities or penal institutions in relation to investigations, prosecutions, trials or enforcement proceedings.

4. RESTRICTIONS ON THE INTERNATIONAL TRANSFER OF DATA

The Law also introduces additional requirement if the transfer of personal data is to be made abroad. While the general rule remains that explicit consent will be required for all forms of transfer abroad, in the situation that data is transferred abroad pursuant to one of the aforementioned exceptions, the Law dictates that such transfer may only take place if the recipient country provides sufficient safeguards.

In the situation that the recipient country has not been included on the list of countries (which will be but have not been yet determined and announced by the Board) providing sufficient safeguards, both the transferring and the recipient data controllers must submit written undertakings stating that they will provide sufficient protection and obtain the permission of the Board. In accordance with the oral confirmation received by the Board, the Board then prepares a draft and template undertaking as to be used for the data transfers to the countries not providing sufficient safeguards.

Since the list of the secure countries has not been published, once it is prepared and shared, the relevant template will also be applicable for all international transfers of personal data based on any legal ground except the explicit consent of the data subjects.

Furthermore, as per a separate provision of the Law, reserving any rights or obligations established under international agreements, in the situation that a transfer of data abroad would seriously harm the legitimate interests of the Turkish republic or the data subject, such transfer abroad can

harm the legitimate interests of the Turkish Republic or the data subject, such transfer abroad can only be made pursuant to obtaining an opinion from the relevant public body or institution. It should be noted that there has been no further guidance as to the implementation of this provision, including a lack a specification as to which public bodies or institutions may be considered as relevant to the transfer abroad.

It should also be noted that there is currently no obligation regarding the execution of a written agreement of standard contractual clauses between a data controller and a data processor to which the data is being transferred.

As the Board was only formed in January 2017, the list of countries that have been deemed to provide sufficient safeguards have not yet been finalised and published. However, the Law states that the sufficiency of the safeguards provided by a country shall be determined on the following conditions:

- whether or not the country is party to international agreements that Turkey is party to;
- the situation of reciprocity regarding data transfer to Turkey;
- the nature of the personal data, processing purpose and duration for each data transfer;
- the data protection legislation and implementation of the country; and
- the measures that are being undertaken by the data controller in the country.

5. DATA LOCALISATION | RESIDENCY REQUIREMENTS

5.1. Financial data

With regard to financial data, certain legislative measures such as the Law on Payment and Security Agreement Systems, Payment Systems and Electronic Currency Organisations 2013, require financial institutions to keep their primary and secondary systems within Turkey. This requirement prevents the systematic transfer of such data abroad.

Furthermore, the Banking Law 2008 introduces specific confidentiality obligations for persons who, due to their position and task, are in possession of secret information relating to banks or their client. The Law on Bank Cards and Credit Cards 2006 imposes a similar obligation on this industry too. These provisions have sometimes been interpreted as preventing the transfer of such data abroad.

5.2. Residency Requirement under Capital Markets Law

Based on the regulative authority granted to the Capital Markets Board by Article 128 of the Capital Markets Law numbered 6362, the Capital Markets Board has issued a communique requiring primary and secondary systems to be within Turkey. The relevant Communiqué on Information Systems Management numbered VII-128.9 (only available in Turkish here) entered into force on 5 January 2018 and is applicable to the primary and secondary systems of the followings subject to the Capital Markets Law:

- Borsa İstanbul A.Ş. (Istanbul Stock Exchange);
- Stock exchanges, stock market operators and other organised/regulated markets;
- Pension funds;
- Istanbul Clearing, Settlement and Custody Bank (İstanbul Takas ve Saklama Bankası A.Ş.);
- Central Securities Depository of Turkey (Merkezi Kayıt Kuruluşu A.Ş.);
- Portfolio custodians;
- Capital Markets Licensing Registry and Education Institution (Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.);
- All capital markets institutions, publicly held companies listed under Article 35 of the Capital Markets Law;
- Turkish Capital Markets Association (Türkiye Sermaye Piyasaları Birliği); and
- Turkish Appraisers Association (Türkiye Değerleme Uzmanları Birliği).

