

ON A NEW AND COMPLEX REGULATION DIRECTLY RELATING TO BANKS:

What Does the Regulation on Sharing of Secret Information Bring?

Dr. Murat Volkan Dülger*

To determine the scope, form, procedures and principles regarding the sharing and transfer of information in the nature of bank secrets and customer secrets the “Regulation on Sharing of Confidential Information” (“Regulation”) was published in the Official Gazette dated 4 June 2021 and numbered 31501 to enter into force on 1 January 2022. **First of all, what does this mean? Accordingly, everyone within the scope of the Regulation must comply with the provisions of this Regulation as of January 1, 2022!** I will explain below who needs to be compatible with what.

On the other hand, in terms of the close relationship of the issue with the personal data protection legislation, it is extremely important and necessary to consider it together with the data protection legislation in order to determine what obligations the Regulation imposes on whom.

Before that, it is useful to remind a change made a short time ago in order to better understand the Regulation. Because, with the 10th article of the “Law on the Amendment of the Banking Law and Certain Laws” numbered 7222, which was published in the Official Gazette dated February 25, 2020 and numbered 31060, some amendments were made to the Banking Law numbered 5411. However, these changes have been the subject of criticism, especially for their lack of clarity. It is pleasing that the subject has been handled with a Regulation this time, in that it includes more detailed explanations on personal data processing activities carried out in the banking sector. However, it should be noted that the Regulation brings about many new question marks.

Finally, it should be noted that the Regulation was published by the Banking Regulation and Supervision Agency (“BDDK”), and the BDDK is the body responsible for executing the provisions. I will mention some confusions in this respect later on.

In this article, I will try to explain who should do what as a result of the said Regulation. Where it is not clear what to do, I will state my own opinion and suggestion.

* Assoc. Prof. of Criminal Law and IT Law.

I. Some Basic Concepts

In order for the provisions of the regulation to be fully understood, the basic concepts contained herein must be clear and specific. Because, what these concepts mean is needed in order to determine the scope of who should comply with these provisions. At this point, the first criticism should be brought to the fact that some concepts in the Regulation are not directly defined. This situation causes confusion in the understanding of the provisions.

Let's try to clarify some of the basic concepts in the Regulation by reading together with the banking legislation and personal data protection legislation.

1. Customer Secret vs. Bank Secret Distinction

In the Regulation, the concepts of “bank secret” and “customer secret” draw attention first because these concepts are included in the 1st article of the Regulation titled “Purpose and Scope”, but these concepts, which are important enough to explain the purpose of the Regulation, are not explained in the definitions article. However, these concepts are both quite broad and closely related to other legislation. Since the regulation regulates the sharing and transfer of confidential information, these concepts need to be explained in more detail.

In this respect, the first issue to be addressed is about what the word “secret” means. The secret, in general, is an issue that threatens to harm the personal rights of its owner, and it is important both personally and socially to remain confidential, and since it may contain confidential information about any situation, the types and classifications of secrets are quite high.¹ As a matter of fact, there are many regulations in our legislation that deal with the concept of secrecy. From this point of view, the word secret can be defined as “information that is not generally known to everyone and is not possible or likely to be known by everyone in general unless it is disclosed by those who know”.

The concept of customer secret is regulated in the 3rd paragraph of the 4th article of the Regulation as in the 3rd paragraph of the 73rd article of the Banking Law No. 5411 (**“Law No. 5411”**): *“Data belonging to real and legal persons, which are formed after establishing a customer relationship with banks specific to banking activities, become customer secrets”*. In the continuation of the paragraph, we see that the concept of customer secret is explained a little more and “any information showing that a real or legal person

¹ **Hilal Üçüncü**, Medeni Yargılama Hukukunda Kişisel Verilerin ve Sırların Korunması, İstanbul, Onikilevha Yayıncılık, 2019, s. 21 vd.

customer is a customer of the bank” is included in the scope of customer secret. If it is necessary to explain these regulations with an example:

As soon as Bank X establishes a customer relationship with a third party that is a real or legal person Y, all data belonging to person Y is customer secret for Bank X. Any information that serves to show that person Y is a customer of Bank X is also included in the concept of customer secret. In addition, after the customer relationship is established between Bank X and person Y, the information regarding person Y as a result of the transactions made within the framework of this relationship is also within this scope.

However, it should be underlined that the scope of the confidentiality obligation is not limited to the concept of customer confidentiality. I will state the scope of this obligation below.

