2021

LAW ALMANAC

SRP | legal

strategy regulation policy


SRP
legal
strategy regulation policy

@srplegal

SRP | legal

strategy regulation policy

TABLE OF CONTENTS

Dear Clients and Contacts,

During these times, everyone's common reproach is that time is passing by so rapidly and the desparation of not being able to stop it. Is time slipping away or are we just struggling to keep up with developments, since everything around us has been unfolding before us in such a fast pace? Undoubtedly, the ones that manage time effectively are the winners. In other words, while it is impossible to stop the passage of time, we can always follow and be aware of the changes and developments that are racing against the sands of time.

An almanac, defined as a yearbook in the dictionary, is a calendar compilation published as a book which includes a record of events which happened within a year. To rephrase it, an almanac is a journal that paints a picture of the events from the past year. As we are unable to control time's arrow, so it is best we focus on the fact that we are able to observe the historical course of previous developments that we have been aware of, but have forgotten, or those which we were never aware of in the first place. This inevitably provides us with an opportunity to absorb at a future date, the time we have already consumed.

In line with this objective, we are proud and pleased to share our "**2021 SRP-Legal Almanac**" for the first time, compiling all innovations and legislative amendments in the field of technology, recent developments in different fields of law such as payment services and competition law, and moreover, the effects of COVID-19 on administrative and legal mechanisms, which took hold of us in the year 2021, so as to enable you to digest the past year which went by in the blink of an eye.

We wish the 2021 SRP-Legal Almanac, which we prepared as to provide you with a handbook that includes subjects you may desire to look back at, will generate a useful resource that gives you the opportunity to follow the developments that emerged in the past year on a monthly basis, regarding the above-stated fields.

Att. Dr. Cigdem Ayozger Ongun, PhD, LL.M. | SRP-Legal Founder and Managing Partner

Please read the QR code
for our Founder and Managing Partner
Att. Dr. Cigdem Ayozger Ongun's video
message about the almanac.

January

01 **Personal Data Protection Board Announced Its Decision Regarding a Bank's Failure to Act in Compliance with the Given Instructions.**

02 **The Personal Data Protection Board Rendered a Principle Decision Regarding Unlawful Transfer of Data Subjects' Personal Data to Third Parties by the Data Controller, Contrary to Personal Data Protection Law Numbered 6698.**

03 **The European Union is in an Attempt to Reshape the Rules of the Internet!**

04 **Instant and Continuous Transfer of Funds (ICTF) System Brought into Service for Citizens!**

01 - Personal Data Protection Board Announced Its Decision Regarding a Bank's Failure to Act in Compliance with the Given Instructions

As a result of the complaint of the data subject complainant, regarding the data controller Bank (**"Data Controller"**) who did not fulfil its obligation to inform in accordance with Article 11 of the Personal Data Protection Law numbered 6698 (**"PDP Law"**), the Personal Data Protection Board (**"Board"**) rendered a decision dated 08.10.2020 and numbered 2020/766 ("Decision Dated 08.10.2020") regarding the Bank's failure to comply with the previous Board Decision dated 06.02.2020 and numbered 2020/98 (**"Decision Dated 06.02.2020"**), which required the correction of the deficiencies in the Bank's privacy notice.

In its Decision Dated 06.02.2020, the Board has stated the lack of compliance of the privacy notice on the Data Controller's website with the relevant provisions of the Communiqué on Principles and Procedures to be Followed in Fulfillment of the Obligation to Inform (**"Communiqué"**) due to the facts that the personal data processing conditions stipulated by the PDP Law are not clearly manifested and an impression is created where different purposes of personal data processing may occur, that the privacy policy published in the website of the Data Controller cannot be regarded as the act of informing, that the obligation to inform should be fulfilled during the collection of the personal data and as activity-based; and served an instructive notice to the Data Controller requiring the necessary arrangements to be made regarding the aforesaid statements.

Upon examination of the information and documents provided by the Data Controller Bank following the Decision Dated 06.02.2020, the Board determined that;

- A privacy notice was prepared by the Data Controller following the serving of the Board, such privacy notice included which personal data is processed in a categoric and detailed manner, and plain and clear

which legal grounds, to which legal and real persons, and the retention and processing periods of such personal data,

- However, such privacy notice, instead of informing on the personal data processing conditions such processing is based on, included only the relevant paragraphs and sub-clauses of Articles 5 and 6 of the PDP Law as contrary to the Communique,
- Regarding the different activities carried out by the Data Controller, even though a specific privacy notice is used for credit card applications, such privacy notice does not contain the personal data (categorically) processed, the purposes of the processing, the legal grounds of the processing and other elements specific to activities in detail, and it is not prepared in accordance with the Communiqué; and for the real estate loan service, the general privacy notice of the Bank is used instead of an activity-specific privacy notice.

Following the preceding assessments, the Board is convinced that the Data Controller acted in violation of the sub-clause 5 of Article 15 of the PDP Law for the reasons that the Data Controller did not prepare its privacy notice in accordance with the Communiqué and did not follow the instructions within the Decision Dated 06.02.2020, and decided to enforce an administrative fine of TRY 120.000 on the Data Controller.

02 - The Personal Data Protection Board Rendered a Principle Decision Regarding Unlawful Transfer of Data Subjects' Personal Data to Third Parties by the Data Controller, Contrary to Personal Data Protection Law Numbered 6698

The Personal Data Protection Board (**"Board"**), in its Principle Decision dated 22.12.2020 and numbered 2020/966 (**"Principle Decision"**), envisaged that the data controllers should establish mechanisms enabling them to confirm the contact information of the data subjects in order to prevent the personal data of the data subjects from being sent to third parties through communication channels such as mobile phone or e-mail, as contrary to Articles 4 and 12 of the Personal Data Protection Law numbered 6698 (**"PDP Law"**).

The Board determined that the data controllers who operate in the sectors such as e-commerce, telecommunication, transportation, and tourism, in order to provide documents containing personal data such as invoices, statements, reservation documents to the data subjects within their scope of activities, and as a result of such data subjects' incorrect telephone and e-mail statements, send such documents containing data subjects' personal data to third parties instead. However, as per the Principle Decision, in accordance

with the Article 4 of the PDP Law, data controllers have an active duty of care to maintain the personal data accurate and up-to-date while processing of the same, provided that such personal data constitutes and generates a result regarding the data subject. Besides, it is of importance that the data controllers keep the channels open to ensure for data subjects to provide accurate and up-to-date information where necessary.

Within this frame, the data controllers should take reasonable measures (sending verification codes/links to the phone numbers and/or e-mails etc.) to confirm the contact details of the data subjects in order to

- Determine the source from where the personal data is obtained,
- Determine the accuracy of the source from where the personal data is collected,
- Prevent the negative consequences that the data subjects may encounter due to their personal data being incorrect.

The Board also underlined in this Principle Decision that data controllers are obliged to take all necessary technical and administrative measures in order to ensure the appropriate level of security to prevent unlawful processing of and unlawful access to the personal data, and for maintenance of the personal data in accordance with Article 12 of the PDP Law.

03 - AThe European Union Is in an Attempt to Reshape the Rules of the Internet!

On 15.12.2020, the European Commission (“**Commission**”) submitted the proposal of the drafts of the Digital Services Act (“**DSA**”) and the Digital Markets Act (“**DMA**”).

More specific and additional obligations are imposed on very large online platforms with the DSA. In accordance with the regulations within the scope of the DSA, all online intermediaries offering their services in the single market, regardless of whether they are in the European Union (“**EU**”), are obliged to comply with the new rules. The DSA also imposes clear obligations on internet operators regarding user complaints against illegal acts.

Within the scope of the DMA, the aim is to adapt the competition rules into the digital sector. The DMA prohibits EU Member States from enforcing their own laws or regulations on “gatekeeper” platforms that go beyond the DMA. The draft introduces the concept of “Gatekeeper”. Gatekeeper and their platforms can be defined as: “Very large organizations that control “core services” such as search engines, social network services, certain messaging services, operating systems, and online brokerage services. technology companies…”. These companies are appointed by the decision of the Commission and this appointment imposes a set of behavioral obligations for the appointed online service provider. Both proposals shall be directly implemented across the EU if adopted.

Some important issues regulated under the DSA are as follows:

- Regardless of the category of service offered, it is a common obligation for all service providers to provide a transparent and secure online environment.
- It is a common obligation for all service providers to comply with the decision to remove the content due to illegal content given by the courts of Member States or Authorities.
- Service providers that do not have an establishment in the EU are required to appoint a legal representative, in one of the Member States.
- Liability for exemption and conditions for exemption have been determined.
- General monitoring or active information collecting obligations for online intermediary service providers shall be no longer prohibited, and online intermediary service providers shall act against illegal content.

- Within the scope of user complaints, an obligation to take immediate action upon complaints has been imposed. (Notice and Action system)
- Regarding online advertising, transparency obligations have been regulated for online platforms.
- Additional obligations are placed on "very large online platforms" to manage systemic risks.

Some important issues regulated under the DMA are as follows:

- Provided that it does not affect the operability of the respective operating system or device, if users wish to uninstall the applications that have originally come with their devices, such uninstallation will be permitted.
- Gatekeepers shall be prohibited from competing with the business users using the data collected from business users.
- The DMA prohibits gatekeepers from imposing the obligation to become a member in order to use services other than the main platform service regarding business users and end users.
- Gatekeepers shall be prohibited from restricting users' access to services acquired outside of the gatekeeper platform.
- Gatekeepers shall not prevent access to third-party application stores that compete with their own applications. However, gatekeepers shall limit the ability of these applications to interfere with "the integrity of the hardware or operating system.".
- Gatekeepers shall observe a fair and non-discriminatory method among users when accepting business users into the application store.
- Gatekeepers shall be prohibited from mixing the data they collect from their customers with data from data brokers or business users. Gatekeepers shall also be prohibited from directly (without pre-approval) registering users in additional services.

Penalty:

- The penalties shall be determined by the Member States so as not to exceed 6% of the global turnover in the case of the DSA and 10% of the global turnover in the case of the DMA.
- In terms of violations of secondary obligations such as not responding to the information and document requests of the Commission in due time, providing incorrect and misleading information, or not meeting

the database access requests of the Commission as it should be, undertakings may be fined not exceeding 1% of their annual turnover.

