25 March 2020

INFORMATION NOTE ON THE REGULATION ON THE INFORMATION SYSTEMS OF BANKS AND ELECTRONIC BANKING SERVICES

In order to align the current legislation with the European Union Payment Services Directive 2 and to strengthen the legal basis of open banking activities; ***Regulation on the Information Systems of Banks and Electronic Banking Services*** *("**Regulation**") has been published on the Official Gazette No. 31069 dated March 15th, 2020.*

I. INTRODUCTION

The draft regulation has been open for public consultation since December 25, 2008 and it has finally been finalized into a comprehensive legal regulation by the Banking and Supervision Agency ("**BRSA**") and recently published on the Official Gazette on March 15th, 2020. The Regulation will enter into force on July 1st, 2020.

Moreover, the Communiqué on the Principles of the Management of Information Systems' of Banks[1] ("**Abolished Communiqué**"), which constituted the only detailed regulation on the subject so far, has been abolished to be effective as of July 1st, 2020.

The Regulation, which also covers a number of provisions in the Abolished Communiqué with the taking into account the latest developments and increasing security requirements in today's information systems, contains important principles regarding information systems security and risk management for the banks. As a result, the banks operating in Turkey are now required to ensure their compliance with the Regulation through making additional investments and technical infrastructure upgrades.

The key elements of the Regulation are summarized below.

II. MAIN CHANGES INTRODUCED

1. First of all, certain institutional arrangements were envisaged with the Regulation in order to ensure that the banks' information systems management progress in line with the principle of good governance:

- An Information Systems Strategy Plan, Information Systems Strategy Committee and Information Systems Steering Committee must be established within banks by the approval of the board of directors as part of their duty of efficient monitoring of information systems.

- The data that is valuable for the bank and/or used in the banking activities as well as the tools, systems or processes where the data are transported, stored, transmitted or processed are defined as "*information assets".*

- The information assets that banks obtain and use in the course of their activities should be classified and recorded in an inventory (Information Asset Inventory) within the framework of an Asset Classification Guide prepared by the Information Security Committee to be created separately. By specifying the definition, relative value, security class, owner and guard of each

[1]Published on the Official Gazette numbered 26643 and dated 14 September 2007.

asset in the inventory, procedures of control for the security requirements of each information asset will be facilitated.

- In addition, it is envisaged that a corporate information strategies risk management process is required to be established to monitor and analyze the possible risks due to the use of information technologies in banking activities.

- Other functions and officials that needs to be designated for the management of banks' corporate activities are provided as; information security officer, liaison officer, information systems continuity management process officer, external service relations officer, information systems internal control officer and information systems internal audit officer.

2. The issue of information security management is dealt with in detail in the Regulation:

- The board of directors should establish an information security management system that takes reference of national or international standards or best practices and includes the performance of certain mandatory activities. The Information Security Committee, which is responsible for submitting annual reports to the board of directors, will be responsible for the management of the activities for the establishment and implementation of an information security policy.

- As regards data privacy; an aggravated duty of care has been introduced regardless of whether the media in which the data used in banking activities are kept is available on paper or electronic media. The encryption keys and algorithms to be developed for ensuring data privacy also should be compatible with today's technology.

- The data may be shared with third parties at home or abroad only in exceptional cases foreseen in the law or upon a request by client which can be proved through a written or permanent data storage medium.

- The concept of open consent, which is subject to widespread discussions within the framework of the Turkish Personal Data Protection Law No.6698 ("**PDPL**") as well as international data privacy regulations, is defined in the Regulation as "*consent on a specific subject, based on information and announced with free will*". In addition, it has been stated precisely that the clients' express consent to for the processing of his/her information cannot be foreseen as a prerequisite for the service to be provided.

- The methods of access to the information assets hosted by the bank by the clients has been regulated in detail and banks have been obliged to establish the necessary identification, password verification and track record mechanisms in line with the separation of duties principle. So much so that; relevant processes need to be designed and operated in such a way as to not allow a single person to start or complete a critical process by him/herself.

- In terms of network security, security configuration and cyber incident management; the protective mechanisms listed in the Regulation should be established. In addition, for cyber incident management, a Corporate Cyber Incident Response Team with sufficient technical and operational skills should be established. The Regulation also foresees the establishment of comprehensive training programs to increase information security awareness.

3. Outsource service procurement is regulated in detail as well:

- Regulation provides that banks' information systems may be outsourced as a whole or in part; provided that a number of conditions that predict the bank's control over information systems are fulfilled. In addition; an adequate oversight mechanism that enables the assessment and

management of the risks posed by the outsourced service as well as the maintenance of effective relationships with the service providers must be established by the management.

- The use of cloud computing services by outsourcing is also made possible by the Regulation.

- It is foreseen as possible to receive cloud computing services with a private cloud service model over hardware and software resources allocated to a single bank, or with a community cloud service model, where hardware and software resources are physically shared between multiple banks, but where separate resources are logically assigned to each bank and serving only that bank. On the other hand, receiving outsourced services with a community cloud service model in activities such as credit and credit card applications and payment services is subject to the permission of BRSA.

- However, if an outsource service or cloud computing service is received for an activity that is covered by the bank's primary or secondary systems, the information systems used by the service provider to carry out their service activities and their backups will also be evaluated within the scope of bank's primary and secondary systems and hence need to be maintained domestically.

4. Electronic banking services has been subjected to advanced standards for each distribution channel:

- Various electronic distribution channels that banks can provide services under today's conditions such as internet banking, mobile banking, telephone banking, open banking services and ATM and kiosk devices have been arranged under the title, "electronic banking services", and each distribution channel is subjected to detailed regulations in terms of authentication and transaction security.

- As in the Abolished Communiqué, for electronic banking services, the principle of informing customers clearly about all terms of service is adopted. In addition; basic information about the bank's legal personality, the rights and responsibilities of clients, the terms and conditions of service or any other explanation to inform the customers should be included on banks' own website or the website where the service is provided in a remarkable manner and these information and explanations should be clear and understandable.

- Moreover; it is deemed compulsory for all kinds of information involving sensitive or secret data such as receipts, extracts or bank statements to be transmitted to clients via electronic distribution channels of the bank itself. Within the framework of the regulation, "*sensitive data*" refers to the data belonging to the customer in the event of the seizure of which by third parties, the mechanisms of identification of clients would be damaged. Here, it should be noted that; the concept of "*sensitive data"* in the context of the Regulation appears incompatible with that of the PDPL.

III. OTHER PROVISIONS

With the aim to provide functionality in the units to be established pursuant to the Regulation, BRSA is authorized to define exceptions within the framework of criteria such as a bank's scale, information systems dependency, and number of personnel or outsourced services.

Should you have any queries on our above note, please do not hesitate to contact us.

Contact

Ece Güner Toprak
Managing Partner
eg@guner.av.tr

Ömer Erdoğan
Partner
oe@guner.av.tr

Güner Hukuk Bürosu
Levent Caddesi, Alt Zeren Sokak No.7 Levent
34330, İstanbul
T +90 212 282 4385
F +90 212 282 4305
info@guner.av.tr
www guner av.tr