Another point to note here is that data belonging to legal entities are also included in this concept. Because, in accordance with the regulations introduced by the Law on the Protection of Personal Data No. 6698 (“KVKK”), only the data of real persons are considered within the scope of personal data. The data of legal persons are not within the scope of the concept of personal data and therefore KVKK unless they contain information about the real person.²

As an answer to the question of at what point personal data can come into question, it will be possible to talk about personal data only in cases where there is a customer secret regarding a real person. This means that data belonging to real persons will be subject to the regulations brought by the KVKK in any case, since it will be considered personal data whether or not a customer relationship is established. In that case, customer secret data regarding real person customers will have the character of customer secret as well as being personal data. On the other hand, customer secrets belonging to legal entities are not within the scope of KVKK, but will only be customer secrets and are within the scope of the said Regulation.

On the other hand, another type of secret in the Regulation is bank secret. However, this concept is not directly defined and is more ambiguous compared to customer secret. Before the regulation, there was no consensus on what this concept meant in the doctrine. While a large majority consider bank secrets as a superset that includes legal person and real person data with which no customer relationship has been established, as well as customer secrets and sensitive data, others define bank secrets as information pertaining to the bank’s own internal structure. Although no direct definition has been

² KVKK Rehberi, “Tanımlar”, Erişim Tarihi: 05.06.2021, <https://www.kvkkrehberi.com/tanimlar>

made in the regulation, paragraph 5 of article 5, titled “*Cases exempted from the obligation to keep confidentiality*”, is a bit of a guide. The phrase “*information that is not a customer secret but only a bank secret but contains only the bank's information...*” used here gives the impression that the bank secret contains only the bank’s information. From the general use of the Regulation, I think that bank secrecy refers only to information about the internal structure of the bank. However, this concept needs to be clarified directly rather than just an impression.

2. De-identification, Processing and Aggregation

The concepts of de-identification and aggregation, which are included in Article 3 of the Regulation, titled “Definitions”, are not frequently encountered concepts in Turkish legislation. Let’s look at these concepts and definitions of the concept of processing, which we are more familiar with from the European General Data Protection Regulation (“GDPR”).

a. De-identification

De-identification appears as “Pseudonymisation” in GDPR. This concept was regulated for the first time under the Turkish legislation with the Regulation on Personal Health Data dated 21 June 2019. De-identification, which is a technical term that is encountered for the second time, means that personal data are stripped of their clear identifiers and generalized by means of technologies such as blurring, encryption, key coding and data sharing, and stripping them of their identifiable features.

In the said Regulation, the concept of de-identification is similar to the way it was defined before: customer-related data; it is defined as processing in a way that cannot be associated with the relevant customer, provided that technical and administrative measures are taken so that the real/legal person whose identity is identified or identifiable cannot be associated with the customer and without combining them with other data stored in a different environment.

The related concept is different from anonymization, which is a method frequently used within the scope of KVKK. Although both methods are similar and confused in that they allow their data, such as name, address or card number, to be masked by means of removal or encryption. The difference between the two is that de-identification is recyclable. In the de-identification method, when it is necessary to re-attribute the data to the person, thanks to a separate information such as the encryption key, this information can be converted and the

data that makes the person identifiable can be accessed again.³ This method offers a temporary solution rather than placing the data in the category of non-personal data. As a matter of fact, as we can understand from Recital No. 26, re-identification is possible even after this method, thanks to developing technologies. Therefore, de-identified personal data remains as personal data under GDPR.⁴

As a matter of fact, when we look at the definition of the Regulation given above, the obligation to take technical and administrative measures draws attention. This obligation is in the nature of a precaution against the possibility of re-identification, in line with the EU's obligation to take technical measures for data processors.

A problem that may arise in the definition of regulation is that the definition is limited to the concept of customer. Based on such a limitation, the question arises whether de-identification is required when it comes to sharing the data of people who are not yet customers.

b. Data Processing

Another concept covered in the definitions article is data processing. In the aforementioned article, this concept is similar to the definition of processing personal data in article 3 of the KVKK. It is defined as *"any kind of operation performed on data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, sharing, transferring, taking over, making available, classifying or preventing its use"*.

