Privacy Tracker

Alerts and legal analysis of legislative trends

Using the cloud under the Turkish data protection law

Ozan Karaduman

Privacy Bar Section | Privacy Tracker | Jan 11, 2017

The Turkish law on the protection of personal data came into force April 7, 2016. It is important not just because it is the first of its kind regulating the protection of personal data from a general perspective, but also because it brings many new obligations with which persons or entities dealing with personal data have to comply.

The Data Protection Law is also a step towards the ultimate goal of harmonizing the Turkish legislation with the European Union legislation. Taking this into consideration, the Data Protection Law was prepared based on the European Directive 95/46/EC. Although the Data Protection Law is very similar to the Directive, it is not a complete replica.

One major difference involves the obligation of consent and how companies providing cloud services in Turkey must take this obligation into consideration. Rather than a full analysis of the rules for different types of cloud services under the Data Protection Law, this article aims to raise awareness for cloud service providers and their clients regarding the obligation of consent under the Data Protection Law and how it is different than the Directive.

Obtainment of consent – the difference

The general rule for processing of personal data and sensitive personal data is that such data may only be processed with the explicit consent of the related person. Explicit consent has been defined as: consent, related to a specific issue, based on information and declared with free will. As it may be understood from this definition, the Data

Protection Law does not deem all kinds of consents as sufficient. The person whose data will be processed must know to what they give consent and must clearly express their consent. In this context, for example, consent obtained in English from non-English speakers in Turkey would not be deemed explicit consent.

At this point, it is important to mention the difference between the Data Protection Law and the Directive in relation to consent with regards to cloud services. Under the Directive, there is a definition of third party, which excludes data processors. Under the Data Protection Law, there is no definition of third party, and therefore everyone except the data subject and the data controller is a third party. As a result, data processors (including cloud service providers) are third parties under the Data Protection Law. Meaning, in order for a data controller to transfer its data to a cloud service provider and have the cloud service provider process the data, the data controller would need to obtain the consent of the data subjects or would need to fall under one of the exceptions set forth below. The Data Protection Law does not deem the existence of an agreement between the data controller and the cloud service provider sufficient for the transfer of data from the data controller to the service provider.

Exceptions for the obtainment of consent

Although the Data Protection Law has proposed obtaining consent of the related person as the main rule for the processing of personal data, certain exceptions have been introduced to this rule. In the presence of any of the following exceptions, data may be processed without explicit consent of the data subject:

- In cases clearly proposed in laws,
- In cases necessary for protection of life or bodily integrity of the person, or another person, in case such person cannot express consent or whose consent is legally invalid due to physical disabilities,
- In case it is necessary to process the personal data, related to the parties of the contract, provided that it is directly related to establishment or performance of a contract,
- In case it is mandatory for the data controller to fulfil its legal obligations,
- In cases where the data is made manifestly public by the related person,
- In cases mandatory for establishment, exercise or protection of a right,

- In cases where the processing of data is mandatory for legitimate interests of the data controller, provided the fundamental rights and freedoms of the related person are not prejudiced.

Unlike exceptions related to personal data, the situations constituting exceptions related to sensitive personal data have greater limitations. These exceptions are: When processing personal data of a special nature – with the exception of health and sexual life, such processing must be allowed by laws. For data related to health and sexual life, the exception to the requirement of consent is that the processing of such data can only be conducted by persons under the obligation of confidentiality or by authorized institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and care services.

Moreover, in addition to the processing conditions given above, the Data Protection Law states that, as an additional condition for processing sensitive personal data, sufficient measures determined by the Data Protection Board must be adopted. Since the additional measures in question have not been determined, this condition is not applicable at this time.

Transfer of personal data

The Data Protection Law has also regulated the transfer of personal data to third persons and foreign countries. This is important for the cloud service providers as in order for a cloud service provider to be able to provide service the client needs to transfer the data to the service provider (which will be regarded as a third party), and in some cases the facilities of the service providers are located abroad. The general rule for both transferring the data to a third party and transferring the data abroad is that the transfer must be made following the explicit consent of the data subject. As in processing data, exceptions have been given in the law concerning transfer.

With respect to transfer to third persons, in cases where the data to be transferred is within the "explicit consent exceptions" specified above, explicit consent will not be sought for transfer.

Concerning transfer to foreign countries, if the data to be transferred is included within the exceptions to explicit consent given above, it must be considered whether the destination country has "sufficient protection" to be able to conclude the transfer abroad without explicit consent. The data processed within the framework of such exceptions, may only be transferred when there is sufficient protection in the destination country. If there is not sufficient protection in the destination country, the

data controller in the foreign country must provide a written commitment stating that sufficient data protection would be provided and the Personal Data Protection Board must authorize the transfer.

The Personal Data Protection Board will determine countries that provide sufficient protection. The board has been formed very recently and has not been able to list the countries providing sufficient protection as of the date of this article.

Conclusion

Under the Data Protection Law, an agreement between the cloud service provider and the cloud service client is not sufficient for the client, a data controller, to transfer the personal data it holds to the cloud service provider. If the personal data is to be transferred to the cloud service provider in Turkey, one must review whether the data subjects have given consent to the data controller for their personal data to be transferred to the cloud service provider (the data processor). If consents have been given, the personal data can be transferred; if not, the personal data can only be transferred if the transfer to the cloud service provider falls under the exceptions set forth above.

Additionally, if the facilities of the cloud service provider are abroad and therefore the personal data will be transferred abroad, the same principles apply; the only additional step to be taken is to see whether the country where the data is to be transferred offers sufficient protection as mentioned above.

The Personal Data Protection Board's list of countries offering sufficient protection will also be very important once it is published. In cases where the client does not know where the cloud providers' servers are located or does not have the right to choose among the available servers, they must inquire about those locations. And if the country where the servers are located is not among the countries on the list, they must take the necessary steps mentioned above.

This requirement of consent to transfer personal data from data controllers to data processors is onerous. In an age where businesses tend to rely on cloud services more, this will be a complication in the business process. A cloud service provider is not an ordinary third party; it acts under the authority of the data controller and although the power of the client on the processes of the cloud service provider changes based on the cloud service type, in all cases the cloud service is a part of the business organization of the client. Moreover, the Data Protection Law sets forth that a data controller will be jointly liable with the data processor for the security of the personal data and this

should be sufficient motive for the clients to choose their cloud service providers wisely and to protect the personal data. In light of the foregoing, we believe that the cloud service provider should not be subject to the same consent requirement as an ordinary third party.

photo credit: Turkish flag via photopin (license)