However, in accordance with the Capital Markets Board's decision numbered i-SPK.62.1, announced with Bulletin No. 2018/10 (only available in Turkish here), the primary information systems of the publicly held companies (which are not subject to the independent audit related to their IT systems yet in accordance with one of the new communiques i.e. Communiqué on Independent Audit of Information Systems numbered III-62.2) will not be required to be in Turkey. The Capital Markets Board highlighted that the scope of the independent audit may be extended as to cover the publicly held companies as well and therefore, when they start to be subject to the relevant independent audit, they will be required to keep their primary systems in Turkey.

Irrespective of the above, in accordance with Article 10(3) of the Communiqué on Information Systems Management numbered VII-128.9, the information to be classified for the relevant entity as a highly important and portable storage mediums providing access to such information shall not be

taken outside the organisation of the relevant entities. Furthermore, the management of outsourced services related to the IT systems shall also be subject to detailed regulations under the Communiqué and Article 18 of the same regulates the details of surveillance mechanism required

Communiqué and Article 16 of the same regulates the details of surveillance mechanism required to be established over the relevant third party and the matters required to be regulated in the agreement to be signed between the capital markets entity and the outsource company which will provide IT services.

6. SECTOR-SPECIFIC RESTRICTIONS

6.1. Health data

On 20 October 2016, the Ministry of Health published Regulation on the Processing of Personal Health Data and the Maintenance of Privacy ('the Health Data Regulation') (only available in Turkish here). The Health Data Regulation introduced new conditions relating to the processing and transfer of personal health data. However, it has been amended with an additional regulation published on 24 November 2017 (only available in Turkish here) and new and compelling conditions to the processing and transfer of personal health data have been eliminated. Therefore, the provisions of the Health Data Regulation have become in line with the Law.

While the subject matter of the Health Data Regulation and the fact that it was published by the Ministry of Health as a regulatory measure indicated that it is intended to only apply to healthcare service providers and other associated persons, the provisions detailing the scope of application has been worded in a way to include data controllers that fall outside of this definition, particularly any employer that is processing and transferring health data of their employees.

The Health Data Regulation had introduced an important provision specific to the transfer of personal data abroad, stating that such transfer of personal health data abroad could only be conducted should such data be made anonymous, regardless of whether or not consent had been obtained. However, as explained above, this restriction is not applicable now and health data may also be transferred to abroad with the explicit consent of the relevant data subject.

6.2. Financial data

With regard to financial institutions that are subject to the legislative and regulatory measures listed above, as the requirement to maintain primary and secondary systems in Turkey is still in effect, it should be ensured that such systems and the relevant data are maintained within Turkey.

7. DATA TRANSFER SOLUTIONS

As stated above, the primary rule for transfer of personal data - both within Turkey and outside of Turkey - is obtaining explicit consent from the data subject. While the areas of exceptions that apply to the transfer of data within Turkey do mean that transfer activities can be more readily made within the country, the additional element of 'country providing sufficient safeguards' for transfers abroad leads to additional compliance considerations.

While the Law does allow for exceptions to the requirement of explicit consent to also apply to transfer of data abroad, at the time of writing there have not been any official updates on the status of the list of countries that are identified as countries providing sufficient safeguards. As the Board needs to receive feedbacks of various governmental bodies (such as the Ministry of Justice and the Ministry of Foreign Affairs) in order to determine which countries will be deemed as secure countries, the countries that provide such sufficient safeguards have not yet been published. Still, as far as we have been informed by its officers, the list may be expected to be published soon.

While it is widely expected that countries within the European Union will be considered to be within the scope of countries sufficient safeguards, due to the fact that reciprocity is listed as a determinant factor, there is even a degree of uncertainty regarding the full extent of its inclusion. Furthermore, there is currently no indication as to which other countries may be included on this list.

Therefore, when considering current and future transfer of personal data, data controllers should consider the nature of the data transferred and the recipient country. In relation to general personal data, in the situation that the purpose of transfer falls under one of the aforementioned areas of exception, the data controller may consider transfer abroad without obtaining explicit consent. As the list of countries providing sufficient safeguards has not yet been finalised, it will be up to the data controller to make a reasoned judgment regarding the recipient country, with the caveat that should the recipient country later not be included on the final list, the data controller will have to go additional administrative steps in order to secure the ongoing transfer abroad of personal data.