However, it is not specified as a contradictory to KVKK that data processing would take place according to the ways in which these transactions are carried out on the data, because personal data will be processed only if the activities mentioned in the definition given above in the KVKK are carried out *"fully or partially automatically or by non-automatic means provided that they are part of any data recording system"*. In order to be able to talk about data processing within the scope of the regulation, there is no such obligation as understood from the definition. On the other hand, it is seen that all kinds of data processing are included in the confidentiality obligation with the second paragraph of Article 4 of the Regulation. Therefore, since there is no restriction, it is understood that the realization of the activities in the definition by all means is considered as data processing within the framework of the Regulation.

³ Termsfeed, Pseudonymization, Anonymization and the GDPR, Eriřim Tarihi: 05.06.2021, <https://www.termsfeed.com/blog/gdpr-pseudonymization-anonymization/>

⁴ ICO, What is personal data?, Eriřim Tarihi: 05.06.2021, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/>

Considering that the concepts of data recording system and partially automatic ways, which are controversial within the scope of KVKK, are not included in the relevant Regulation and that all transactions carried out on the data, regardless of the means, are included in the scope of confidentiality obligation, it would not be wrong to say that the concept of data processing is handled more broadly by the Regulation, and therefore, in this respect, a more protective attitude is displayed than the approach of KVKK to personal data.

c. Aggregation

The concept of aggregation, which is also included in the definitions article of the Regulation and which we have not encountered before, is defined as *“processing of customer-related data in such a way that it cannot be associated with an identified or identifiable natural/legal person customer by combining it with data on other customers for statistical purposes such as grouping, summarizing, and collective display”*. In cases where it is possible to apply the aggregation method in accordance with the regulation, this method should be preferred.

Although this concept is similar to anonymization, it differs from it in some ways. For one thing, the subject of aggregation is not personal data, but “customer-related data”. I explained the differences above. On the other hand, while it is possible for personal data to be data that determines or can identify a real person, data regarding both real and legal persons are counted among the customer data that will be the subject of aggregation. Therefore, it is aimed to avoid conceptual confusion by using the concept of aggregation regarding customer data as a counterpart to the concept of anonymization regarding personal data. I must state that this is an appropriate way of thinking and method.

II. Obligation of Confidentiality

The regulation mainly relates to the obligation to keep secrets. Some basic concepts are explained above. These explanations were about what to hide. Now let’s look at how and in what ways it should be stored.

1. What is the Obligation of Confidentiality?

The main rule regarding the confidentiality obligation is stated in Article 4 of the Regulation, titled *“Confidentiality Obligation”*, by repeating Article 73 of the Law No. 5411. Accordingly, in accordance with the confidentiality obligation, *“those who learn the secrets of banks or their customers due to their qualifications and duties cannot disclose such secrets to anyone other than the authorities expressly authorized by law in this regard”*.

In addition, this obligation will continue after leaving office.

2. Scope of Confidentiality Obligation Pursuant to the Regulation

In the continuation of Article 4 of the Regulation, there are explanations regarding the scope of confidentiality obligation.

Firstly, as mentioned above, the Regulation did not limit the data processing activity in terms of the methods used. Because no related expression was used in the definition of the concept against KVKK. In the definition of personal data processing in the KVKK, there is an extra expression of *“Personal data is fully or partially automated or by non-automatic means provided that it is a part of any data recording system”* compared to the Regulation. The fact that this phrase is not included in the Regulation suggests that it does not matter in which ways the operations performed on the data are carried out in order to carry out data processing activities in accordance with the Regulation.

As a matter of fact, in article 4/2 of the Regulation, the obligation to keep confidential is regulated in such a way that the information that is in the nature of customer secret is obtained and learned by non-automatic or non-automatic methods. **What does this mean? Even a bank’s writing of customer secret information on an ordinary piece of paper is a transaction within the scope of the Regulation and is subject to confidentiality obligation.** Therefore, it should be noted that the scope of the obligation is regulated quite broadly in this respect.

In the article 4/3 of the regulation, the status of the data regarding the persons with whom no customer relationship has been established is regulated: *“Even if a customer relationship has not been established, obtaining and learning the customer secret information held by another bank is also subject to the obligation within the scope of the first paragraph.”*

For another bank, the situation of information that is not a customer secret is stated in Article 4/3 of the Regulation: “including personal data, data relating to real and legal persons, which existed before the establishment of a customer relationship with banks and which do not qualify as a customer secret of another bank, are not classified as confidential on their own, it becomes a customer secret when it is processed alone or together with the data formed after the establishment of the customer relationship specified in the third paragraph, showing that the person concerned is a bank customer.”

