New Requirements for Banks in terms of Data Storage and Data Transfer

The Banking Law No. 5411 ("Banking Law") was amended by the Law No. 7222 Amending Banking Law and Other Codes (“Amendments”), published in the Official Gazette on February 25, 2020, introducing important provisions regarding the data practice of banks'. Based on the provisions, Banking Regulation and Supervision Agency (“BRSA”) introduced Regulation on Banks’ Information Technology and Electronic Banking Services (“Regulation”) published in the Official Gazette on March 15, 2020, as a secondary regulation, and have binding provisions related to data processing and transferring.

Definition of Customer Confidential Information

According to the amendments on Article 73 of Banking Law, all the data relating to real and legal persons generated after establishing a customer relationship with banks for banking activities are deemed as customer confidential information.

As can be noted in this definition, customer relationships established in line with services performed by banks other than banking activities are excluded from the scope of customer confidential information. Besides, the data obtained by banks in cases where they provide services without establishing a customer relationship indirectly are also excluded from this definition.

The definition of customer confidential information can both contain personal data and non-personal data. Thus, it is important to seperatly identify if the data is personal data according to Law on Personal Data Protection (“PDPL”) and stays within the scope of customer confidential information.

The transfer of customer confidential information

As a result of an evaluation based on economic security, the BRSA is authorized to prohibit the transfer of customer confidential information or banking secrets with third parties abroad, as well as to make decisions regarding information systems used by banks and their backups.

Customer confidential information can only be transferred to third parties abroad or within the country upon specific instructions or requests of the customer. The provision clearly states that customer’s explicit consent, obtained according to PDPL, is not sufficient to transfer the customer confidential information to third parties within the country or abroad. The only exceptions to the restrictions of transferring data are the mandatory legal provisions in other laws, audits, court requests, M&A deals and information that must be disclosed to some specific ministries.

Whether it is in the scope of the exemptions or not, data deemed as confidential can only be shared if it is limited to stated purposes and is exclusively restricted with the attainment of such objectives.

It is important to highlight that it is not possible to transfer customer confidential information abroad without the specific instructions or requests of the customer based on the tools stated at PDPL Article 9 and the Binding Corporate Rules announced by Data Protection Authority (“DPA”).

In this context, there are two issues to be taken into account when it comes to the transfer of customer confidential information abroad: (i) Receiving the customer's instruction or request per the Banking Law, and (ii) Complying with the requirements of Article 9 of PDPL.

System Localization

As stated above, with the Amendments, BRSA has been authorized to decide to keep the primary and secondary systems used by banks in carrying out banking activities within the country.

Article 11/4 of the Regulation on the Internal Systems and Interior Capital Adequacy Assessment Process of the Banks issued by BRSA before the Amendments, was already obliging the banks to keep their primary and secondary systems within the country. Article 25 of the Regulation, issued after the Amendments, also indicates that the banks must keep their systems, regardless of how many back-ups there are, within the country. In addition, in case of receiving an external service or cloud computing service for an activity within the scope of primary or secondary systems, the information systems used by the external service provider or cloud computing service in carrying out the activities must also be installed within the country.

Besides the localization requirement, there are further requirements for approving the external service provider in respect of services and products provided in the fields of critical information systems and security. According to Article 29 of the Regulation, it is an important selection criteria that the products/services related to security and critical information systems are produced in Turkey, or the producers have an R&D center in Turkey.

Sanctions

According to Article 159 of Banking Law, the ones who do not comply with the conditions of transferring customer confidential information according to Article 73 can face imprisonment for up to three years and a judicial fine of up to two thousand days. Also according to Article 148 of Banking Law, BRSA is authorized to impose administrative fines on those who do not comply with the Banking Law or regulations issued pursuant to the Banking Law. On the other hand, the incompliant transfer of personal data within the scope of PDPL might be subject to administrative fines under the PDPL and criminal sanctions under the Turkish Criminal Law.

Conclusion

Evaluating the Amendments with the provisions of the Regulation together, firstly, the banks must define the data they hold in line with the customer confidential information definition at Banking Law and personal data definition on PDPL. Then, the transfer method must be set according to the requirements specified for each data set. In addition, there are still uncertainties regarding the transfer of personal data abroad, so it would be appropriate to consider different dimensions of data transfer within the scope of both personal data and customer confidential information.