Turkey requires explicit consent for export of personal data

Companies may rely on exemptions or written agreements to provide an adequate level of protection. **Ilay Yılmaz** and **Gonenc Gürkaynak** of ELIG Gürkaynak Attorneys-at-Law explain.

The long-awaited Law on the Protection of Personal Data (DP Law) was approved by the Turkish Parliament on 24 March 2016, and published in the Official Gazette on 7 April 2016. The transition periods that were set out in the DP Law have finally expired and the DP Law is now fully in effect.

Similar to the European Union's Data Protection Directive 95/46/EC (EU Directive, repealed by the GDPR) and the General Data Protection Regulation (GDPR), the main objectives of the DP Law are: (i) to protect the fundamental rights and freedoms of individuals in relation to the processing of their personal data, particularly with respect to the confidentiality of their private lives, and (ii) to regulate the procedures and principles to be followed, along with the obligations to be fulfilled, by the individuals who and legal entities which process personal data.

The transfer of personal data is one of the primary issues of concern for foreign data controllers who conduct (or intend to conduct) business activities in Turkey. The established practice in Turkey with respect to the transfer of personal data abroad differs from the European Union's practice, even though the DP Law is based mainly on the EU Directive.

Requirements for transfer of personal data abroad

According to the DP Law, the primary requirement for transfers of personal data abroad is obtaining the explicit consent of the data subject(s). Unlike the EU Directive and GDPR, the relevant article of the DP Law states that personal data cannot be transferred abroad without the explicit consent of the data subject(s). Having said that, it should be noted that there are certain significant exceptions to this basic rule.

These exceptions make it possible to transfer personal data abroad without the explicit consent of the data subject(s) by following a two-step process.

The first step requires that the data processing in question must fulfill one of the following conditions: (i) data processing is clearly mandated by laws, (ii) data processing is necessary to protect the vital interests or bodily integrity of the data subject or of a third person, where the data subject is physically or legally incapable of giving explicit consent, (iii) processing the personal data of the parties to a contract is necessary, on condition that the data processing is directly related to the formation or execution of such a contract, (iv) processing is required for the data controller's compliance with a legal obligation, (v) the data in question has been made public by the data subject, (vi) processing is mandatory for the establishment, exercise or protection of a legal right, or (vii) processing is required for the legitimate interests of the data controller, provided that such data processing does not harm or violate the fundamental rights and freedoms of the data subject.

The second step requires that the country to which the personal data will be transferred must have adequate levels of protection for the personal data processing. Furthermore, these conditions must be satisfied cumulatively; in other words, one of the conditions described above (in step 1) as well as the requirement regarding the existence of adequate levels of protection (step 2) must be fulfilled together in order to qualify for this exception.

With that said, it should be noted that special categories of personal data are subject to stricter data protection rules and entail a more extensive level of protection. Data concerning a data subject's racial or ethnic origin, political opinions, philosophical beliefs, religious denomination, sect or other beliefs, clothing and attire, membership of associations, foundations or trade unions, criminal convictions and security measures, along with one's biometric and genetic information (i.e., special categories of personal data) require the explicit consent of the data subject before processing. However, such data may be transferred without the explicit consent of the data subject if the processing is clearly mandated by legislation. On the other hand, personal data related to one's health or sexual activities (which are also deemed as special categories of personal data) may be processed without the explicit consent of the data subject only if the data is processed by authorized entities and institutions or by persons who are bound by a duty of confidentiality for the purpose of the protection of public health, the provision of preventative medical, diagnostic and treatment services, and the planning, management and financing of healthcare (treatment and maintenance) services. For the transfer of special categories of personal data abroad, the "adequate level of protection" requirement remains in effect as well, in addition to the above restrictions and conditions.

Under this regulatory scheme, the Turkish Data Protection Board ("Board") has been authorized to determine the list of countries that will be deemed to provide an "adequate level of protection". However, the Board has not so far declared or recognized any country as possessing an adequate level of protection, and data controllers have been forced to seek other options for complying with the DP Law, one of which may be obtaining the explicit consent of the data subjects.

Moreover, if data controllers can show that their data processing activities fall under one of the "exceptions" explained above but the current level of protection is not deemed to be adequate in the country to which the personal data will be transferred, then the data controllers in Turkey and the data controller/processor abroad (to whom

the data will be transferred) may sign a written agreement undertaking to provide an adequate level of data protection, which should then be submitted to the Board for approval.

