Data Protection in Turkey & New Data Protection Requirements in E-Commerce

In the 21st century, thanks to the continuous technological developments, individuals, companies and governmental authorities are easily able to access an immeasurable amount of data, with a simple click. The other side of the coin is that it is technically possible to collect internet users’ personal data without their consents.

Protection of personal data has a direct influence on the development of e-commerce. Individuals tend to use the internet more, if they trust that their personal data are protected and not shared with third parties. With the widespread usage of the internet and e-commerce, this situation prompted governments to adopt strict measures for the protection of personal data. In Turkey, there is no specific piece of legislation that governs the protection of personal data. In fact, data protection is a new concept in Turkish law and most people are not aware of their rights and obligations. There is a draft law on data protection (the “Draft Law”). This was prepared in 2008, but has not been enacted yet. Data protection is dealt with under the Turkish Constitution (the “Constitution”) and various laws (such as the Civil Law, the Labor Law, the Turkish Code of Obligations (the “TCO”), the Turkish Penal Code (the “TPC”), etc.) at a high-level.

The Constitution stipulates that every individual has the right to request protection of his/her personal data. This right entitles individuals to be informed of their personal data, to have access to their data, request revision or removal of their data and learn whether their data is used for right purposes. In addition, an individual’s personal data may only be processed upon his/her explicit consent.

None of the laws noted above explicitly describe what should be considered as “personal data”. However, according to the criminal law chambers of the Court of Appeals, a “personal data” can be any type of information that identifies an individual and distinguishes him/her from other individuals in the society. According to the Court of Appeals, identity information (such as identity number, name, surname, date and place of birth, parents’ name, etc.), place of residence, criminal records, occupation, level of education, personal phone number, e-mail address, blood type, marital status, fingerprints, DNA, biological samples such as hair, nail and saliva, sexual or religious preferences, medical records, ethnical origin, philosophical, religious or political view, memberships with trade unions, are amongst an individual’s personal data.\(^1\) If the data is considered to be anonymous or easily accessible, that data may not be classified as personal data.

Personal data protection is also regulated by the TPC. According to Article 135 of the TPC, if a person illegally records personal data, he/she will be sentenced to imprisonment for one to three years. Similarly, Article 136 provides that a person who illegally obtains personal data or shares them with or spreads them to third parties will be sentenced to imprisonment for two to four years. If the offender of the crime is a legal entity, then such legal entity will be subject to security measures (e.g. return of monetary benefits that are gained through the

\(^1\) Court of Appeals, 12th Criminal Law Chamber, E. 2013/10672, K.2013/15772, T. 10.06.2013.
crime). In addition, from a civil law point of view, these actions are considered as a breach of personal rights and the offender (an individual or a legal entity) may be requested to indemnify damages of the person whose personal rights are violated.

The Labor Law is another piece of legislation that regulates the protection of personal data. Under Article 75 of the Labor Law, an employer must keep personal files for each employee. These files must contain information in relation to the employment relationship such as employees’ position in the company, salaries, benefits, number of used/unused annual leave days, etc. Pursuant to this requirement, the files may contain personal data of employees. The same article states that an employer must act in good faith in compliance with the Labor Law and other relevant legislation while using employees’ personal information, and keep them confidential for the employees’ benefit. Similarly, Article 419 of the TCO states that an employer may use the personal data of an employee, only if it is required for the performance of a contract or in order to determine whether or not the employee is inclined to his/her duty.

Protection of Personal Data under the Law on Electronic Commerce

The long-awaited Law on Electronic Commerce (the “E-Commerce Law”) entered into force on 1 May 2015. The E-Commerce Law’s primary purpose is to regulate the fundamentals of electronic commerce and to protect the privacy of individuals who carry out transactions electronically. The E-Commerce Law defines “electronic commerce” as the activities and transactions that occur in the electronic environment without any face to face communication. The E-Commerce Law primarily regulates the obligations of individuals and legal entities that provide electronic commerce services and electronic commerce environment for third parties’ financial and commercial activities.

Under Article 10 of the E-Commerce Law, service providers and intermediary service providers must protect and preserve the individuals or legal entities’ personal data obtained within the scope of electronic commerce activities. They are not entitled to transmit such personal data to any other third parties without the consent of individuals or legal entities. Although the E-Commerce Law governs the protection of personal data, it does not contain any provision on how this protection mechanism should be enforced. Currently, it is possible to say that the provisions related to data protection under the E-Commerce Law are not sufficient to provide a real protection.

The implementation of the E-Commerce Law will be addressed by secondary legislation to be prepared by the Ministry of Customs and Trade. As of the date of this bulletin, there is no draft regulation detailing the E-Commerce Law’s provisions on data protection, except for the Regulation on Commercial Communication and Commercial Electronic Messages, which provides that in order for personal data to be shared with third parties and/or be processed or used for other purposes, the relevant individuals’ consent must be obtained.

Draft Law on the Protection of Personal Data

Turkey, as a member of the Council of Europe has signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981, but the Turkish Parliament has not yet ratified this convention. Turkey does not currently have a specific data protection law in force. The Turkish Parliament is working on the Draft Law, which has been in draft form since 2008. The Draft Law was prepared to ensure compliance with the

---

2 Please see our e-bulletin dated November 2014, titled “Overview of the New Electronic Commerce” for further information on the Law on Electronic Commerce.
European Union’s data protection policies. According to the Draft Law, any personal data including information on an individual’s religion, political view, ethnical origin, membership to an association or a labor union, health and private life and criminal penalties cannot be kept, without such individual’s written consent. Under the Draft Law, in order to transmit an individual’s personal data to a foreign country, this individual’s prior written consent must be obtained.

The Draft Law stipulates the establishment of a “Data Protection Board” (as a public organization with administrative and financial autonomy) to regulate data protection related matters. The Data Protection Board will be the highest authority, authorized to render decisions on whether there is violation of personal rights linked with data protection. It will also be empowered to prepare regulatory procedures regarding the processing of personal data. Following its establishment, the Data Protection Board will set up a data recording registry. Individuals and legal entities processing personal data will be registered with this registry before forming a data-file.

According to the Draft Law, personal data -following receipt of its owner’s consent- can be transmitted to foreign countries, only if there is an equivalent legislation on data protection in the relevant foreign country. If there is no such protective legislation in the foreign country, the Data Protection Board’s approval will be required to transmit personal data. Since the Draft Law is not yet enacted, as of today, there is no governmental authority in Turkey to deal with such matters.

Gökçe İldiri (gildiri@kolcuoglu.av.tr) & Melis Özenbaş (mozenbas@kolcuoglu.av.tr)

© Kolcuoğlu Demirkan Koçaklı Hukuk Bürosu 2015