- The Commission reserves the right to impose fines on very large online platforms apart from the regulations of the member states, up to 6% of their turnover.
- If a violation decision is issued about a gatekeeper's company three times by the Commission, it will be considered as a systematic violation and behavioral and structural measures may be taken.

04 - Instant and Continuous Transfer of Funds (ICTF) System Brought into Service for Citizens!

On 08.01.2021, Central Bank of Turkey ("**CBT**") made a press announcement regarding the new generation 24/7 instant retail payment application, Instant and Continuous Transfer of Funds ("**ICTF**") system. The system has been proceeded as of 08.01.2021.

With the ICTF System, the Easy Addressing System that allows electronic payment systems to be used in a practical and easy way through using Turkish Republic Identity Number, telephone number and e-mail address has also been opened to use.

Although a 50 Turkish Liras ("**TL**") limit has been initially set in the system, the limit will gradually increase up to a 1000 TL limit.

Unlike EFT, the greatest convenience brought by the ICTF system is that the process can be completed every hour of the day and every day of the week in a maximum of 25 seconds, and a notification shall be sent to the receiver and the sender. It is stated that if the process takes longer than the specified period, the process shall be canceled.

The system does not apply only to person-to-person transfers but may also be used for commercial payments. With the ICTF system, transactions may also be made with the Easy Address defined by the customer besides the IBAN number.

The transactions to be made using the system in question shall be made from the ICTF section of the mobile or internet branches of banks or payment institutions.

ICTF may only be used for TL transfers and may only be performed through drawing account transactions. If the transfer does not meet the criteria, the transaction shall not be canceled but shall be regarded as a normal EFT.

February

01 COVID-19 Deferred Tax Payments in Certain Sectors.

02 Certain Loan Debts of Tradesmen and Artisans Who are Aggrieved Due to COVID-19.

03 Constitutional Court Decision Regarding Corporate E-mail Account Examined by the Employer is Published.

04 The Commercial Advertising and Unfair Commercial Practices Regulatio is Amended.

05 Personal Data Protection Board Announced Its Decision numbered 2020/905 Regarding the Personal Data Breach Notification by an Insurance Company.

06 Personal Data Protection Board Rendered a Decision numbered 2020/787 on the Data Breach Notification of a Company Operating in the Healthcare Sector.

01 - COVID-19 Deferred Tax Payments in Certain Sectors

COVID-19 continues to lead to changes and setbacks in numerous issues worldwide and in our country. Many measures have been taken to address these setbacks. Additionally, regulation amendments have been introduced. Measures have also been taken in order to protect taxpayers within the scope of the policies taken against the pandemic. Many regulations have been introduced to provide taxpayers with various opportunities. The regulations regarding deferral of the tax payments are as follows:

1 - General Communiqué on Tax Procedural Law

The General Communiqué on Tax Procedural Law (**"Communiqué"**) was published in the Official Gazette dated 25.01.2021 and numbered 31375. In accordance with the Communiqué, the measures taken by the Ministry of Internal Affairs (**"Ministry"**) regarding tax deferral are as follows:

- Taxpayers in the sectors that temporarily ceased their activities or whose activities have been terminated completely, shall benefit from the "force majeure" provisions stipulated under the Tax Procedural Law No. 213.
- Taxpayers that carry out their commercial activities in movie theatres, coffee houses country gardens, internet cafes, electronic game saloons, billiard halls, clubhouses, tea gardens, swimming pool facilities,

Turkish baths, saunas, amusement parks shall be regarded as in a force majeure situation as of December 1, 2020.

- Regarding the taxpayers who are subject to the force majeure provisions;

The submission periods have been extended until the end of the 26th day of the month following the expiration of the force majeure and the payment periods of the taxes accrued on the basis of these declarations have been extended from the month following the month in which the declaration should be submitted, starting from the first period for which the declaration submission period was extended, to the end of the following month respectively for each period, for the documents mentioned below:

- Withholding Declarations (including Withholding and Premium Service Declarations) and Value Added Tax Declarations and "Form BA-BS" notifications and e-Books that must be prepared and signed within the said period and whose legal period corresponds to the force majeure period;
- The payment of the "Electronic Ledger Certificates" and e-Ledgers and secondary copies of the related certificate files, which must be uploaded to the Revenue Administration Information Technology System within the same period.
- Force majeure provisions will be applicable for the deferral of the declaration and payment periods regarding the tax deductions of declarations in the case that it is compulsory to notify the information on earnings based on prime value and services related to the force majeure period in accordance with the Social Security Legislation through the Withholding and Premium Service Declaration.

2 - Deferral of Accommodation Tax

In accordance with Article 42 of the Law on Restructuring Certain Receivables and Amending Some Laws dated 11.11.2020 and numbered 7256, the effective date of the accommodation tax which was set as 01.01.2021 has been amended as 01.01.2022.

In conclusion, the current periods regarding the deferral possibilities granted to taxpayers within the scope of the taken measures have been explained above. With the Communiqué, deferral provisions regarding the sectors subject to force majeure have been regulated. In addition, the repayments of the restructured debts stipulated under the Law No. 7256 on Restructuring Some Receivables and Amending Some Laws have commenced as of January, 2021.

02 - Certain Loan Debts of Tradesmen and Artisans Who Are Aggrieved Due to COVID-19

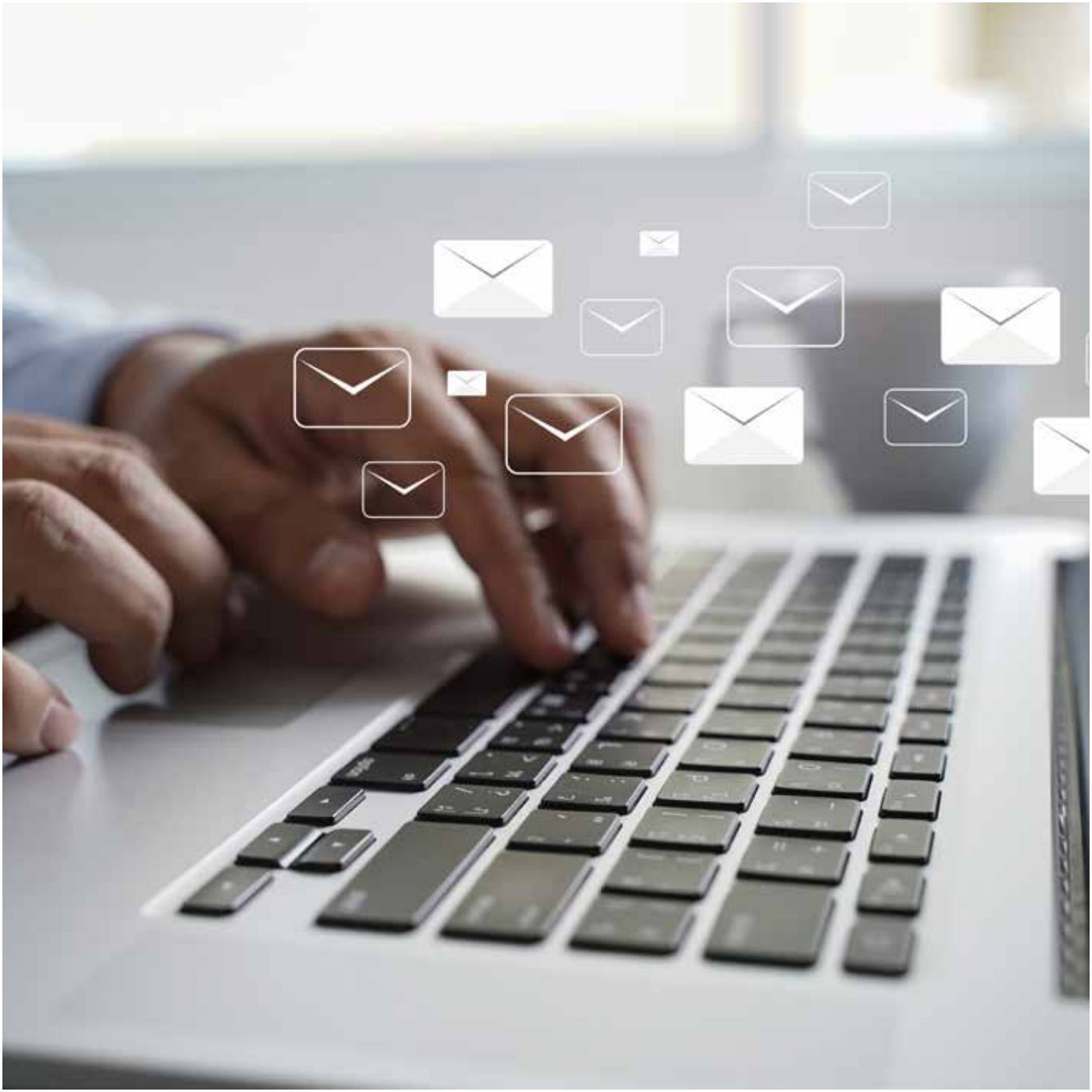
The Presidential Decree (“**Decree**”) published in the Official Gazette dated 04.02.2021 and numbered 31385 regulates the procedures and principles regarding the deferral of debts arising from low-interest loans used with the guarantee of Tradesmen and Craftsmen Credit and Guarantee Cooperatives (“**TCCGC**”) or directly from HalkBank, by the tradesmen and craftsmen whose businesses are economically damaged due to COVID-19 and who are operating throughout Turkey under the Turkey Tradesmen and Craftsmen Credit and Guarantee Cooperatives Central Union. The aforementioned decision entered into force on the date of publication, effective as of 01.01.2021. The provisions regulated by the Presidential Decree are as follows:

1 - Deferral of Credit Debts

Debts arising from low-interest loans used by tradesmen and craftsmen with the guarantee of TCCGC or directly from Türkiye Halk Bankası on 31.12.2020 or a prior date, and those that cannot be collected on Due Date/Partial Payment Due Date/Fiscal Period and which are not yet included in the scope of receivables to be liquidated and those that will become due between the dates of 01.01.2021 and 30.06.2021 and are not redeemed as of 04.02.2021 effective from 01.01.2021, shall be deferred to and spread through the remaining due date referred to in the loan redemption table, without any changes in the number of installments determined in the starting of the Due Date/Partial Payment Due Date/Fiscal Period by accruing interest in accordance with the relevant legislation in the Due Date/Partial Payment Due Date/Fiscal Period without requiring an application.
During the deferral period, the portion of the installment/principal debt and the interest to be accrued on the tradesmen and craftsmen in accordance with the relevant decisions and the related bank and insurance transactions tax shall be added equally to the remaining installments.