Multinational firms should keep in mind that these rules also apply to personal data transfers between group companies.

The Board's guidance on data transfers abroad

The Board has published Guidance on the Transfer of Personal Data Abroad[1] (Guidance) in order to explain the applicable rules to data controllers who intend to transfer personal data abroad and data subjects whose personal data will be transferred. In addition to this Guidance, the Board has also published sample letters of commitment, including the minimum requirements with respect to the legal documents (warranties) to be prepared and submitted by data controllers for transfers of personal data abroad, if the country to which the personal data will be transferred does not provide adequate levels of protection. The Board has issued two different letters of commitment to be used by the data controllers and data processors who transmit/receive personal data. These letters of commitment can be found on the official website of the Board.[2]

Parties to these letters of commitment basically declare and certify that they will comply with the Turkish data protection legislation and affirm that they accept the Board's authority (i.e., with respect to the notification obligations). The letters of commitment are also required to include certain information, such as information on the data subject groups, categories of data, purposes of the data transfer, technical and administrative measures that will be taken by the data recipient, and the data controller's information in the Data Controllers Registry Information System (VERBIS"), which has not yet been established. The Board has started to receive applications for the approval of such letters of commitment. There is no specific timeframe set out for the approval procedure under the relevant legislation, and the Board has so far refrained from providing an estimated time period for this process.

Comparing the Turkish and EU jurisdictions in practice

In the European Union jurisdiction, the European Commission has the power and ability to determine, on the basis of Article 45 of the GDPR, whether a country outside the European Union offers an adequate level of data protection, whether through its domestic legislation or through its international commitments, treaties and agreements.

In the Turkish jurisdiction, the Board has the authority to determine the countries which provide an adequate level of protection, by consulting the relevant public administrations and agencies if necessary and also by evaluating the international agreements that Turkey is a party to, the reciprocity agreements related to data transfers between Turkey and the country that is seeking to obtain the personal data, the categorization of the personal data, as well as the purpose and period of processing for each specific data transfer, the relevant legislation and practice in the foreign country to which the data will be transferred, and the security measures that the data controller in that foreign country pledges and commits to provide.

Even though the European Commission has so far recognized and designated certain countries[3] as providing an adequate level of data protection, the Board has not yet published the list of "whitelisted" countries that are deemed to offer adequate data protection measures. Therefore, data controllers in Turkey should either obtain the explicit consent of data subjects or execute the above-mentioned letters of commitment and submit them for the approval of the Board.

It should also be remembered that while "appropriate safeguards", such as binding corporate rules, standard contractual clauses, approved codes of conduct or certification mechanisms, ad hoc contractual clauses and reliance on international agreements, may be used in the European Union to legally transfer personal data abroad in the absence of an "adequate protection" decision, the DP Law and the relevant secondary legislation in Turkey do not mention or foresee any of these safeguards.

Customs Union Agreement between Turkey and the EU

The European Union and Turkey are linked by a Customs Union Agreement,[4] which entered in force on 31 December 1995. According to Article 10 of this agreement ("Obligation to Observe Confidentiality"), personal data may only be transmitted if the level of personal data protection afforded by the legislations of the parties is equivalent. The same article also states that the parties must ensure, as a minimum, a level of protection that is based on (and in line with) the principles of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108),[5] which was the first legal instrument addressing personal data protection for several Member States of the Council of Europe. It would be appropriate to acknowledge that the personal data protection afforded by Turkish legislation was not equivalent to the level of protection in the European Union until the enactment of the DP Law. Furthermore, Turkey is still not recognized or listed as one of the countries with an adequate level of protection by the European Commission. Therefore, in order to transfer personal data from Turkey to the European Union based on the Customs Union Agreement, it is recommended that data controllers in Turkey obtain the explicit consent of their data subjects or utilize the aforementioned letters of commitment by also meeting the conditions for one of the exemptions discussed above.