In the light of the explanations, let’s examine the determination of the customer secret and the scope of the confidentiality obligation through an example:

Sample: Bank A has established a bank-customer relationship with Joint Stock Company B as of now. The natural person C is the customer of Bank D. Bank E, on the other

hand, is in talks with Joint Stock Company F, but is currently a client of Bank A. Real person G does not have the title of customer before any bank.

Accordingly, the state of being included in the following concrete examples of customers being secret or confidentiality obligations are as follows:

Status	Customer Secret	Confidentiality Obligation
Data belonging to Corporation B for Bank A	✓	✓
Data of natural person C for Bank D	✓	✓
Data belonging to Corporation F for Bank D	×	✓
Data belonging to Corporation F for Bank A	✓	✓
Data obtained after establishing a customer relationship between Bank A and Joint Stock Company B	✓	✓
Any information showing that natural person C is a customer of Bank D	✓	✓
Data of natural person C for Bank A	×	✓
Data of natural person G for Bank A, D and E	×	×

If some of the pre-existing data of natural person G are used together with the data that emerged after the customer relationship with Bank A, the pre-existing data will be used for Bank A.	✓	✓
If some of the pre-existing data of natural person G are used together with the data that emerged after the customer relationship was established with Bank A, the pre-existing data is for Banks D and E	×	✓

3. Exceptions to the Obligation of Confidentiality

In Article 5 of the Regulation, the exceptions to this obligation are dealt with in a clear, systematic and broad way.

First of all, in accordance with Article 5/1, sharing the information in the nature of bank secret or customer secret with the authorities expressly authorized by law will not constitute a violation of the confidentiality obligation.

Provided that a confidentiality agreement is made pursuant to Article 5/2 and only for the stated purposes, the sharing of bank secrets or customer secrets within the scope of the situations listed in the aforementioned paragraph shall not constitute a breach of the confidentiality obligation. Among the situations that will not constitute a violation of the confidentiality obligation; banks and financial institutions exchange all kinds of information and documents directly among themselves or through companies to be established by the Risk Center or at least five banks or financial institutions, preparation of consolidated financial statements, risk management and internal audit practices, valuation studies to be carried out for the purpose of selling shares representing 10% or more of the bank's capital also include providing information and documents.

I do not think it is necessary to explain all of the exceptions in the Regulation here one by one. Because the concept of customer secret is clearly defined in the Regulation and the processing activity is regulated in a way that covers all kinds of processing, it is quite appropriate that the exceptions to the said obligation are regulated in a wide manner. Otherwise, a result that exceeds its purpose and cannot be applied in practice will emerge, which is an extremely dangerous situation for legal regulations. Moreover, it should be underlined that banks are already subject to KVKK and other banking legislation, and now they are also subject to the said Regulation. Therefore, customer secrecy and other obligations are still valid for banks, most importantly, there is no exception in terms of being subject to Article 6, which I will specify below, therefore, I must say that I find such a wide and detailed regulation of the exceptions to the obligation of secrecy appropriate in terms of making the banking and finance sector work while keeping secrets.

III. General Principles Regarding Sharing Confidential Information

Article 6 of the Regulation, titled “*General principles regarding the sharing of confidential information*”, regulates the rules to be followed while sharing this information. When the regulations in the article are examined, it is seen that they are in compliance with the principles stated in the KVKK.

I. The Principle of Proportionality

Although the concept of proportionality is a controversial concept, the principle of proportionality has been explained within the scope of the Regulation. Accordingly, it should be understood from this principle that the realization of the stated purpose cannot be achieved without some of the shared data.

In the relevant article, the minimum elements required to be satisfied that the principle of proportionality exists are specified:

- i. If it is related to the stated purposes, the shares contain only as much data as required by the said purposes
- ii. It can be demonstrated that all of the data or data sets contained in the shares are necessary for the realization of the stated purposes,
- iii. Application of these methods if the aforementioned purposes can still be achieved when the data to be shared is aggregated, de-identified or anonymized,
- iv. If the customer whose information will be shared is not also a common customer of the parent, controlling partner or group company, the confidential information regarding the real/legal person customer to be shared with these parties is not of

a nature to make the identity of the said customer specific or identifiable, and the above-mentioned methods are used,

- v. Designing the parties to be shared and the sharing methods in a way that creates the least possible data copy.