Tradesmen and craftsmen shall undertake that they will not reduce their number of employees during the deferral period. Otherwise, they shall be excluded from the scope of the deferral provisions.

The revenue losses calculated during the deferral period will continue to be paid by the Ministry of Treasury and Finance. Enforcement proceedings shall not be initiated for the deferred loans from 04.02.2021 until the end of the deferral period. Within the scope of the relevant decisions regarding the use of low-interest loans on demand, Türkiye Halk Bankası may open a low-interest loan within the deferral period upon request and the provisions preventing the opening of loans shall not be applied.



03 - Constitutional Court Decision Regarding Corporate E-mail Account Examined by the Employer is Published

With the Constitutional Court Decision ("**Decision**") dated 12.01.2021 and numbered 2018/31036 and published in the Official Gazette dated 05.02.2021 and numbered 31386, the allegations regarding the violation of the right to demand the protection of personal data and freedom of communication within the scope of respect for private life, were decided upon. The case manifested itself in the form of the termination of the employment contract by the employer of the applicant working in a private bank, due to his correspondence via corporate e-mail investigated by the employer.

1 - Events and Facts

In the employment contract signed between the applicant and the employer, there are provisions stating that the e-mail address may only be used for business purposes and may be audited by bank inspectors without prior notice.

As a result of the inspector investigation conducted on the allegation that the applicant was working in a company registered to his wife, it was established that the applicant sent documents to the accountant of the company established on behalf of his wife using his corporate e-mail address and made a loan application by negotiating loans with other banks.

In his defense, the applicant stated that he was only helping his wife and that this situation affected his job performance, albeit from time to time.

As a result of the report, the employment contract was terminated for acting against the working principles of the bank due to the fact that the applicant carried out transactions in a way that would affect performance during working hours and engaged in commercial activities.

2 - The Applicant's Allegations

The applicant stated that his correspondence through his corporate e-mail accounts was inspected without prior notice and without his consent, and as a result, his employment contract was unfairly terminated and thus his right to respect for private life and freedom of communication were violated.

3 - Evaluation

It has been stated that, as a rule, communication tools provided to the employee **may be inspected and restrictions may be stipulated** within the scope of the management authority of the employer for legitimate reasons that may be **justified**, such as ensuring the control of the flow of information by carrying out the works effectively, protection against criminal and legal liability related to the actions of the employee, measuring efficiency or security concerns.

The interference made by the employer to the employee's right to demand protection of his personal data and freedom of communication must be **relevant** to the determined purpose, **sufficient** and **necessary**, and the data obtained shall be used for the determined purpose.

In the case in question, the employer **has a legitimate interest** in accessing the e-mail content, since with the processing of personal data through the corporate e-mails of the employees and controlling the communication flow are related to the effectiveness of the business carried out.

In addition, it was clearly stipulated in the employment contract that the corporate e-mail allocated to the applicant would only be used for business purposes and that the corporate e-mail could be audited by the bank management without prior notice and consequently the employment contract could be terminated. It must be accepted that the applicant has given his consent by signing the employment contract.

4 - Judgement

It has been decided that the right to request the protection of personal data within the scope of the right to respect for private life guaranteed under Article 20 of the Constitution and the freedom of communication guaranteed in Article 22 of the Constitution were not violated.

04 - The Commercial Advertising and Unfair Commercial Practices Regulation is Amended

One of the important problems relating to the protection of consumers is the application of a hidden price increase by reducing the weight, quantity and similar aspects of basic consumption products, mainly foods and cosmetics and cleaning products. In order to prevent these, an amendment has been made in the secondary regulation. In this context, the amendment made to the Regulation on Commercial Advertising and Unfair Commercial Practices is as follows:

1 - **Regulation Amending the Regulation on Commercial Advertising and Unfair Commercial Practices**

The Regulation Amending the Commercial Advertising and Unfair Commercial Practices Regulation was published in the Official Gazette numbered 31384 and dated 03.02.2021. With the amendment, the following clause has been added to the section titled "**Deceptive Commercial Practices**" in the "Exemplary Applications Regarded as Unfair Commercial Practices" of the Regulation:

- 20) Misleading packaging practices that **give the impression that no change has been made, even though a change has been made** in one of the items length, weight, area, volume dimensions and similar elements in a way to **differentiate the unit price** of a product offered to consumers.

Administrative sanctions shall be imposed on those who do not act in accordance with the regulation in the amendment made in accordance with Article 77 of the Law on the Protection of Consumers numbered 6502, which constitutes the legal basis of the Regulation. The regulation change shall be effective as of **01.04.2021.**

05 - Personal Data Protection Board Announced Its Decision numbered 2020/905 Regarding the Personal Data Breach Notification by an Insurance Company

The Personal Data Protection Board (**"Board"**) rendered a decision dated 24.11.2020 and numbered 2020/905 (**"Decision"**) regarding a data controller insurance company's (**"Data Controller"**) failure to take the necessary technical and administrative measures to ensure data security and to fulfill the obligation to notify data breach.

In the data breach notification submitted by the Data Controller, it is stated that, (i) the data breach has occurred due to a cyber-attack imposed upon the test server of the website and was detected the same day; (ii) the access efforts directed to the login page of the website which were attempted from abroad and made multiple times periodically were not detected; (iii) the database which included personal data was erased during the breach, and replaced by ransom notes; (iv) the data base was possibly copied before it was erased; and (v) the number of data subjects affected by the data breach is 311, whereas the personal data affected by the breach included national identity numbers, names, surnames, e-mails and vehicle registration plates of the data subjects.

Within the scope of taking necessary technical and administrative measures to ensure data security in accordance with Article 12, paragraph 1 of the Personal Data Protection Law numbered 6698 (**"PDP Law"**), the Board determined in terms of the Data Controller that;

- The test server where the data breach occurred was not included in the periodical leak tests, thus it demonstrates that the necessary controls were not exercised;
- Even though a Procedure on the Data Safety and Data Breach was prepared by the Date Controller, the controls indicated thereby were not provided;
- The test page was accessible worldwide and the passwords were not at a sufficient complexity and strength level;
- Considering that after the breach it was possible to exercise the testing processes on the test server before recording of the personal data, the personal data would not be jeopardized if such technology were used before the breach as well;
- Methods for providing secure communication and strong authentication methods as additional safety guard were not used in accessing the test server;

- National ID number which is of importance to data subjects was included in the personal data that is affected by the breach, although the adverse outcome of the breach might have been decreased by storing important personal data as encrypted according to their level of confidentiality, sufficient care was not demonstrated by the Data Controller. In light of these evaluations, the Board decided to impose an administrative fine of TRY 300.000 on the Data Controller in accordance with Article 18, paragraph 1, subsection (b) of PDP Law, due to failure of taking necessary technical and administrative measures to ensure data security in accordance with Article 12, paragraph 1 of the PDP Law.

Within the framework of the data breach notification obligation regulated in Article 12, paragraph 5 of the PDP Law, the Board also assessed that the Data Controller;

- did not make a data breach notification to the Personal Data Protection Authority (**"Authority"**) within the period of 72 hours as of the detection of the data breach in accordance with the Board Decision dated 24.01.2019 and numbered 2019/10;
- did not notify the data subjects who were determined to be affected by the breach in accordance with the Board Decision dated 18.09.2019 and numbered 2019/271, and the announcement made on Data Controller's website could not be regarded as a notification to the identified data subjects in this context.

In light of these assessments, the Board concluded that the Data Controller did not notify the Authority and the data subjects properly, and decided to impose an administrative fine of TRY 30.000 on the Data Controller in accordance with the Article 18, paragraph 1, subsection (b) of PDP Law.

06 -Personal Data Protection Board Rendered a Decision numbered 2020/787 on the Data Breach Notification of a Company Operating in the Healthcare Sector

Personal Data Protection Board (**"Board"**) rendered a decision (**"Decision"**) dated 09.10.2020 and numbered 2020/787 regarding the data breach notification made by a data controller (**"Data Controller"**) operating in the healthcare sector.

It is stated in the Decision that the Data Controller submitted a data breach notification indicating that (i) the data breach which started on 30.09.2020 was a result of a vulnerability of an application used worldwide; (ii) the data breach was detected and ended on 05.10.2020; (iii) the supporting documents regarding the employee trainings organized within the last year of the data breach, and the technical and administrative measures taken before and after the data breach were submitted to the Authority; (iv) a notification would be

made to the data subjects who are affected by the data breach, within 3 days of the notification submitted to the Board.

The Board made the following determinations regarding the data breach notification submitted by the Data Controller:

- The data breach has occurred due to a vulnerability in a commonly used application, thus it cannot be expected from the Data Controller to interfere in this situation;
- The Data Controller has detected the breach in a short period of time;
- The personal data affected by the data breach is easily accessible, since such data is provided on the private company stamps and at the public sources;
- It has been stated by the Data Controller that the data subjects would be notified in up to three days after the data breach notification was submitted to the Board;
- The possibility of an adverse outcome due to the data breach is low in terms of the data subjects;
- The Data Controller has taken reasonable administrative and technical measures.

In light of its assessments, the Board decided not to impose any additional sanctions on the Data Controller in accordance with Article 12 of the Personal Data Protection Law numbered 6698, provided that the supporting documents regarding the data breach notification made to the data subjects are submitted to the Board.