While some data controllers have chosen to proceed with transferring data abroad without explicit consent to countries within the EU, other data controllers in Turkey have designed their current data collection procedures to ensure that the explicit consent of the data subject is always obtained. Legally speaking, unless an approval of the Board is received to transfer personal data of data subjects resident in Turkey to abroad, the only legal ground applicable to transfer of such personal data is the explicit informed consents of the data subjects in the current situation. The data controller/processor should also be aware that when the legal ground to transfer such personal

data is the explicit consent of the relevant data subjects, data subjects may always opt-out from their explicit consent for the processing (including transfer and retention) of their personal data abroad.

abroad.

Furthermore, in the situation that the data to be transferred is personal data of a special nature, as the scope of exceptions are a lot more limited, it is advisable for data controllers to ensure that they design data collection, processing and transfer procedures that obtain explicit consent of the data subject relating to the transfer of their data abroad.

Finally, particular care must be made to ensure that data controllers include provisions detailing the full range of administrative and security measures that the third party data processors it engages adheres to. This is primarily to ensure that the data controller satisfies their obligations under the Law and can provide grounds of defense or mitigation before the Board should a complaint be made regarding the personal data that has been transferred to third parties, whether nationally or abroad.

8. SANCTIONS

As per the Law, the breach of provisions relating to the protection of personal data can lead to both administrative fines and criminal penalties.

With regard to potential criminal penalties, the Law refers to the relevant provisions of the Criminal Code that detail the sanctions for the unlawful recording and/or accessing of personal data. As per Article 136 of the Criminal Code, unlawfully obtaining or transferring personal data is punishable by a two to four year prison sentence.

In addition to criminal sanctions, the Law also contains provisions detailing administrative fines that are to be applied in the situation of infringement. There are four main breaches that have been defined in the context of a potential administrative fine:

- a data controller not satisfying their obligation to inform the data subject;
- the data controller not satisfying the data security requirements;
- the data controller not implementing the decisions of the Personal Data Protection Authority ('KVKK'); and
- the data controller not satisfying their obligation to register on the Data Controller Registry.

With regards to issue surrounding the transfer of personal data, the most readily identifiable breaches would be either a failure to satisfy data security requirements or a failure to implement the decisions of the KVKK. These breaches can be sanctioned with administrative fines ranging

the decisions of the KVKK. These breaches can be sanctioned with administrative fines ranging from TL 5,000 (approximately €1,000) to TL 1,000,000 (approximately €200,000).

Depending on the nature of the breach, specifically as to whether the breach constitutes a criminal or administrative offence, the data controller will either be referred to the prosecutor or the Board.

ABOUT THE AUTHORS

Begüm Yavuzdoğan Okumuş

Gün + Partners

Begüm Yavuzdoğan Okumuş is a Managing Associate at Gün + Partners and specialises in corporate, competition law, IT and telecommunications law. Begum advises on general corporate and commercial law matters and transactional issues, particularly mergers & acquisitions, and on competition law regulations. She represents multinational and local businesses in a variety of industries, including pharmaceuticals, telecoms and information technologies.

Begum regularly advises multinationals in the telecommunications industry, including various IT companies, in relation to licensing regulations and other regulatory aspects of the Turkish telecommunications legislation and on data privacy rules. She provided general legal advice to a telecommunication authority of a Middle Eastern country regarding the current licensing system and licensing types for telecommunication services in Turkey.

begum.yavuzdogan@gun.av.tr

RELATED CONTENT

NEWS POST

International: South Korea and US agree to strengthen ICT cooperation

NEWS POST

EU: Commission reaches agreement with Parliament and Council on free flow of non-personal data

OPINION

Vietnam: National Assembly approves cybersecurity law

NEWS POST

Mexico: Convention 108 decree published in Official Diary of the Federation

NEWS POST

Vietnam: National Assembly approves cybersecurity law