However, in order to talk about the existence of this principle, which is defined in detail in the regulation, it is necessary to check that all the above-mentioned conditions are met. Due to the necessity of applying the principle of proportionality, this audit, which must be done, may cause a functional problem in terms of banks' business processes.

II. Sharing Data on Real Person Customers

The article 6/2 of the Regulation regulates the sharing of confidential information regarding real person customers. During this sharing, it was stated that it was necessary to act in accordance with Article 4 of the KVKK. Since banks are subject to KVKK in any case, it is appropriate not to create a conflicting situation in this regard and to act in harmony by referring to the KVKK.

III. Customer's Active Request or Instruction

Article 6/3 of the Regulation regulates the customer's request or instruction for information sharing. In Article 73/3 of the Law No. 5411 with the amendment dated February 25, 2020 mentioned above, the phrase "even if explicit consent is obtained" added to the paragraph has been subjected to many criticisms by us, such as the fact that explicit consent is dysfunctional and the concept of explicit consent loses its credibility in the eyes of the legislator. The main reason for these criticisms is that a separate request or instruction is expected from the customer despite the existence of explicit consent. Accordingly, even if the customer has given explicit consent for the sharing, it is not possible to realize the transfer without forwarding the request and instruction to the relevant bank. With article 6/3 of the Regulation, this situation has been preserved, only the cases that are exempted from the confidentiality obligation are excluded.

On the other hand, in the aforementioned paragraph, with the statement that "*the customer's explicit consent to sharing his information or giving a request or instruction cannot be made a prerequisite for the services to be provided by the bank*", the binding of the explicit consent to the service condition in accordance with the KVKK has been prevented.

Another point to be mentioned here is about the distinction between a natural person and a legal person. Because in accordance with the article 6/3 of the Regulation, explicit consent and customer request or instruction are kept separate from each other. In this case,

one of the questions that comes to mind is whether explicit consent within the scope of KVKK is applied to real persons, while only customer requests and instructions will be sufficient for legal persons, since they are not within the scope of KVKK. If there is a relevant situation for legal entities, it emerges that both the explicit consent and the conditions of the request and instruction must be met when it comes to transferring data belonging to real persons. However, in this case, what will be the conditions for the explicit consent to be obtained from legal persons and how will they be determined? Although these issues remain unclear within the scope of the Regulation, the reason for the existence of this problem is that, in our opinion, instead of making regulations based on the main principles in the Law on the Protection of Personal Data, the BDDK – rightfully – handles and regulates the issue only in terms of the banking and finance sector. This creates these contradictions and accordingly, many problems arise in practice. However, the expectation of those affected by such regulations and the implementers is that such regulatory agencies come together and take into account all sensitivities and make regulations that will not cause contradictions, ambiguity or confusion.

The regulation on the form of the customer’s request or instruction is in Article 6/4 of the Regulation. Accordingly, the request or instruction;

- can be obtained in written form or, provided that it is provable, it can also be obtained through permanent data storage. Permanent data storage is explained as follows in the definitions article: Recording the information sent by the customer or sent to him in a way that allows for a reasonable period of review in accordance with the purpose of this information and any means or medium, such as text message, e-mail, internet, CD, DVD, memory card and similar, that allows copying without modification and allowing access to this information exactly. It is appropriate that an alternative method has been introduced in this way in accordance with electronic media as well as written.
- Provided that it can be canceled or changed at any time by the customer using the same methods as the request or order, it may cover more than one transaction, and the request or instruction for continuous transactions may be indefinite. At this point, the question arises, if a request or instruction is to be received by the bank for only one transaction, whether it should be canceled or changed by the customer. It is not mandatory that the request or order received for a transaction contrary to the arrangement be canceled and changed.
- It is essential that the customer can be inquired and viewed through distribution channels for electronic banking services.

Paragraph 6 of Article 6 of the Regulation is also an arrangement that includes the active request or instruction of the customer. Accordingly, it has been stated that initiating the relevant transaction by the customer or entering an order by the customer through the distribution channels for electronic banking services will replace the customer's request or instruction in terms of transactions where it is obligatory to share customer secret information. In this way, in addition to the explicit consent pursuant to the KVKK, the active demand requirement for data sharing within the scope of the Regulation is fulfilled without deteriorating the user experience through transactions and order entry means initiated by the customer by adapting to the digital world.