March

01 **Procedures And Principles Regarding Turnover Loss Support For Food And Beverage Service Enterprises Are Determined.**

02 **The Presidency Of The Republic Of Turkey Announced The Human Rights Action Plan Through An Announcement Meeting Held İn Ankara On March 2, 2021.**

03 **The Law On Technology Development Zones And Amendments To Certain Laws.**

04 **Personal Data Protection Board Rendered A Decision Regarding An Insurance Company's Requirement Of Explicit Consent For Providing Service To The Data Subject.**

05 **Personal Data Protection Board Rendered A Decision On Complaints Regarding The Correction Or Deletion Of Past Health Data.**

06 **Personal Data Protection Board Rendered A Decision Regarding A Complaint On Unauthorized And Unlawful Access To An E-Mail Account Which Was Used By The Data Subject Partner Of The Company.**

07 **Personal Data Protection Board Announced Its Decision On The Notice Regarding The Negligent Spoilage And Subsequent Destruction Of Scientific Data Samples Recorded For Scientific Purposes.**

08 **The Procedures And Principles For The Determination, Prevention And Elimination Of Price Squeezing Has Been Published!**

09 **Personal Data Protection Board's Decision Regarding Processing Of Biometric Data Of Municipal Officers For Time Keeping Purposes is Published.**

10 **Limits Concerning Identification Has Been Changed In Prepaid Card, Life Insurance Contracts And E-Money Transactions.**

01 - Procedures and Principles Regarding Turnover Loss Support for Food and Beverage Service Enterprises are Determined

Procedures and principles regarding the turnover loss support to be granted to enterprises operating food and beverage services, due to the coronavirus epidemic, have been determined by the Presidential Decree numbered 3505 ("**Decree**") published in the Official Gazette dated 06.02.2021 and numbered 31387. Accordingly, the procedures and principles regulated by the Decree are as follows:

1 - Turnover Loss Support

- Turnover loss support will be covered from the appropriation to be placed in the budget of the Ministry of Commerce ("**Ministry**").
- Enterprises which may benefit from the support are those which started their business that commenced before the 2019 calendar year or in the 2019 calendar year and are active taxpayers as of 27.01.2021. The enterprises which may benefit from the support have to continue their business during this period, and their turnover in the calendar year 2019 must be 3 million Turkish Liras or less. In addition, their turnover in the calendar year 2020 must have decreased by 50% or more compared to the turnover in said year.
- The turnover loss support shall be given on the basis of 3% of the reduced turnover of the companies in the 2020 calendar year compared to the turnover in the calendar year 2019. This amount shall be a minimum of 2000 TL and a maximum of 40.000 TL to be paid at once.

- Value added tax declarations submitted for the taxation periods in the calendar years 2019 and 2020 as of 27.01.2021 shall be taken as basis for the determination of the turnover calculation. The declarations (including correction statements) submitted for the periods in the calendar years 2019 and 2020 after the said date shall not be taken into account in the calculation.
- If a business is entitled to receive a support both under this Decree, and under the President Decree No. 3323 (**"Decree No. 3323"**) that regulates support to be granted to tradesmen and craftsmen and real person merchants, the amount they are granted under Decision No. 3323 shall be deducted from the turnover loss support.
- If it is determined that an excessive or unjustifiable turnover support is made, it shall be collected by the tax offices in accordance with the provisions of the Law No. 6183 dated 21.07.1953 on the Procedure for Collection of Public Receivables.
- The application period and other procedures and principles regarding turnover loss support shall be determined by the Ministry.

02 - The Presidency Of The Republic Of Turkey Announced Human Rights Action Plan Through An Announcement Meeting Held İn Ankara On March 2, 2021

The objectives for the protection of the personal data are announced through the Announcement Meeting of the Human Rights Action Plan held in Ankara on 02.03.2021 by the Presidency of the Republic of Turkey.

The objectives for the protection of the personal data are as follows:

i. Adapting the Personal Data Protection Law to the standards of the European Union, in order to provide the protection of individual privacy in the personal data processing,

ii. Procuring the opportunity to appeal to the administrative jurisdiction instead of appealing to the penal court of peace, against the administrative fine decisions of the Personal Data Protection Board,

iii. Providing public access to all decisions of the courts of first instance and the courts of appeal, within compliance with the principle of protection of the personal data,

iv. Providing public access to the decisions of the Ombudsman Institution and Human Rights and Equality Institution of Turkey, by means of the protection of the personal data.

03 - The Law on Technology Development Zones and Amendments to Certain Laws

With the transition of the information and document management in the physical environment to the electronic environment, there has been a need for the verification of the information and documents in the electronic environment. In this context, the Electronic Signature Law (**"the Law"**) numbered 5070 has entered into force as of 23 July 2004 in order to provide security regarding transactions in the electronic environment.

As a reflection of the digital transformation experienced within legal entities due to the pandemic conditions, the Law was amended. The amendments made to the Law, pursuant to The Law on Technology Development Zones and Amendments to Certain Laws published in the Official Gazette numbered 31384 and dated 3 February 2021 are as follows:

1 - The following paragraph has been added to Article 10 of the Law:

"Electronic certification service provider may securely and remotely install the qualified certificate to the identification card if the service provider could remotely and securely confirm the identity card information of the people who are given qualified certificate via Republic of Turkey identity card."

- With the amendment, it will be possible to carry out certification processes without physically gathering or needing a physical document.

2 - ADDITIONAL ARTICLE 1 titled "Electronic Stamp" has been added:

"An electronic stamp is electronic data attached to other electronic data or linked logically to electronic data and used to verify the stamp owner's information.

The owner of the electronic stamp is the public institutions and organizations, public administrations, public professional organizations and higher organizations, public and private legal entities, judicial authorities and notaries that create the electronic stamp.

An electronic stamp is the evidence record that the electronic document or data was created by the stamp owner and guarantees the origin and integrity of the document or data.

The electronic stamp has the same legal status as any physical stamp, including the official stamp.

Without the consent or request of the stamp owner for the purpose of creating an electronic stamp; those who obtain, export, copy and recreate stamp creation data or stamp creation tools and those who create electronic stamps using unauthorized stamp creation tools are punished with imprisonment from one to three years and a judicial fine of not less than fifty days. In case the offense is committed by employees of electronic certificate service providers, these penalties are increased up to half.

The provisions on electronic signature regulated under laws shall also be applied to electronic stamps by analogy.

The rights, powers, and obligations of electronic certificate service providers regarding the electronic signature specified in the laws are also applied to the electronic stamp. Administrative fines specified in Article 18 shall be imposed on electronic certificate service providers who act contrary to these obligations.".

With the amendment, public institutions and organizations, public administrations, public professional organizations and higher organizations, public and private law legal entities, judicial authorities and notaries shall be able to use electronic stamps. However, those who create a stamp without the consent or request of the stamp owner or who use electronic stamp means may be imprisoned from one to three years or be subject to a judicial fine of not less than fifty days.

3 - ADDITIONAL ARTICLE 2 titled "Website authentication certificate and other electronic certificates" has been added:

"Website authentication certificate is an electronic record that connects a website with the information of the real or legal person who owns this site.

Other electronic certificates using similar infrastructure are certificates issued by electronic certificate service providers through public key infrastructure to be used for purposes such as encrypting electronic data or determining the integrity, undeniability and source of data.

The provisions on electronic signature regulated under the laws shall also be applied to the website authentication certificate and other electronic certificates using similar infrastructure by analogy.

The rights, powers, and obligations of electronic certificate service providers regarding electronic signature under the laws are also applied to the website authentication certificate and other electronic certificates using similar infrastructure. Administrative fines specified in Article 18 shall be imposed on electronic certificate service providers who act contrary to these obligations."

With the website verification certificate, an important step has been taken to ensure information security on the internet. It may be possible to see its reflections on data and information security, especially in terms of data-intensive financial and e-commerce sites.

Provisions in the legislation on electronic signature shall be applied to electronic stamps, website authentication certificates and other electronic certificates by analogy.

As a result of the digitalization that intensified with the pandemic, the change in the name of providing the remote management of information and documents can be considered as a positive development.


MEDICAL

04 - Personal Data Protection Board Rendered a Decision Regarding an Insurance Company's Requirement of Explicit Consent for Providing Service to the Data Subject

The Personal Data Protection Board (**"Board"**) rendered a decision dated 03.09.2020 and numbered 2020/667 (**"Decision"**) regarding a complaint of the data subject complainant (**"Complaint"**) for the request of the data controller insurance company (**"Data Controller"**) to obtain explicit consent for the renewal of the health insurance policy arranged on behalf of their family and thus the proceeding allegedly violates the Personal Data Protection Law numbered 6698 (**"PDP Law"**).

Through its evaluation within the framework of the Complaint, the Board determined that (i) personal data related to health and sexual life can only be processed with the explicit consent of the data subject under Article 6, sub-clause 3 of the PDP Law, (ii) that the health data included in the health insurance policy are deemed to be personal data of special nature and cannot be processed without the explicit consent of the data subject under Article 6, sub-clause 3 of the PDP Law.

Following its abovementioned determinations, the Board decided that the proceeding subject to the Complaint does not constitute a violation of the PDP Law and therefore, there is no procedure to be established under the PDP Law.


2
C
USA/UK
32
CUP
EU
10
ES/FR
85
033805 568057

05 - Personal Data Protection Board Rendered a Decision on Complaints Regarding the Correction or Deletion of Past Health Data

The Personal Data Protection Board (**"Board"**) rendered a decision dated 06.02.2020 and numbered 2020/93 (**"Decision"**) regarding the complaints (**"Complaints"**) of the complainant data subjects (**"Complainant"**) in respect of the rejection of correction or deletion of health reports and psychiatric diagnoses, which were recorded in the past for various reasons and currently causing problems due to inaccuracy, by the data controller Ministry (**"Data Controller"**).

Within the defense that was requested of the Data Controller, the Data Controller stated that; (i) requests for deletion of personal data of the data subjects could be rejected by the data controller on the grounds that processing conditions for personal data are not fully eliminated, pursuant to Article 12 of the Regulation on the Deletion, Destruction and Anonymization of Personal Data published in the Official Gazette dated 28.10.2017 and numbered 30224, (ii) the deletion of past psychiatric diagnoses of individuals from their health history could pose serious dangers in terms of public security and public order, (iii) in accordance with Article 28, sub-clause 1 the Personal Data Protection Law numbered 6698 (**"PDP Law"**) it is stated that the PDP Law will not be implemented in cases of public security and public order by full exemption, (iv) in accordance with Article 6, sub-clause 3 of the PDP Law, personal data may be processed by the data controller without seeking the explicit consent of the data subject, (v) the letters written by the relevant physician, chief physician, provincial health directorate or the relevant General Directorate regarding the inadvertently recorded diagnoses should be forwarded to relevant General Directorate for deletion of the same, (vi) it is required to apply to the relevant provincial health directorate for diagnoses that are not proven to be inadvertently recorded, (vii) the diagnoses that are proven to be made inadvertently or no longer affecting the person could be deleted.

