**Informative Note Obtained from Relevant Turkish Authorities**

Turkey has signed and ratified the main human rights treaties. Additionally Turkey is party to the European Convention on Human Rights and recognizes the right to communications to the European Court of Human Rights. According to the Article 90 of the Turkish Constitution, these conventions and treaties, which include the right to privacy, have supremacy in the Turkish law system.

According to the Turkish Constitution;

- Turkey is a democratic state governed by the rule of law, respecting human rights (article 2)

- Everyone has the right to demand respect for his/her private and family life. (article 20)

- The domicile of an individual shall not be violated. (article 21)

- Everyone has the freedom of communication. Privacy of communication is fundamental. (article 22)

- Everyone has the right to own and inherit property. (article 35)

The articles 20,21 and 22 of the constitution have been amended, with the act (Nr: 4709) dated 3 October 2001, so as to align the specific restrictions on these rights to be within the framework of European Convention on Human Rights.

The right to individual communications to the constitutional court was recognized by the act (Nr: 5982) dated 7 May 2010 amending the article 148, governing the mandate of the constitutional court. By this amendment, individuals will have the right to apply to the constitutional court before applying to the European Court of Human Rights.

In addition to this provision, the same amendment included the addition of a clause to the article 20 of the constitution, according to which, everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person’s explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.

Turkey gave start to its studies to make a specific law regarding data protection with regard to the EU harmonization process in 1995. A commission was formed to prepare a law regarding data protection. The commission finished its studies in 2003 by submitting the Draft Law Regarding Data Protection.

The Draft Law, which sets the regulations regarding the content and procedures of processing personal data, so as to protect the fundamental rights of the individuals has been transferred to the Prime Ministry in order to be discussed in the Parliament. Once the enactment procedure is completed, the draft law is designed to be the framework law and all relevant regulations will be aligned with this legislation.

International principles related to the processing of personal data, transfer abroad of these data, the rights and obligations of those processing these data, principles related to the security of these data and a mechanism to monitor and oversee this field is envisaged in the said draft law.

The Board for Protection of Personal Data, which is planned in the draft law to be the said monitoring mechanism, will have the mandate to conduct ex officio monitoring and investigation duties, regarding the processing personal data in accordance with the law, upon communications from individuals. The Board also has the mandate to conduct regulative and administrative sanctions in necessary situations.

In addition to this Board, Turkish Human Rights Institute was founded by the law (Nr. 6332) on 21 June 2012, in order to conduct work on protection and promotion of human rights, prevent abuses, combat torture, evaluate and monitor communications in this field, education and research projects in this field.

With the aim of regulating the processing and storage of personal data, as well as protecting the privacy of these data in the electronic communications sector, a guideline was issued by the Ministry of Transport, Maritime Affairs and Communication. The said guideline was enacted on 28 July 2012.

In addition to the above mentioned regulations in the field of privacy and the protection of personal data, amendments have been made to the penal code and penal procedure code in order to ensure respect to private life and its protection.

In this respect, some crimes cited in the Turkish Penal Code and some protection measures in the Turkish Penal Procedure Code have been reorganized by the law (Nr: 6526) dated 21 February 2014, which foresees amendments in the Anti-Terror Law, the Penal Code and some other laws.

Important amendments were made by the said law, in the fields including, detection, interception and recording of communication and monitoring measures by technical means. The decision making regarding these interception measures was put under a more effective process of supervision and the timeframe for these measures was tightened. A more effective protection of private life is aimed by these amendments.

With this aim, with respect to the detection of communications,

\* The notion of “serious suspect based on concrete evidence” for the detection of communications was introduced

\* A consensus vote among the members of Heavy Penal Code is necessary for this measure

\* A document indicating the owner of the telephone line is necessary for this measure.

\* The timeframe of the measure can be limited by 3 months (previously 6 months) and it can be extended for only an extra 3 months.

With respect to designation of covert investigator,

\* A covert investigator can be designated only under the circumstances of “serious suspect based on concrete evidence”

\* A consensus vote among the members of Heavy Penal Code is necessary for the designation of a covert investigator.

\* Information obtained as irrelevant to the crime will be deleted immediately.

With respect to interception by technical means,

\* The notion of “serious suspect based on concrete evidence” for the detection of communications was introduced

\* A consensus vote among the members of Heavy Penal Code is necessary for this measure

\* The timeframe of the measure can be limited by 4 weeks (previously 8 weeks) and it can be extended for only an extra 4 weeks.

The amendments with the law (Nr: 6526) also include provisions regarding the protection of private data. In this respect, the sanctions for illegal accumulation, recording, sharing, obtaining and keeping of personal data have been increased. These sanctions are multiplied if the relevant data is subject to measures mentioned above. By this clause, a more effective protection of the private data, obtained by legal proceedings, is aimed.

Processing data illegally is defined as a crime in Turkish Penal Code. Individuals whose data are processed (and/or kept) have right to apply to the court (Turkish Penal Code, Article 25) to demand compensation of pecuniary and non pecuniary damages. (Code of Obligations, Article 58) Law Regarding Electronic Signature includes provisions related to the obligations of electronic certificate service providers. According to the Law, service providers can collect only necessary data of the candidates for e- certificate. Unrelated data should not be collected. Service provider has obligations to ensure the security of data (Article 12). Additionally, Law on Right to Information, which provides individuals to access information, excludes disclosure of personal data. If public security is the matter, personal data can only be collected with the consent of data subject (Article 21).

In addition to the provisions of the Penal Code and Penal Proceeding Code, the specific regulations on data protection in telecommunications in Turkey are as follows:

Electronic Communications Law, By Law on Consumer Rights in Electronic Communications by Sector, By Law on Authorization in Electronic Communications Sector and Law on Processing and Protection of Privacy of Personal Data in Electronic Communications Sector.

Electronic Communications Law is the framework legislation which provides general provisions regarding electronic communications sector. The Law charges Information and Communication Technologies Authority (ICTA) with making regulations and carrying out necessary supervisions on processing and privacy of personal data (Article 6.1.c). According to the Law, ICTA can impose obligations to operators for maintaining security of their subscribers' data (Article 12.2.d). Unsolicited communication is the only issue regarding data protection which is dealt in details in the law.

The law leaves other issues regarding data protection to be held by inferior legislations. In this regard, By Law on Authorization in Electronic Communications Sector which includes the provisions of the overall rights and obligations of operators has a general provision for data protection as well. According to it, operators are obliged to obey the regulations regarding protection of personal data (Article 19.2.ç).

By Law on Processing and Protection of Privacy of Personal Data in Electronic Communications Sector is the main secondary legislation that concern provisions for data protection in electronic communications. It includes detailed provisions regarding data retention, traffic data, location data and sanctions for infringements. According to it, operators are obliged to provide network security and to inform their subscribers about the risks. They cannot process traffic and location data for the purposes other than their service purposes. They should erase such data as soon as the specified purpose is achieved.