IV. Data Transfer Abroad

Under article 6/11 of the Regulation, the issue of transfer abroad is discussed. The BDDK is authorized to prohibit the sharing of all kinds of data, which are customer or bank secrets, with third parties abroad. This authorization has brought the BDDK to the agenda in addition to the Personal Data Protection Board regarding the transfer of personal data. Here, when it comes to sharing and transferring personal data of bank customers, it remains unclear which institution will be authorized.

However, the principle of reciprocity is based on the sharing to be made pursuant to the provision of the same article. Therefore, when sharing is made with parties in a country that does not comply with the principle of reciprocity, the Board may restrict, stop or prohibit such sharing. When all these regulations are taken into account, it would not be wrong to say that the scope of these powers given to the BDDK regarding overseas transfer is quite wide. As a matter of fact, it should be noted that the Board, as well as being authorized to prohibit, is also authorized to supervise whether the principle of reciprocity required for overseas transfers is complied with. In terms of KVKK, transferring of personal data abroad is still one of the most uncertain and controversial points of this subject; I should also state that I do not find it appropriate to introduce such a regulation on it. The authority to determine the principles and procedures for the transfer of personal data abroad has been given to the Personal Data Protection Board ("KVK Board"), and many regulations and explanations have been published, including the criteria to be taken into account, on the subject of the KVK Board. Despite this, the issue of transfer abroad still remains unclear and poses a major problem in terms of implementation. On the one hand, while there is a desire for the issue to be resolved in the most applicable way, as soon as possible by all the practitioners of the issue, it would not be appropriate to leave a new regulation on the issue, authorize a new institution, set a criterion, cause an inquiry as to what the criteria previously determined by

the KVK Board would be. Therefore, I foresee that this regulation will complicate the issue, especially in terms of the authorized institution, rather than providing benefits.

V. Information Sharing Committee

In accordance with Article 7 of the Regulation, titled “Information Sharing Committee”, banks are obliged to establish an Information Sharing Committee. The responsibility of this committee is as follows; coordinating the sharing of customer secret and bank secret information, including the shares within the scope of Article 5 of the Regulation, taking into account the principle of proportionality mentioned in Article 6, and recording these evaluations by evaluating the appropriateness of the sharing requests.

Since banks are institutions that process and transfer personal data intensively, it is important that they establish committees in compliance projects with KVKK. With this new regulation, it will be beneficial for banks to benefit from the members of the KVKK committee in the formation of the information sharing committees, to choose among these members and to establish a structure in which these two committees work in cooperation.

Conclusion

In the light of all the explanations made above regarding the said Regulation, I must state that there is a Regulation that needs to be published in general and that I find it appropriate that this regulation has been made. However, I still consider it as a major deficiency and negativity that some of the concepts I have mentioned above are either not defined at all or are not adequately defined, and that different regulatory institutions that touch the same issue by providing coordination between institutions do not issue a common legislation.

Within the scope of the amendment made in February and the relevant regulation, an administrative (semi-autonomous) institution such as the BDDK was authorized for its own sector. As it is known, in our developing and changing world, information technologies are also developing day by day. It is possible that such authorizations will be granted to many more sectors in the future. However, it is unclear how the regulations will affect each other. Therefore, it will be difficult to determine who is responsible for legal problems that may arise due to this sectoral recognized authority. Due to the aforementioned ambiguous situation, the BDDK’s publication of a guide on how and in what ways the regulations in the Regulation should be applied in the future, in order to avoid problems for banks in practice, and containing concrete examples regarding the obligations brought under the regulation, will make a positive contribution to the solution of possible problems.

On the other hand, the Regulation brings with it many problems regarding international transfer. Because, in the transfer of customer secret information, the provisions on keeping secrets after the amendment made in the Law No. 7222 and the Banking Law No. 5411, as it is a special and subsequent law, will be considered as special legal provisions against the KVKK. As a matter of fact, the Regulation, which is the subject of this article, was issued in accordance with this amendment. This means that even if explicit consent is obtained in the transfer of customer secret data to third parties, requests and instructions from customers will also be required. The fact that the request and instruction of the customer is deemed necessary almost disregards the concept of explicit consent, which is considered within the scope of KVKK.

Finally, although there is no harm in making sector-specific regulations, it should be noted that these regulations should not harm the principle of unity of law. Otherwise, it will face the danger of undermining the security of law. In addition, if the holistic protection approach is not taken as a basis in future sector-based regulations, it will be inevitable to encounter many more problems in practice.