As a result of the examination made by the Board, it was decided that, (i) there is no procedure to be established within the scope of the PDP Law because the processing conditions did not cease in terms of the personal health data of the Complaints, (ii) the Data Controller continues to process the personal health data subject to the Complaints in accordance with Article 6, sub-clause 3 of the PDP Law, (iii) therefore, there is no procedure to be established within the scope of the PDP Law.


100/1.25
160/0

06 - Personal Data Protection Board Rendered a Decision Regarding a Complaint on Unauthorized and Unlawful Access to an E-Mail Account Which was Used by the Data Subject Partner of the Company

The Personal Data Protection Board ("**Board**") rendered a decision dated 27.01.2020 and numbered 2020/59 ("**Decision**"), following the complaint ("**Complaint**") of the data subject complainant ("**Complainant**") regarding unauthorized and unlawful access to the personal e-mail account (@nameofthecompany.com.tr) which consists personal data and was used within a Limited Liability Company ("**Limited Company**") of where the Complainant is a partner; changing access settings of the e-mail; and the rejection of the request by the data controller owner of the IP addresses to which this e-mail is affiliated ("**Data Controller**") on deletion and removal of all the data in the e-mail account in question.

Within the defense that was requested of the Data Controller company, it is stated that (i) the General Manager of the Data Controller company is also the partner and the authorized manager of the Limited Company, (ii) the e-mail account owned by the Limited Company is not the personal account of the Complainant, but it is an account which was allocated to follow transactions of the company, (iii) it is certain by the decision of the Commercial Court of First Instance and the Prosecutor's Office that the access to the e-mail address with the company extension in question was not illegal, (iv) the e-mails accessed from backup servers are only submitted to the Court and the Prosecutor's Office as part of the criminal complaint as evidence in relevant cases, (v) the allegations that the e-mail account of the Complainant was accessed and the access settings were changed are far from the truth and such claims were denied by the Court and the Prosecutor's Office, (vi) the request to delete all data, backups and copies of the e-mail account of the Complainant was rejected due to prevent the spoliation of evidence, (vii) it is lawful to audit the backup records of the e-mail address with the extension of the company, due to fulfilling the duties of a manager in accordance with the Article 626 of the Turkish Commercial Code numbered 6102.

As a result of the examination of the Complaint of the Complainant, the defense of the Data Controller and the related legislation provisions, the Board determined that, (i) processing is carried out for the purpose of establishing, exercising and protecting a right within the scope of Article 5, sub-clause 2, paragraph (e) of the Personal Data Protection Law numbered 6698 ("**PDP Law**"), (ii) processing of personal data by means of filing a lawsuit at the Commercial Court of First Instance via using personal data is in accordance with the scope of Article 28, sub-clause 1, paragraph (d) of the PDP Law, and (iii) in light of the aforementioned determinations, there is no procedure to be established under the PDP Law regarding the Complaint.


In
Out

07 - Personal Data Protection Board Announced Its Decision on the Notice Regarding the Negligent Spoilage and Subsequent Destruction of Scientific Data Samples Recorded for Scientific Purposes

The Personal Data Protection Board (**"Board"**) rendered a decision dated 30.10.2019 and numbered 2019/316 (**"Decision"**) on the complainant doctor's (**"Complainant"**) notice (**"Notice"**), regarding the data controller Hospital (**"Data Controller"**) who has recorded the patient records of data subject chronic patients' (**"Data Subjects"**) on local computers and hospital data system; stored the blood, serum and tissue samples (**"Samples"**) taken from the Data Subjects in a proper environment to be used in projects; caused the Samples to spoil as a result of not taking the reasonable care to keep the samples under appropriate conditions; and therefore, the Data Controller did not fulfill its obligations regarding data security in accordance with Article 12 of the Personal Data Protection Law numbered 6698 (**"PDP Law"**).

The Data Controller stated in its defense submitted to the Board that (i) the Data Subjects whose patient records are kept are regular patients with ongoing treatments, (ii) the refrigerators that the Samples have been kept were not used until they malfunctioned, all records are kept regarding the malfunction, it is investigated whether the Samples were good to use and the Samples were destroyed due to their spoilage, (iii) there are no patient consent forms regarding the Samples and since the Samples were spoiled there was no scientific value of any match with the patients, (iv) any analysis of the Samples would violate the scientific ethic rules due to lack of the patient consent forms, and the Samples were not made subject to analysis because of spoilage and were not used in any other research.

After examining the Notice and the defense of the Data Controller, the Board determined that (i) the Samples gathered from the Data Subjects should be considered as personal data since the Samples are stored in a way that the identity of the patient can be determined, (ii) the classification and recording of the personal data in question according to certain criteria is a personal data processing activity, (iii) pursuant to Article 28, sub-clause 1, section c of the PDP Law, the PDP Law provisions are not applicable in case of personal data processed with scientific purposes provided that national defense, national security, public security, public order, economic security, right to privacy or personal rights are not violated or their processing does not constitute a crime; and that there is no procedure to be established under the PDP Law regarding the Notice.

08 - The Procedures and Principles for the Determination, Prevention and Elimination of Price Squeezing Has Been Published

The "Procedures and Principles for the Determination, Prevention and Elimination of Price Squeezing" (**"Procedures and Principles"**), updated with the Board Decision of the Information Technologies and Communication Authority (**"Authority"**) dated 09.02.2021 and numbered 2021/DK-SRD/36, has been approved and published on the official website of the Authority. The said Procedures and Principles will enter into force as of 01.04.2021. The previous "Procedures and Principles Regarding the Determination, Prevention and Elimination of Price Squeezing" (**"Old Procedures and Principles"**), which entered into force as of 01.07.2014 has been abolished. The content of the said procedures and principles are as follows

1 - Legal Basis:

The aforementioned Procedures and Principles have been drafted on the basis of sub-clauses (a), (d), (ı) and (k) of Article 4 and Articles 6, 7, 13, 14, 20 and 60 of the Electronic Communication Law published in the Official Gazette dated 10.11.2008 and numbered 27050 (Repeating) , Article 10 of the Market Analysis Regulation published in the Official Gazette dated 27.11.2012 and numbered 28480, Articles 5, 7 and 11 of the Access and Interconnection Regulation published in the Official Gazette dated 08.09.2009 and numbered 27343, and Articles 5, 15 and 17 of the Tariff Regulation published in the Official Gazette dated 12.11.2009 and numbered 27404.

2 - Regulation:

The said Procedures and Principles aim to provide and protect effective and sustainable competition. For this purpose, the Procedures and Principles are determined regarding the prevention of price squeezing in wholesale and retail tariffs and the measures to be applied if they involve price squeezing **by an undertaking with effective market power and / or a partner, affiliate or partnership operating within the same control structure in a vertically related market** which are subject to price squeezing obligation within the scope of the relevant market analysis.

The provisions regulated within this scope are as follows:

- Prerequisites for the application of price squeeze obligation and its analysis,
- Scope of the price squeezing analysis,
- Implementation of price squeezing analysis,
- Providing necessary information and documents for price squeezing analysis,
- Information on the model to be used in price squeezing analysis,
- Calculation of retail level costs to be used in price squeezing analysis,
- Calculation of wholesale costs to be used in price squeezing analysis,
- Performing price squeezing analysis,
- Administrative sanctions,
- Current tariffs of undertakings with effective market power in relevant markets.

3 - The Amendments Pursuant to the New Procedures and Principles

In the Old Procedures and Principles that entered into force in 2014, the Elements to be the Basis of Price Squeezing Analysis and Model was structured as a single annex covering all services in which a single price squeezing analysis was applied. In the newly published Procedures and Principles, the procedures and principles of the price squeezing analysis to be applied to Fixed Voice Services Offered at Retail Level and Broadband Internet Services Offered at Retail Level have been structured in two separate annexes. As per the New Procedures and Principles while the regulations within the scope of Fixed Voice Services Offered at Retail Level have not been amended, the procedures and principles regarding Broadband Internet Services Offered at Retail Level have been amended.

09 - Personal Data Protection Board's Decision Regarding Processing of Biometric Data of Municipal Officers for Time Keeping Purposes is Published

Pursuant to the decision (**"Decision"**) of the Personal Data Protection Board (**"Board"**) dated 01.12.2020 and numbered 2020/915, upon the complaint of an employee working as an official of the data controller, stating that their personal data is processed through fingerprint scanning devices for work entry and exit tracking, it was decided upon the instruction of the data controller to terminate biometric data processing for employee tracking and to remove the existing system. The content of the decision in question is as follows:

1 - Subject of the Application:

In the complaint made by the data subject, it was stated that:

- Personal data is processed with fingerprint scanning devices in order to track employees' entry and exit,
- Data subject applied to the data controller with the request of deletion of her/his fingerprint information by the data controller and to be informed regarding the process,
- In the reply provided to the applicant, it was declared that the data in question shall not be deleted from the data controller's systems,
- Fingerprint data cannot be processed without the data subject's consent and the request of the applicant for deletion of the data has not been accepted despite official application.

2 - Defense of the Data Controller:

It was stated that:

- The employee was informed regarding data processing activities and the policies and procedures regarding the protection and processing of personal data were drafted, and the data controller was audited by the Independent Audit Firm and was certified with the BS10012-2009 Data Protection and Personal Information Management Standard Certificate.
- Data subject's application was not submitted via a Personal Data Protection Application Form, additionally the application was not submitted to the employee who acts as a data controller representative, and instead was submitted to the Directorate of Human Resources and Education with the title Request for Information and Documentation, hence the application was not regarded as within the scope of the PDP Law, and there was no statement indicating that the fingerprint cannot be deleted,

- In accordance with the Employee Tracking System (**"PDKS"**) implemented by the Presidency, fingerprint data obtained from employees are used only for time keeping, the fingerprint system has been disabled due to the epidemic, the fingerprint data that has been turned into a template which cannot be viewed and processed in any way and the encrypted fingerprint template used is a special algorithm which may not be accessed by third parties.

3 - Evaluation:

It has been evaluated by the Board that:

- The processing of fingerprint data of the employee by the data controller for time keeping is considered as the processing of special category of personal data, since fingerprint data is considered biometric data,
- Fingerprints obtained from the employee in accordance with the employee tracking system, are used by the data controller for time keeping, however, considering that the data subject has complained about the processing of fingerprint data without his consent, it is concluded that the data subject does not give explicit consent to time keeping via the use of fingerprint data,
- It is concluded that the data processing is contrary to the principle of proportionality,
- The data subject made a request for the deletion of his personal data, but the data controller did not consider the application of the data subject within the scope of the Law and did not respond to the request of the data subject regarding deletions, and thus this case is contrary to good faith.