Key issues and major risks

Despite the similarities between Turkish and EU legislation, the DP Law differs from the Directive 95/46/EC and the GDPR in a number of crucial aspects, especially with regard to the transfer of personal data abroad. Therefore, companies that intend to conduct business in Turkey (and multinational firms in particular) should not make the mistake of assuming that the procedures regarding the transfer of personal data would be the same in Turkey as in the EU merely because the DP Law is based on the Directive 95/46/EC, and they should seek to obtain the explicit consent of

their data subjects. If they wish to transfer personal data abroad without the explicit consent of the data subjects, they must ensure that the data transfer is covered under one of the exemptions explained above by also utilizing the Turkish versions of the letters of commitment and obtaining the Board's approval accordingly.

Administrative fines: Even though the DP Law lists the administrative fines that will be applied to parties who fail to fulfill their obligations under the DP Law, no administrative fine has been determined in relation to transfers of personal data abroad.

However, the DP Law asserts that those who fail to fulfill their obligations relating to data protections shall be subject to an administrative monetary fine ranging from 15,000 Turkish liras up to 1,000,000 Turkish liras (around US$160,000). Since transferring personal data abroad without obtaining the explicit consent of the data subjects or without executing the letters of commitment and obtaining the Board's approval would be deemed to constitute a violation of data protection obligations, these administrative fines might be applied to data controllers who fail to transfer personal data abroad according to the rules of the DP Law.

Criminal sanctions: Moreover, the DP Law declares that the relevant articles of the Turkish Criminal Code shall also be applied for crimes pertaining to the handling of personal data. According to the relevant article of the Turkish Criminal Code (Article 136), parties that convey, give, transmit or acquire personal data illegally may be subject to imprisonment from two to four years.

AUTHORS

İlay Yılmaz and Gonenc Gürkaynak are Partners at ELIG Gürkaynak Attorneys-at-Law.
Emails: gonenc.gurkaynak@elig.com
ilay.yilmaz@elig.com

REFERENCES

1 Guidance on the Transfer of Personal Data Abroad, available (in Turkish) at kvkk.gov.tr/SharedFolderServer/CMSFiles/ca163cb6-39ad-4024-870a-8a9508c92387.pdf
2 kvkk.gov.tr/Icerik/5255/Taahhutnameler (in Turkish)
3 The countries which the European Commission has deemed adequate for cross-border data transfers are Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, The United States (for data protected by the EU-US Privacy Shield) and Uruguay.
4 Customs Union Agreement between Turkey and European Union, available at www.avrupa.info.tr/sites/default/files/2016-09/Custom_Union_des_ENG_0.pdf
5 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108), available at rm.coe.int/1680078b37

Finland issues an important RTBF decision

Finland's Supreme Administrative Court ruled in August that Google must remove a convicted man's information from its search engine data, due to implications for his privacy. The Data Protection Ombudsman, Reijo Aarnio, had said in his opinion that the prison sentence constituted inhuman suffering for the mentally-impaired man, and the fact that anyone could access information about his health on the Internet had a detrimental impact on his life, and irreparable damage.

The man had been sentenced to ten years and six months in prison for a "diminished responsibility murder". The imprisonment had ended in July 2017. The Supreme Administrative Court found that information about the man was sensitive information.

This case will set an important precedent for Right to be Forgotten (RTBF), as this case puts privacy first against the public's right to information. Finland thus applied the EU's Right to be Forgotten although it has not yet passed adapting legislation for the GDPR. The 2014 decision by the European Court of Justice on a Spanish man, Mario Costeja González, against Google, introduced this principle.

France's DPA publishes assessment of the first four months of the GDPR

France's Data Protection Authority, the CNIL, says that the GDPR has significantly raised individuals' awareness of privacy issues. On the other hand, it has caused the office much extra work. Since the GDPR entered into force, it has received more than 600 data breach notifications (it had been typically seven per day). Also, the number of complaints has gone up 64% compared to last year.

Some 24,500 organizations have designated a Data Protection Officer, and two organisations have started collective action proceedings; la Quadrature du Net and NOYB (against Google, Instagram, WhatsApp and Facebook).

France adopted, on 21 June, its new national law implementing the GDPR. A separate implementing decree was adopted on 1 August. The CNIL has issued several new guidelines, including on blockchain. It says that the GDPR applies to blockchain when it includes personal data, and organisations should conduct a Data Protection Impact Assessment to evaluate any risks to personal data, and the necessity and proportionality of using this technology.

• *See www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application*

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK