Client Alert | Banking & Finance

The Draft Regulation on the Information Systems and Electronic Banking Services of the Banks announced for public consultation

January 2019

Authors: **Güniz Gökçe**, **Ege Güleç**, **Selin Kaledelen**, **Seçil Bilgiç**

On 25 December 2018, the Banking Regulatory and Supervisory Authority ("**BRSA**") published the Draft Regulation on the Information Systems and Electronic Banking Services of the Banks ("**Draft Regulation**"). The Draft Regulation will govern information systems management and electronic banking services as well as related risk management. Once adopted, the Draft Regulation will replace the BRSA's Communiqué on Principles Regarding the Information System Management of the Banks[1] ("**Communiqué**").

The Draft Regulation mainly covers those issues that are currently regulated under the Communiqué and the Regulation on the Internal System and the Internal Capital Adequacy Assessment Process[2]. In addition, there are some brand new areas of regulation by the BRSA under the Draft Regulation.

What is New?

Once adopted the Draft Regulation will be the most detailed secondary legislation governing information systems and electronic banking in Turkey. The Draft Regulation introduces many new concepts and procedures for the Banks, such as the requirements applicable to sensitive data, trace recording mechanisms and asset monitor.

Here are some highlights from the key new terms under the Draft Regulation:

Sensitive Data

"Sensitive data" is defined as "data qualified as secret and data used for identity authentication" and is subject to different rules compared to "non-sensitive data" on data secrecy, trace recording mechanism, cyber-incident management, network security, cyber security awareness, system improvement, movement and set-up, identity authentication, customer briefing and data localization requirements.

Although there may be an overlap, sensitive data differs from:

(i) "personal data" defined under the Personal Data Protection Law numbered 6698 ("**PDPL**"); and

1 published in the Official Gazette on 14 September 2007

2 published in the Official Gazette on 11 July 2014

(ii) ("sensitive payment data" defined and regulated under the Communiqué on the Management and Audit of the Information Systems of Payment Institutions and Electronic Money Institutions.

"Sensitive payment data" can be described as the personalized security credentials which are used in payment orders or user identification authentication, such as password, security question, certificate and encryption keys, PIN, card number, date of expiry, CVV2, CVC2 codes. Examples of "sensitive data" on the other hand, include debit card, credit card, and identification numbers. Therefore, it seems that "sensitive payment data" may overlap to a certain extent with what would constitute "sensitive data" under the Draft Regulation.

Generally, the Draft Regulation prescribes greater protection for sensitive data compared to non-sensitive data. By way of example, while Banks are only required to ensure secrecy of data used in their banking services, the Draft Regulation specifically requires Banks to use end-to-end secure communication while sensitive data is being transferred and to store sensitive data in encrypted form.

Information Assets and Asset Inventory

In order to ensure adequate controls for the security requirements of information assets, the Draft Regulation requires Banks to prepare a detailed asset inventory for all of its information assets by categorizing them. While the Draft Regulation does not provide a definition for the term "asset", it appears to be similar to its meaning under ISO/IEC 27001 International Standard[3].

The following information must be included for each information asset within the asset inventory:

a. Definition that will clearly distinguish the asset;

b. Its relative value for the bank;

c. Its location;

d. Its security class and values such as its secrecy, integrity, and accessibility that determined in the designation of that class;

e. The owner of the asset; and

f. The asset protector.

For all data having a value for the bank, Banks should also create a data inventory that includes the abovementioned items. In the scope of data inventory, information regarding the owner of the data and the data monitor should be included instead of the information regarding the owner of the asset and the asset monitor.

Trace Recording Mechanism

The Draft Regulation introduces a trace recording mechanism requirement for the Banks with respect to the transactions and incidents within the framework of their information system. This mechanism should enable the authorized persons to track cyber-incidents and gather evidence. Trace recording is more complicated than the "audit trace" which was a regulated concept under the Communiqué[4]. Trace recording includes both audit trace records and the records regarding the identity of the persons who had access or attempted to access the information asset and the type of transactions that were concluded by the user.

At minimum, trace recording mechanisms should include information regarding:

a. The system that created the record;

b. The data, time, and time zone for the record;

---

[3] ISO/IEC 27001 International Standard is a list of standards that can be used by the parties to assess an organization's ability to meet the organization's own information security requirements. Particularly, ISO/IEC 27001 lays out the requirements for establishing, implementing, maintaining and continually improving an information security management system.

[4] under the Communiqué, "audit trace" is defined as "records that would allow tracking a financial or operational transaction from start to the end".

c. The change made, the transaction or incident that created the record; and

d. The individual user or system related to the record.

Trace records regarding transactions that lead to a change in records regarding banking activities, transactions that change, copy, display, query, or allow to access sensitive data, activities that authorize access to, change, and retake critical information assets, as well as all unauthorized access attempts to these assets should be kept open to access within the bank for minimum three years. In addition, Banks should also back-up all trace records and store them for ten years in accordance with the Banking Law numbered 5411.

This storage requirement seems to create an exception for the obligation of deletion, destruction, and anonymization of personal data under the PDPL. Under Article 7 of the PDPL, processed personal data should be deleted, destroyed, or anonymized once the reasons necessitating their processing cease to exist. However, the Draft Regulation requires to store trace records, which may involve personal data, for ten years, i.e. even after the reason for processing ceases to exist.

Banks outsourcing their duties related to information systems should also ensure that the trace records created by the outsourcing company conform to the Banks' own standards and records are available to the Bank.

Telephone Banking

Though a common practice for many years, telephone banking was not directly regulated by the BRSA per se. The Draft Regulation aims to fill this void and includes a chapter on telephone banking where it lays out the security and service principles for telephone banking. Importantly, the Draft Regulation lists certain requirements for telephone banking, such as owning adequate telephone line capacity or giving the option to the customer to talk to a call-center official or customer representative.

Open Banking Services

As a response to the ever-increasing popularity of open banking services, which is recently regulated under the EU Regulations under the Payment Services Directive 2 ("**PSD2**")[5], the BRSA also sets some ground rules for such services.

Open banking services are defined as the electronic distribution channel that customers or parties acting on behalf of the customers execute banking transactions or instruct the bank to execute such transactions through remotely accessing the financial services provided by the bank through API, web service, or FTP. While API is defined as application programming interfaces that are created so that a piece of software may utilize the functions designed under another, the Draft Regulation does not provide definitions for web service and FTP. Moreover, according to the Draft Regulation, retail customers may not benefit from open banking services and banks may not use these services as a channel for internet banking.

The Draft Regulation also foresees an important exception for open banking services and states that, provided that communications between the customer, party acting on behalf of the customer, and the bank take place through end-to-end secure means, and banks adopt additional controls and limit the customers' access to sources, authentication mechanisms that include only one component will not violate the Draft Regulation's default two independent components requirement.

What has Changed?

In addition to the new concepts and regulations explained above, the Draft Regulation introduces new layer of principles and procedures for certain concepts which are currently regulated under the existing regulations.

[5] The PSD2 is a Directive issued by the European Commission which regulates payment services throughout the European Union. Aiming to increase consumer protection, promote innovation and improve the security of payment service, PSD2 builds on the first Payment Services Directive which was introduced in 2009 so as to create a single market for payments in the European Union. Specifically, PSD2 enables bank customers, both retail customers and businesses, to use third-party providers to manage their finances.

Information Systems as Corporate Management Applications

Similar to the Communiqué, Article 4 of the Draft Regulation provides that the Board of Directors is responsible to:

(i) administer the information system management as part of corporate management practices;

(ii) procure necessary human resources and funding for the proper management of the information systems; and

(iii) ensure effective control over the information systems so as to guarantee the safety, confidentiality, integrity, and accessibility of information assets.

The Draft Regulation provides further detail on such management and requires the Board to adopt an information system strategy plan, create an information system strategy committee, and an information system direction committee.

Moreover, Banks are required to establish information system policy, procedure, and process documentation that describes the procedures and principles required both to protect information assets and to manage risks arising out of the use of information systems. Notably, at least one member of the bank's board of directors should also be a member of the information system strategy committee.

Electronic Banking Services

The Draft Regulation introduces "electronic banking services" as a chapeau term for internet, mobile, telephone, and ATM banking and open banking services, and sets out common rules for these services.

As did the Communiqué, the Draft Regulation also requires electronic banking services to adopt identity authentication mechanisms that include two components that are independent from each other and to ensure the confidentiality of the data regarding identity authentications. This authentication is based on the use of two elements categorized as "knowledge" (something only the user knows e.g. password or a PIN) and "possession" (something only the user possesses e.g. electronic signatures, fingerprints) for validation of transaction or the user.

Importantly, the onus to prove that the transaction was made by the customer will be on the Bank if the transaction in question was executed without meeting this two-component requirement.

Corporate Cyber Incident Intervention Team

With references to the Communiqué on the Establishment, Duties and Activities of Cyber Incident Intervention Teams, the Draft Regulation also requires Banks to establish a Cyber Incident Intervention Team ("**CIIT**") and notify the BRSA of these teams' contact information.

Before a cyber-incident, the CIIT should regularly conduct leakage tests, track trace recordings, and carry out cyber security awareness events. During a cyber-incident, the CIIT is responsible for managing the intervention carried out by the information system unit and coordinating the unit's personnel. If a cyber-incident turns into a crisis or there exists a leakage or exposure of sensitive or personal data, the corporate CIIT must inform the sectoral CIIT of this development. However, the Draft Regulation does not explain what constitutes a "crisis".

Outsourcing Services

As for outsourcing of a service by the Banks, the Draft Regulation further details the requirements of the Regulation on the Procurement of Support Services by Banks. Particularly, the Draft Regulation sets out the minimum requirements that must be included in an outsourcing agreement, such as definitions regarding the service levels, conditions that would terminate the service, and provisions with respect to measures that the outsourcing company must take so as to prevent the interruption of the bank's information systems. If the outsourcing is in connection with the advertisement services that search engines or social media platforms provide, the agreement should also require the search engine or social media platform to prevent fake advertisements in the name of the Bank and to reimburse damages that may arise due to these fake

advertisements. Importantly, Banks may not outsource their duties regarding the information system internal control and internal audit activities.

A Bank may outsource its duties regarding information systems only if:

(i) The Bank has the controlling role and power to decide on the management, content, design, access, control, audit, update, and right to information and reporting regarding the banking activities and obligations under the banking body of law,

(ii) The Bank is well aware of all the details regarding the management of information systems,

(iii) The Bank itself conducts the internal control activities, such as the establishment of an authorization mechanism that would enable access to the bank's data and databases in accordance with the bank's own authorizations and the review of the authorization of all the applications that the bank utilizes and trace recordings, and

(iv) Except for the intellectual property regarding the particular software, the Bank owns any type of information regarding all the accounts, records, and transactions that arise within the scope of the outsourcing.

Cloud Computing

As an important type of outsourcing, the Draft Regulation explicitly authorizes Banks to utilize cloud computing services, yet impose strict conditions for such use. If the Bank employs cloud computing for services within the scope of primary and secondary systems, the cloud must be established solely for the use of Banks and be in line with the banking legislation.

The Draft Regulation also sets different rules for the use of private cloud service model and community cloud model. If in line with the abovementioned criteria, Banks may freely utilize private cloud service model, which is a model based on software and hardware devoted to a single bank. However, if a bank wishes to use a community cloud model for main banking application, credit and credit card application, and payment services, it must seek the BRSA's approval for such use. Moreover, while the community cloud may physically share hardware and software sources, the model must assign different logical sources for each bank and solely serve for Banks.