4 - The Decision:

It has been decided upon the instruction of the data controller to immediately destruct data related to fingerprints processed and stored by the data controller, to promptly notify third parties to whom the fingerprint data was transferred, to provide alternative means of time keeping and employee tracking, and to terminate the current practice.

10 - Limits Concerning Identification Has Been Changed in Prepaid Card, Life Insurance Contracts and E-Money Transactions

The Communiqué on the Amendment of the "Financial Crimes Investigation Board General Communiqué (No: 5)" (No: 18) ("**Amending Communiqué**") published in the Official Gazette dated 26.02.2021 and numbered 31407 has entered into force as of 01.05.2021. With the amendment, the monetary amounts based on identification have been updated within the scope of simplified measures, and implementation requirements have been arranged. The amendments brought by the said Amending Communiqué are as follows:

1 - Amendments Brought by the Communiqué

- In cases where money laundering or terrorist financing is suspected, the simplified measure shall not be applied. The subject shall be reported to the Financial Crimes Investigation Board ("**MASAK**") as a suspicious transaction report. Simplified measures shall not be used in transactions that are considered risky.
- In life insurance contracts, the limit on transactions that can be made by merely taking identity information without the need for confirmation documents when determining the identity of natural persons has been increased. According to this:

– The limit, which was set as 3000 TL and below for the total premium amount to be paid within 1 year, has been amended as 5000 TL and below transactions.

– The limit set as single premium transactions with a premium amount below 7500 TL has been amended as transactions below 12.500 TL.

- With the amendment introduced, the simplified measure may be implemented for the individual pension contract linked to the group in addition to the employer group pension contracts.
- For sales of prepaid cards, which cannot be used for fund transfer and are only used for cash withdrawal or purchase of goods and services, the upper limits of transactions, for which identification is not required, have been amended. Accordingly:

– The limit that should not exceed the cash withdrawal amount within the same year has been increased from 300 TL to 500 TL.

– For single-use transactions that cannot be reloaded, the limit that shall not exceed the amount of heavy money has been increased from 750 TL to 1250 TL.

– In transactions that can be reloaded, the limit that shall not exceed the total loading limit and in any case the total balance within a month has been increased from 750 TL to 1250 TL.

- The upper limits of transactions for electronic money institutions that do not require identification have been increased.

In Transactions Regarding the Procurement of Electronic Money:

– The limit that shall not exceed the cash withdrawal amount within the same year has been increased from 300 TL to 500 TL.

– If there is no possibility of reloading, the limit that shall not exceed the amount of funds stored electronically has been increased from 750 TL to 1250 TL.

– The limit, which shall not exceed the total loading amount and in any case the total balance within a month for those who can be reloaded, has been increased from 750 TL to 1250 TL.

In Transactions Regarding Mobile Payment Services:

– The limit that shall not exceed the one-time transaction amount has been increased from 300 TL to 500 TL.
– The limit that shall not exceed the monthly transaction amount has been increased from 750 TL to 1250 TL.

- The scope of simplified measures has been expanded in transactions where the client is a listed company.
- Government Business Enterprises are also included in the scope of simplified measures.
- For legitimate betting companies, a simplified measure may also be applied if the users make transactions with their own credit cards.

April

01 Turkey's Competition Authority Has Launched An Investigation Into The Online Advertising Sector.

02 The Regulation Prohibiting The Use Of Crypto Assets In Payments is Published.

03 The Regulation On Remote Identification Methods And Establishment Of Contractual Relations In Electronic Environment To Be Used By Banks Has Been Published In The Official Gazette.

04 The Eu Commission Announces The First Ever Legal-Framework Regarding The Framework Of Rules Related To Artificial Intelligence.

05 Deadlines Regarding Prohibition Of Employment Contract Termination And Unpaid Leave Are Extended.

06 The Termination Date Of The Istanbul Convention For The Republic Of Turkey is Determined.

01 - Turkey's Competition Authority Has Launched an Investigation into Online Advertising Sector

Turkey's Competition Authority has launched an investigation into the online advertising sector on March 6, 2021, after the Board's meeting on January 21, 2021. It is aimed to find out the structure and functioning of the sector, the structural and / or behavioral competition problems in the sector and discuss the adequacy of existing competition law instruments and possible new instruments, in order to establish an effective competition. In this respect, it is planned to meet with policy makers, enterprises and association of undertakings in order to find out market failures and competition problems and to propose solutions in the process.

Sector stakeholders who want to share their opinions and suggestions about the investigation, will be able to send them until June 21, 2021 to the address reklamcilik@rekabet.gov.tr. If stakeholders have confidentiality requests for their opinions, they are required to submit these requests together with their opinions.

02 - The Regulation Prohibiting the Use of Crypto Assets in Payments is Published!

The Regulation Prohibiting Payments Through Crypto Assets issued by the Central Bank of the Republic of Turkey is published in the Official Gazette dated 16.04.2021 and numbered 31456 (**"Regulation"**). The Regulation entered into force on 30.04.2021.

The Regulation defines crypto assets as intangible assets which are created virtually by a technology such as distributed ledger or similar, and are distributed through digital networks but cannot be acknowledged as fiduciary money, deposit money, electronic money, payment instrument, security, or other capital market instruments.

The Regulation prohibits;

i. Use of crypto assets directly or indirectly in payments;

ii. Provision of services for use of crypto assets directly or indirectly in payments;

iii. Development of business models by the payment service providers regarding the direct or indirect use of crypto assets in provision of payment services and export of electronic money, and provision of services regarding development of such business models by the payment service providers;

iv. Mediation of the payment and electronic money institutions regarding fund transfers from and to the platforms providing services on trading, depositing, transferring, or exporting of crypto assets.

In light of the foregoing, although the Regulation prohibits licensed payment institutions and electronic money institutions from using crypto assets in their operations, it does not introduce any regulations with respect to crypto asset trading platforms.

Taking into consideration that the crypto assets reflect only one aspect of the Blockchain technology applications, we believe that this Regulation shall not prevent significant technological developments which are constituted on the Blockchain technology such digital identity, open data, smart contracts in Turkey.

However, we are of the opinion that the Regulation may have a negative effect on the innovative solutions and applications of the licensed payment institutions and electronic money institutions.

03 - The Regulation on Remote Identification Methods and Establishment of Contractual Relations in Electronic Environment to be Used by Banks Has Been Published in the Official Gazette

"The Regulation on Remote Identification Methods and Establishment of Contractual Relations in Electronic Environment to be Used by Banks", ("**Regulation**") has been drafted by the Banking Regulation and Supervision Agency ("**BRSA**") and has been published in the Official Gazette dated 01.04.2021 and numbered 31441. The Regulation, which will enter into force as of 01.05.2021 regulates the procedures and principles for the establishment of a contractual relationship over an informatics or electronic communication device, or as a replacement for the written form or at a distance, which is intended to be used in remote identification methods that may be used by banks to gain new customers and banking services to be offered after the identification of the customer, whether it is distant or not. The procedures and principles regulated by the Regulation are as follows:

1 - <u>Things to Do Before Remote Identification Process</u>

Remote identification takes place in the form of online video calls and communication with each other, without the need for the customer representative and the person to be physically in the same environment.

In the video call method to be used in remote identification, adequate security measures shall be taken by considering possible technological, operational and similar risks.

The remote identification process shall be reviewed at least twice a year and updates should be made to improve the process when necessary.

2 - Customer representative and working environment for remote identification

The video call phase of remote identification will be carried out by a trained customer representative.

The customer representative is required to receive the necessary training, including the legislation on the protection of personal data, at least once a year after each update for remote identification methods and banking services to be offered upon determination of the customer identity.

3 - General principles to be followed with the initiation of the process

In the remote identity verification process, before the video call starts, an application is received via a form that the person shall fill in electronically and through the bank application where the remote identification process is operated.

Risk assessment is carried out regarding the person by using the data obtained with the form.

In the remote identification process to be applied within the scope of the Regulation, only biometric data can be used within the framework of the customer's special categories of personal data. It is possible to use the relevant data electronically by obtaining the explicit consent of the customer.

In summary, following the remote identification or face-to-face identification of the customer through branches, customers whose any of the channels such as internet banking or mobile banking are open to use, declarations of intention to establish a contractual relationship are required.

In order for the contract to be established, whether it is distant or not, all the terms of the contract must be conveyed to the customer through internet banking or mobile banking channels in a way that the customer may read, the customer must receive the declaration of intention for the establishment of the contract and the customer must sign the contract conveyed to him/her.

In the event that the contract is established electronically or the customer's declaration of intention to establish the contract is established at a distance following the identification during the video call phase, it is accepted that the written form requirement for contracts is fulfilled.

04 - The EU Commission Announces the First Ever Legal-Framework Regarding the Framework of Rules Related to Artificial Intelligence

"Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts" ("**Proposal**") regulation has been proposed on 21.04.2021, by the European Union Commission ("**EU Commission**"). The regulation in question is a legal regulation that includes the framework of rules regarding artificial intelligence. The approval of the European Parliament and member states is required for the regulation proposal to enter into force. When the regulation is adopted, the activities of other countries' technology companies operating in EU countries will also be restricted. This Proposal aims to implement the objective for the development of an ecosystem of trust by proposing a legal framework for trustworthy AI. The proposal is based on EU values and fundamental rights; and aims to give the confidence to embrace AI-based solutions, while encouraging businesses to develop them. Some of the issues regulated by the Regulation are as follows:

1 - Definitions

In the proposal, the definition of 44 terms has been made. These definitions include "Artificial Intelligence System" and "User". Accordingly, the Artificial Intelligence System is defined as "***software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with", and User is defined as "Any natural or legal person, public authority, agency or other body using an artificial intelligence system under its authority, except where the AI system is used in the course of a personal non-professional activity.***". Technical issues such as 'training data, 'testing data', 'validation data', 'input data' have also been defined.

2 - Risk Groups

With the proposal, artificial intelligence systems were divided into 3 main groups as "unacceptable risk", "high risk", "low risk" or "minimum risk". Lists regarding the contents of the groups in question are shared in Annex 3. Accordingly, some applications in the high-risk group are as follows:

- Biometric identification and categorisation of natural persons:
  - AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural

- Management and operation of critical infrastructure:
  - » AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
- Education and vocational training:
  - » AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions

In addition, artificial intelligence systems, which are considered to be a clear threat to people's safety, livelihoods and rights, are in the unacceptable risk group and their use is prohibited.

