

**Comparison of Turkish Data Protection Law with EU Directive 95/46/EC**

Authors: Gönenç Gürkaynak, Esq., İlay Yılmaz and Nazlı Pınar Taşkıran, ELIG, Attorneys-at-Law.

Turkey's newly enacted Law on Protection of Personal Data ("Law") is based on EU Directive 95/46/EC ("Directive") on protection of individuals with regard to the processing of personal data and on the free movement of such data. Although the Law is mainly based on the Directive, it is not identical and it differs from the Directive in certain points. The main difference between the Directive and the Law is that Directive focuses on the act of processing personal data rather than the parties to such processing; whereas the Law mainly provides rights and imposes obligations on the parties of a data processing act. Nevertheless this difference also arises due to the nature of these two different pieces of legislation, as the Directive is a supra-national regulation and the Law is a national regulation that is directly binding and applicable without requiring further need for another law. Below please find significant differences of the Law and the Directive:

**Sensitive Personal Data**

The Directive sets out special categories of personal data as "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life". The Law also considers such data as sensitive data, but also adds "appearance and clothing, data relating to criminal records and biometric and genetic data" to the list of special categories of personal data. Both the Directive and the Law stipulates that sensitive personal data may only be processed upon the data subject's consent. For processing of sensitive personal data without the consent of the data subject, the Directive sets out detailed provisions, whereas the Law states that any special data except for data related to health and sex life of the data subject may be processed without the data subject's explicit consent, where e.g., stipulated by laws, or in case of sexual and health data, for the purpose of protecting public health.

**Transfer of Personal Data**

The Law distinctively regulates the transfer of personal data, by distinguishing the transfer of personal data in Turkey and abroad. The Directive regulates transfer of data to non-EU countries and requires that such third party countries must provide an adequate level of protection. The Law's procedure on data transfer is similar to the Directive's, but there are some differences which appear to be enacted in relation to certain developments within Turkey.

Article 9 of the Law regulates transfer of data to third part countries, and states that personal data may only be transferred with explicit consent of the data subject. Accordingly, the adequate level of protection requirement only applies in cases where data processing without the data subject's explicit consent is legitimate. For example, if data processing is necessary for the performance of a legal obligation by the data controller, such as providing data to governmental authorities for tax purposes, the data subject's explicit consent would not be required. In such a case, the data may be sent outside Turkey without obtaining explicit consent of the data subject, provided that the relevant foreign country provides an adequate level of protection. Similar to the application of the Directive, there is an authority, i.e. the Data Protection Board ("the Board") to determine whether the relevant foreign country provides an adequate level of protection or not. However, since the Board will be established within 6 months, this procedure will be enlightened once the Board is established and the provision is implemented in practice.

As for sensitive information, in cases where the personal data may be processed without explicit consent of the data subject (e.g. where stipulated by laws, or in case of sexual and health data, for the purpose of protecting public health), sensitive data may be transferred abroad without explicit consent; provided that a) the relevant foreign country has an adequate level of protection, as determined by the Data Protection Board ("the Board") or if not, b) the data controllers in Turkey make a written declaration that they ensured adequate level of protection in the relevant foreign country and Data Protection Board grants a permission.

In addition to the rules explained above, a new provision that is not included within the Directive states that where Turkey's or the data subject's interests will be seriously

undermined, personal data may be transferred abroad upon the authorization of the Board by taking the relevant public institution or authority's opinion. The provision requires Board's permission, which is rendered by taking the relevant public authority's opinion, for transfer of data which may seriously undermine data subject's or Turkey's interests.

The provision is ambiguous as it does not (i) specify any criteria to assess or determine how the transfer of data abroad may seriously harm Turkey's or relevant person's interest, (ii) precisely define any situation or instance in which transfer of data abroad will be subject to the Board's permission and (iii) designate any authority or specify who will decide whether permission is required with respect to the transfer of data abroad. The Law does not define or determine the scope of or specify any condition or term referred therein.

Since there is no specification or criteria as to these ambiguous conditions that require the Board's permission, the possible consequences of implementation of this provision is not foreseeable at this stage. A data controller or processor may not be in a position to assess and determine whether a data transfer could seriously harm Turkey's or relevant person's interest and require the Board's permission. Considering this provision as a general requirement for all data transfers abroad would be against the purposes of the Law and the article related to data transfers abroad. Therefore one should consider this provision as an exceptional requirement for sensitive issues.

There is also no guidance on how the transfer of personal data will be made between the group companies at this stage.

### **Data Controllers' Registry**

Article 16 of the Law states that Presidency of the Board will establish and maintain publicly available register of controllers (the "Data Controllers' Registry") under the supervision of the Board. Real or legal persons processing personal data must enroll to the register before they start processing. However, the Board may provide an exemption from the obligation to enroll to the registry in so far as this is in line with the objective criteria to be determined by the Board such as the characteristics and the number of data to be processed, whether or not data processing is required by law or whether or not data will be transferred to third parties. The

application to enroll to the register will be made through a notification that includes certain information as set out by the Law. This is a procedure similar to the obligation to notify the supervisory authority which is set forth in Article 18 of the Directive. However, the European Council's approach on the matter differs from the Law's approach. The European Council's approach aims the final control, eliminating notifications and limiting authorizations to the bare minimum and focuses on notification of data breaches. In this regard, the Law appears to be more restrictive than the EU legislation in terms of the detailed registry approach.

### **The Data Protection Board and Data Protection Authority**

The Law requires establishment of a Personal Data Protection Authority ("Authority") as a public entity, which has administrative and financial autonomy, in order to perform the tasks assigned to it by the Law. The Law also states that the Data Protection Board will be the decision making organ of the Authority, which performs the tasks and exercises its authority assigned to it by the Draft Law and other legislation, independently and under its own responsibility. It is also stated that on issues related to its duties, the Board cannot be given any order, directive, advice or suggestion by an organization, an office, an authority or a person of any kind. The EU Directive requires member states to establish authorities to watch and supervise the processing of personal data and principles in regards to this processes, which shall exercise their functions with complete independence from the legislative and executive bodies and emphasizes that this independence is an essential component of the protection of individuals in regards to the processing of personal data; whereas the Law states that the Data Protection Authority shall be related to the Prime Ministry which might cripple independency of the Authority.

The differing provisions of the Law and how they will apply in practice are expected to be clarified during the upcoming months, once the secondary legislation is enacted and the relevant authorities are established.

Article contact: Gönenç Gürkaynak, Esq.

Email: [gonenc.gurkaynak@elig.com](mailto:gonenc.gurkaynak@elig.com)

*(First published in Mondaq on April 25, 2016)*