Notably, the Draft Regulation does not include a definition for the community cloud model. A useful definition is provided by the European Banking Authority in its Final Report on Recommendations on Cloud Outsourcing that defines community cloud as the "cloud infrastructure available for the exclusive use by a specific community of institutions, including several institutions of a single group"

Data Localization Requirement

The Draft Regulation reiterates the Communiqué's requirement to keep primary and secondary systems within Turkey. The primary systems refer to the entire system consisting of the infrastructure, hardware, software and data that enable the execution of banking activities and the electronic recording and use of the data required for the fulfillment of all the responsibilities, which are defined for the Banks under the Banking Law and the regulations thereof and other related legislations in a way that would provide secure access on demand. The secondary systems refer to the backups of the primary system that ensure that these activities are sustained within the period of acceptable downtime set out in the business continuity plan and that all the data required for the fulfillment of all the responsibilities defined for the Banks under the Banking Law and the regulations related thereto and the other related legislations is accessible without interruption and on demand, in case of an interruption in the activities conducted via the primary systems.

If the Bank employs cloud computing for services within the scope of primary and secondary systems, information systems for such cloud and their back-ups will also have to be kept within Turkey. The same rule applies for any other outsourcing of services.

Aside from banking, payment and texting systems which are, by their nature, established abroad, and banking transactions that necessitates interaction, cross-border data transfer requires the approval of the BRSA, even when the Bank has been granted with the explicit consent of the customer. The Draft Regulation does not

explain whether transferring Banks would also have to seek the approval of the Personal Data Protection Authority if the transferred data includes personal data.

Commentary

The Draft Regulation signifies BRSA's efforts to keep up with new technological developments. However, there is room for improvement. The Draft Regulation lacks definition for some important terms, which should be addressed in the further revisions of the Draft Regulation.

Concurrent Authorities

Article 45 of the Draft Regulation refers to data privacy provision which allows Banks to transfer customer data to third parties on the condition that the explicit consent of the customer is obtained. The term, "explicit consent" is defined under PDLP as "freely given specific and informed consent". The Draft Regulation uses the same definition. Albeit featuring many PDLP references, the Draft Regulation lists the BRSA as the sole authority.

Trace Mechanisms

The retention periods for trace and closed-circuit television (CCTV) records are also crucial in terms of the liability of data controllers (Banks) with regard to the Regulation on Erasure, Destruction and Anonymization of Personal Data which requires data controllers to erase, delete or anonymize personal data in accordance with retention periods designated by law or the purpose of data processing.

Open Banking

It should be noted that new Open Banking provision could be seen as a part of European integration efforts following to introduction of revised the Directive 2015/2366/EU, frequently referred as Payment Services Directive 2 (PSD2)[6], which updates and complements the EU rules put in place by the Payment Services Directive (PSD1), 2007/64/EC.

PSD2 allows payment service providers that do not manage the account of payment service user to issue card-based payment instruments to that account and execute card-based payment systems from that account. As PSD2, the Draft Regulation also introduces enhanced security measures to be implemented by all payment service providers including Banks.

Data Localization Requirement

Importantly, data localization requirement may hinder the Banks' ability to utilize cloud computing as many clouds transfer data from one jurisdiction to another based on available bandwidth. In fact, the BRSA's extended data localization effort comes at a time when the European Union reached a political agreement to allow data to be stored and processed everywhere in the EU without unjustified restrictions so as to "encourage creation of codes of conduct for cloud services".

Conclusion

With numerous committees, units, corporate plans, and trace recording and storing mechanisms, the Draft Regulation foresees a complex system to navigate. Once this Draft Regulation is adopted, all Banks will have to implement its requirements no later than 1 January 2020.

---

6 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

Therefore, the prudent approach would be to start examining the Draft Regulation now and take action as soon as practically possible. In the meantime, trainings by the BRSA or the Banks Association of Turkey regarding the nuts and bolts of the Draft Regulation may allow market participants to have a smoother transition to the requirements of the Draft Regulation.

GKC Partners
Ferko Signature
Büyükdere Cad. No: 175, Kat: 10
Levent 34394
Turkey

T +90 212 355 13 00