Applications that manipulate human behavior, prevent free will, and enable social scoring by governments and artificial intelligence systems are included in the "unacceptable" risk group.

AI systems in the low-risk group shall be subject to some transparency obligations. It shall be ensured that the users are aware that they are interacting with a machine while talking with the "chatbots" in this group and make informed decisions.

Applications such as AI-powered video games or spam filters were in the minimum risk group.

3 - High-Risk Artificial Intelligence Systems

A number of requirements have been stipulated for high-risk AI systems. For example, A risk management system shall need to be established for high-risk AI systems.

The risk management system will need to include a process that runs throughout the entire life cycle of the high-risk AI systems and requires regular systematic updates and the steps determined in the regulation.

High-risk AI systems shall need to be designed to keep log records while working. Records to be contained at the minimum has also been determined.

With regard to the provision of human surveillance, high-risk AI systems, including appropriate human-machine interface tools, will need to be designed in such a way that they can be effectively controlled by natural persons while the Artificial Intelligence system is in use. High-risk Artificial Intelligence systems shall be developed to achieve an appropriate level of accuracy, robustness and cyber security in light of their targeted objectives and to perform consistently in these respects throughout their life cycles.

4 – Obligations

First, the obligations of high-risk Artificial Intelligence providers were discussed. It is envisaged that certain policies and procedures shall be drafted to ensure compliance with the regulation.

Some obligations are also set up for high-risk AI system importers and distributors.

Some obligations are also regulated for high-risk AI system users. For example, users of high-risk AI systems must use these systems in accordance with the instructions for use. The operation of the high-risk AI system on the basis of the instructions for use shall be observed. If there is a risky situation, the supplier or distributor shall be informed and the use of the system shall be suspended.

Before launching or putting into service a high-risk AI system, the provider or, where appropriate, the authorized representative shall register this system in the designated EU database.

5 - Penalties

Member States shall lay down the rules on penalties for violations of the regulation, including administrative fines, in accordance with the terms and conditions laid down in the Proposal, and shall take all necessary measures to ensure their proper and effective implementation. The stipulated penalties shall be effective, proportionate and deterrent. They shall pay particular attention to the interests and economic sustainability of small-scale providers and startups.

If the AI system does not comply with any of the requirements or obligations under the Proposal, a fine of up to 30,000,000 EUR or 6% of its worldwide total annual turnover may be imposed.

Finally, the European Artificial Intelligence Board has been proposed to be established.

05 - Deadlines Regarding Prohibition of Employment Contract Termination and Unpaid Leave are Extended

The period for the prohibition of employment contract termination due to Covid-19 pandemic is extended through the Presidential Decision dated 29.04.2021 and numbered 3930 (“**Decision no. 3930**”) published in the Official Gazette dated 30.04.2021 and numbered 31470, starting from 17.05.2021 until 30.06.2021, within the frame of the provisional article 10 of the Labour Act no. 4857 (“**Labour Law**”). Accordingly, employment contracts cannot be terminated until 30.06.2021 except for the reasons stated in the Provisional Article 10 of the Labour Law, nevertheless employers have the right to make the employees take partial or full unpaid leave for at most 3 months until 30.06.2021 as well under the Decision no. 3930. The employee cannot exercise such unpaid leave conditions as a cause for rightful termination of the employment contract.

06 - The Termination Date of the Istanbul Convention for the Republic of Turkey is Determined

It was decided through the Presidential Decision dated 19.03.2021 and numbered 3718 published in the Official Gazette dated 20.03.2021 and numbered 31429, that the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence ("**Istanbul Convention**") be terminated for the Republic of Turkey.

Through the Presidential Decision dated 29.04.2021 and numbered 3928 ("**Decision no. 3928**") published in the Official Gazette dated 30.04.2021 and numbered 31470, the termination date of the Istanbul Convention for the Republic of Turkey is determined as 01.07.2021.

May

01 Matters To Know Regardıng The Regulation On Active Co-Operation For Discovery Of Cartels (“Leniency Regulation”).

02 Crypto Asset Service Providers Are Specified Among The “Obliged Parties” Within The Frame Of The Measures Regarding Prevention Of Laundering Proceeds Of Crime And Financing Of Terrorism.

03 Legal Regulations Regarding Advertising And Marketing Activities Made By Influencers.

04 Financial Crimes Investigation Board Published The Crypto Asset Service Providers Guide.

05 The Report On Competition And Data Protection In Digital Markets: A Joint Statement Between The Cma And The Ico (‘’The Report’’) Has Been Published.

06 The Draft Regulation On Remote Identification Methods And Establishment Of Contractual Relations In Electronic Environment To Be Used By Financial Leasing, Factoring, Financing And Saving Financing Companies Has Been Published.

01 - Matters to Know Regardıng The Regulation on Active Co-Operation For Discovery of Cartels (“Leniency Regulation”)

The Regulation on Active Co-Operation for Discovery of Cartels, (**“Leniency Regulation”**) has been published in the Official Gazette dated 15.02.2009 and numbered 21142. The purpose of the regulation is to regulate the procedures and principles regarding the prevention of the imposed fines specified in the Law No. 4054 on the Protection of Competition (**“Law”**), or the reduction of penalties to be imposed to the undertakings, and the directors and employees of the undertakings who are actively cooperating with the Competition Authority (**“Authority”**) in order to reveal the cartels prohibited by Law. The Regulation consists of two parts: the provisions regarding the Undertakings, and the Managers and the Employees. The procedures and principles regulated by the Regulation are as follows:

1 - Prevention of imposing fines

In terms of undertakings:

The first undertaking to submit the information and documents specified in Leniency Regulation and fulfill the conditions, independently of its competitors, before the Competition Board (**“Board”**) decides to conduct a preliminary investigation, shall not be imposed fines. In addition, while there is no evidence to conclude that the “Agreements between undertakings, concerted actions and such decisions and actions of associations of undertakings that have the purpose of preventing, distorting or restricting competition directly or indirectly in a particular market of goods or services, or that have or may cause this effect, are illegal and prohibited.” prohibition regulated in Article 4 of the Law has been violated, from the decision of the Board to make a preliminary investigation until the notification of the investigation report, the first undertaking to submit the information and documents determined, independently from its competitors and fulfill the conditions, shall not be imposed fines. This provision is only possible if the above-mentioned option is not used.

In addition, while there is no evidence to conclude that the "Agreements between undertakings, concerted actions and such decisions and actions of associations of undertakings that have the purpose of preventing, distorting or restricting competition directly or indirectly in a particular market of goods or services, or that have or may cause this effect, are illegal and prohibited." prohibition regulated in Article 4 of the Law has been violated, from the decision of the Board to make a preliminary investigation until the notification of the investigation report, the first undertaking to submit the information and documents determined, independently from its competitors and fulfill the conditions, shall not be imposed fines. This provision is only possible if the above-mentioned option is not used.

In addition, in order to benefit from the aforementioned provision, there shall be no application made by a manager or employee who submitted the specified information and documents and fulfilled the conditions.

2 - Reduction in fines

In terms of undertakings:

From the decision of the Board of preliminary investigation to the notification of the investigation report, the fines to be imposed on undertakings that present the information and documents determined, independently from their competitors and fulfill the conditions but fail to benefit from the regulation on non-penalty shall be reduced. In this case, the fines to be imposed on the executives and employees of the undertakings who accept the violation and actively cooperate shall also be reduced.

If the fines must be increased due to the prolongation of the violation and similar reasons as a result of the evidence presented, the undertaking presenting the relevant evidence first and the executives and employees of this undertaking who accept the violation and actively cooperate shall not be affected from this increase.

In terms of Managers and Employees:

From the decision of the Board of preliminary investigation to the notification of the investigation report, the fines to be imposed on the executives and employees who provide the specified information and documents, independently from the undertakings that are a party to the cartel and the managers and employees of these undertakings and who fulfill the conditions but cannot benefit from the regulation on non-penalty shall be reduced. As a result of the evidence presented, if the fines need to be increased due to the prolongation of the violation and similar reasons, the manager or employee who presented the relevant evidence first shall not be affected by this increase.

3 - Conditions

- To present the information and documents regarding products affected by the cartel subject to application, the duration of the cartel, the names of the undertakings that are parties to the cartel, the dates and locations of the negotiations with the cartel,
- Not to hide or eliminate the information and documents about the cartel subject to application,
- Unless otherwise stated by the assigned unit on the grounds that it would make it difficult to uncover the cartel, cease to be a party to the cartel subject to application,
- Keeping the application confidential until the notification of the investigation report, unless otherwise specified by the unit in charge,
- To continue active cooperation until the final decision of the Board after the completion of the investigation.

02 - Crypto Asset Service Providers Are Specified Among the "Obliged Parties" Within the Frame of the Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism

The Regulation on the Amendment of the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Amending Regulation**") entered into force through the Presidential Decision dated 30.04.2021 and numbered 3941 published in the Official Gazette dated 01.05.2021 and numbered 31471.

Within the frame of the Amending Regulation, the crypto asset service providers as well as the savings finance companies are specified among the "Obliged Parties" stated under the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism.

03 - Legal Regulations Regarding Advertising and Marketing Activities Made by Influencers!

Influencers also known as social media celebrities are people who have a large number of followers on social media and have the capacity to influence this audience and thus have the effect of changing the purchasing decisions of their followers. Viral marketing method is mostly made by the "Influencer". However, in advertising activities, it is especially necessary to act in accordance with the competition law and to comply with the newly introduced tax regulation. Some of legal regulations regarding advertising and marketing activities carried out through influencers are as follows:

1 - Tax Liability

Marketing activities through influencers are subject to income tax in the status of "advertising", that is, "commercial activity", because they aim to gain popularity to a brand, a service or a product by using the popularity of influencers with high followers. With the "Communiqué on the Amendment of the General Implementation Communiqué on Value Added Tax" (**"Communiqué"**) published in the Official Gazette dated 16.02.2021 and numbered 31397, it has been regulated that the VAT withholding application shall be started by

the Advertising Agencies or by the commercial advertising service providers. The aforementioned Communiqué entered into force in March. In accordance with the VAT withholding practice, if a customer purchases a commercial advertisement service, he / she shall pay the service provider company, not the whole but part of the VAT on the invoice issued by the company and pay the rest to the state on behalf of that company. Finally, if these earnings are not taxed at all, both brands and social media celebrities could face massive sanctions.

