BACK TO DATAGUIDANCE

DataGuidance GUIDANCE NOTES

Turkey - Data Transfers

Begüm Yavuzdoğan Okumuş and Bentley James Yaffe

20 February 2017

About The Authors

Begüm Yavuzdoğan Okumuş is a Managing Associate at Gün + Partners and specialises in corporate, competition law, IT and telecommunications law. Ms. Yavuzdoğan 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.

Ms. Yavuzdoğan 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.

E-mail: begum.yavuzdogan@gun.av.tr

Bentley James Yaffe is an associate with the law firm of Gü + Partners Law Firm and works predominantly in the areas of technology, media and telecommunication law, data protection law and life sciences. In this capacity he has provided legal advice in the areas of telecommunications, internet and data protection law to both multinational companies and local Turkish

1. The Law

The introduction of a legislative measure specifically regulating the protection of personal data in Turkey has been fairly recent, with the Data Protection Law No. 6698 of 2016 ('the Law') (available in Turkish here) 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 relating to illegal access to and transfer of personal data. As per this previous data protection regime, obtaining consent of the data subject was sufficient grounds for processing and/or transfer activities relating to personal data, with no further restrictions imposed on transfer of such data abroad.

The Law has changed this system, by introducing detailed provision 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 controllers in Turkey were forced to amend their approach to transfer of data within and outside of Turkey.

As the Personal Data Protection Board ('the Board') has only recently started operating in January 2017, there are currently no ancillary regulations or the Board's decisions regarding the issues of the transfer of personal data. 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 modeled on the Data Protection Directive (95/46/EC), and as such uses similar definitions.

Personal data: The Law defines this as 'all kinds of information belonging to a real person, whose identity is identified or is identifiable.' With regard to the definition of 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.

The Law also provides definitions for three main stakeholders in the data protection regime: data subjects, data controllers and data processors.

Data subject: This is defined as 'a person whose personal data is being processed.'

Data controller: This is defined as 'the 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: This is defined as '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: This is defined as '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 subject. 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

technology companies. Bentley is a graduate of King's College London Schools of Law and holds and M.A. from the King's College London School of Arts & Humanities for this dissertation titled, 'A Study of the Sufficiency and Effectiveness of the EU Digital Rights Regime.' He is currently studying for an LLM in Communication and Technology Law at Istanbul Bilgi University.

E-mail: james.yaffe@gun.av.tr

- 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 the actions of data controllers, thus making data controllers liable for the activities of processing and transfer of personal data under their control. Furthermore, in the situation that data controllers utilise the services of third party data processors for these processes, 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 does contain a provision that identifies areas of exception that are exempt from the provisions, which are identified as below:

- 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;
- 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 defense, 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. Restriction 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 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.

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 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 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.

6. Sector-specific restrictions

6.1 Health Data

On October 20, 2016, the Ministry of Health published a Regulation on the Processing of Personal Health Data and the Maintenance of Privacy ('Health Data Regulation') (available in Turkish here). The Health Data Regulation introduces new conditions relating to the processing and transfer of personal health data. However, it should be noted that there is currently uncertainty as to the scope of application of the Health Data Regulation.

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 is 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 introduced an important provision specific to the transfer of personal data abroad; stating that such transfer of personal health data abroad can only be conducted should such data be made anonymous, regardless of whether or not consent has been obtained. However, as explained above, the scope of application of this provision is currently unclear. As the Health Data Regulation also clearly provides grounds for other processing and transfer of health data that is conducted pursuant to the obtaining of consent of the data subject, it has been argued that the requirement to make health data anonymous was not intended to apply to parties other than healthcare service providers and other associated persons. However, until a clarification is issued by the Ministry of Health or the Board, there remains a regulatory risk in the situation that personal health data is not made anonymous before transfer, even if consent has been obtained.

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 has only recently been formed, the countries that provide such sufficient safeguards have not yet been published.

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 inclusion of European Union country. Furthermore, currently there is 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.

Furthermore, in the situation that 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 Turkish Personal Data Protection Board should a complaint be made regarding the personal data that has been transferred to third parties; whether nationally or abroad.

8. Sector-specific requirements

With regard to the additional conditions imposed by the Health Data Regulation, issues of compliance are pronounced by the fact that there is currently uncertainty regarding the scope of application. However, until this clarification has been made, there remains a regulatory risk if personal health data is transferred abroad without being made anonymous. Therefore, companies should consider the necessity of the transfer of abroad of such health data and the form in which the transfer is made. Making such health data anonymous before transfer will mean that the data is no longer considered to be within the scope of the Law and is also compliant with the additional requirements set out in the Health Data Regulation.

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.

8. Sanctions & Penalties

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 2 to 4 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 DPA 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 DPA. These breaches can be sanctioned with administrative fines ranging from 5.000 TL (approximately €1,500) to 1,000,000 TL (approximately €310,000).

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