2 - Collaboration Problem

Advertising via Influencer has the characteristics of "commercial advertisement" within the scope of Article 61 of the Law on the Protection of the Consumer. Influencers on social media often state that they use a product and are satisfied, and market the product as "covert advertising". However, in reality, a fee was taken for this sharing and the influencer got an act in return for this veiled advertisement. This situation is regulated within the scope of Article 61 of the Law on the Protection of the Consumer and it is illegal and prohibited.

In such sharing, if the purpose is to actually advertise, the phrase "ad content" or "collaboration" should be included in a way that can be easily seen by everyone. In case of violation of the above-mentioned rules, an administrative fine of 114,326.00 TL shall be imposed in 2021.

3 - In Terms of Competition Law

Every influencer who posts from social media channels must act in accordance with the "Commercial Advertising and Unfair Commercial Practices Regulation" ("**Regulation**") published in the Official Gazette dated 10.01.2015 and numbered 29232. In order to be within the scope of the regulation, in particular, the purchase links of the products and services shall be shared, the notifications directing the purchase shall be made and a "consumer perception" shall be created.

In order to comply with the prohibition of non-competition, it is necessary to include the phrase "advertising content" or "collaboration" in such posts.

Another issue prohibited by the regulation is unfair commercial practices. Unfair commercial applications may also be realized with the Influencer marketing technique.

04 - Financial Crimes Investigation Board Published the Crypto Asset Service Providers Guide

Within the framework of the Regulation on the Amendment of the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism which entered into force through the Presidential Decision dated 30.04.2021 and numbered 3941 published in the Official Gazette dated 01.05.2021 and numbered 31471, the crypto asset service providers have been specified among the "Obliged Parties" stated under the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Regulation**").

Following entering into force of the Regulation, the Financial Crimes Investigation Board ("**MASAK**") published the guide titled the Main Principles for the Crypto Asset Service Providers Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Guide**") on 04.05.2021.

The Guide firstly provides brief explanations regarding the activities of MASAK, and the crimes of laundering proceeds of crime and financing of terrorism. As for the definition of crypto asset, the Guide refers to the Regulation Prohibiting Payments Through Crypto Assets, which is published in the Official Gazette dated 16.04.2021 and numbered 31456 and entered into force on 30.04.2021. The Guide defines the activities of the crypto asset service providers as "the mediation regarding the trading of the crypto assets through electronic transaction platforms".

The Guide also provides detailed and instructive application-oriented information regarding the obligations that the crypto asset service providers have under the Regulation as obliged parties which are,

- Know your customer (especially the identification of natural persons and legal persons, identification in subsequent transactions, and remote identification),
- Suspicious transaction reporting,
- Providing information and documents,
- Regular reporting, and
- Retaining and submission.

The Guide includes information on the administrative and legal sanctions to be imposed in the case of failing to fulfill the obligations that the crypto asset service providers have as obligated parties under the Regulation. Accordingly, failing to fulfill the obligation of know your customer, the obligation of suspicious transaction reporting, and the obligation of regular reporting causes administrative fines to be issued by MASAK under the Law No 5549 On Prevention of Laundering Proceeds of Crime (**"Law no 5549"**). Moreover, failing to fulfill the obligation of not to disclose any information on the suspicious transaction reporting to parties except for the auditors assigned for auditing of obligations and for the courts during trial, the obligation of providing information and documents, and the obligation of retaining and submission causes the sanctions of imprisonment and legal fines under the Law no 5549; whereas security measures are imposed on the legal persons.

The Guide also provides certain detailed examples of suspicious transaction types and draft forms to be used for the suspicious transaction reporting.

05 - The Report On Competition And Data Protection In Digital Markets: A Joint Statement Between The Cma And The Ico (''The Report'') Has Been Published

The Report on "Competition and Data Protection in Digital Markets: a joint statement between the CMA and the ICO" (**"the Report"**) has been published by UK Competition and Markets Authority (**"CMA"**) on 19.05.2021. The Report sets out how to enhance the synergies between the policy agendas and, where to identify the potential for tensions, explains how to address them. The Report focuses on three different views that are: highlighting the interactions between competition and data protection in the digital economy synergies and potential tensions between these policy areas; how the two organizations (CMA and Information Commissioner's Office (**"ICO"**)) are working together to maximize regulatory coherence concerning the use of personal data in digital advertising; understanding and promoting outcomes in the digital economy that simultaneously promote competition and enhance data protection and privacy rights. Highlights of the Report are as follows:

1 - Synergies and tensions between the aims of competition and data protection

The Report highlights the synergies between United Kingdom's respective regimes before recognizing where challenges might occur.

The Report believe that there are strong synergies between competition and data protection objectives, and that many regulatory interventions in digital markets can be designed in a way that supports both objectives. These synergies can be considered under three main categories: user choice and control; standards and regulations to protect privacy; and data-related interventions to promote competition

2 - The role of clear regulation and standards to protect privacy and ensure effective competition

The Report highlights the importance of recognizing as a point of principle that data protection law and competition law complement each other in respect of achieving efficient market outcomes that involve processing personal data.

According to the Report, it is achieved by ensuring that competitive pressures help drive innovations that genuinely benefit users, rather than encouraging behavior that undermines data protection and privacy rights.

Lastly, the Report states that regulation and standards regarding the processing of personal data also serve to maintain a level playing field between competing businesses, the interests of both competition and data protection are strongly aligned.

3 - Data-related interventions to promote competition

According to the Report, data-related interventions to promote competition can be achieved through restricting access to data, or limiting the ability to combine and integrate datasets, for platforms with market power, in order to create a level playing field with other market participants.

However, it is important to pay attention to the potential efficiency costs of restricting the ability of companies to combine datasets, such interventions could in principle deliver strong synergies between the interests of competition and data protection, since they involve restricting the ability to combine and process personal data, at the same time as creating a more level playing field for all businesses to compete fairly.

4 - Outcomes:

Summary of the shared views stated by the Report are as follows:

- Choice architecture and default settings are designed in a way that reflects users' interests;
- Users have more control over their personal data and can make meaningful decisions over whether to withhold access to it or share it with others;
- Users have a real choice over platform and service providers, and can easily switch if they prefer the content, functionality, or data protection approach of an alternative provider;
- Providers of digital services are able to compete with one another by recognizing privacy as an important aspect of quality, or alternatively by offering greater benefits to those users that permit and are comfortable with greater collection of their personal data;
- Platforms are incentivized to innovate and develop new ways to deliver advertising that meets the targeting needs of advertisers using fewer personal data, thus protecting users' privacy to a greater extent.

06 - The Draft Regulation on Remote Identification Methods and Establishment of Contractual Relations in Electronic Environment to be Used by Financial Leasing, Factoring, Financing and Saving Financing Companies Has Been Published

The Draft Regulation on Remote Identification Methods and Establishment of Contractual Relations in Electronic Environment to be Used by Financial Leasing, Factoring, Financing and Saving Financing Companies, (**"Draft Regulation"**) has been drafted by the Banking Regulation and Supervision Agency (**"Authority"**). The Draft Regulation has been published on the official website of the Authority on 07.05.2021. The Draft Regulation regulates the procedures and principles for the establishment of a contractual relationship over an informatics or electronic communication device, or as a replacement for the written form or at a distance, which is intended to be used in remote identification methods that may be used by Financial Leasing, Factoring, Financing and Saving Financing Companies to gain new customers and services to be offered after the identification of the customer, whether it is distant or not. The procedures and principles regulated via the Draft Regulation are as follows:

1 - General principles to be followed before the process is initiated

Remote identification takes place in the form of online video calls and communication with each other, without the need for the customer representative and the person to be physically in the same environment.

The process shall be initiated by the person, continued with the controls applied by information technologies, and completed with the approval and additional controls to be made by the customer representative.

The remote identification process shall be reviewed at least twice a year and updates should be made to improve the process when necessary.

2 - Customer representative for remote identification and working environment

The video call phase of remote identification will be carried out by a trained customer representative. The customer representative is required to receive the necessary training, including the legislation on the protection of personal data, at least once a year after each update for remote identification methods.

In order to give assurance to the person, a suitable environment should be created to reflect that the customer representative is working on behalf of the company.

3 - General principles to be followed with the initiation of the process

In the remote identity verification process, before the video call starts, an application is received via a form that the person shall fill in electronically and through the company application where the remote identification process is operated. Risk assessment is carried out regarding the person by using the data obtained with the form. In the remote identification process to be applied within the scope of the Regulation, only biometric data can be used within the framework of the customer's special categories of personal data.

It is possible to use the relevant data electronically by obtaining the explicit consent of the customer. The entire remote identification process shall be recorded and stored in a way that includes all steps of the process and makes it auditable. In the event of an objection in transactions that cause liability to individuals or a third party, the burden of proof lies with the company.

In order for the contract to be established, whether it is distant or not, all the terms of the contract must be conveyed to the customer through internet or mobile service channels in a way that the customer may read, the customer must receive the declaration of intention for the establishment of the contract and the customer must sign the contract conveyed to him/her.

In the event that the contract is established electronically or the customer's declaration of intention to establish the contract is established at a distance following the identification during the video call phase, it is accepted that the written form requirement for contracts is fulfilled.

June

01 **Privacy Guideline in Digital Games Has Been Published.**

02 **Personal Data Protection Authority Rendered a Decision Regarding an Insurance Company Giving Service Conditional on Explicit Consent.**

03 **Personal Data Protection Authority Rendered a Decision on a Hospital's Data Breach Notice.**

04 **The Personal Data Protection Board Decision on the Obligation to Register with the Data Controllers' Registry for Economic Enterprises Belonging to Foundations, Associations and Trade-Unions Has Been Published in the Official Gazette.**

05 **The Personal Data Protection Authority Published an Announcement on the Obligation of Business Partnerships to Register with the Data Controller Information System.**

06 **Personal Data Protection Board Rendered a Decision Regarding the Data Controller Taking Additional Measures.**

01 - Privacy Guideline in Digital Games Has Been Published

It was announced that the "Guideline to Privacy in Digital Games" (**"The Guideline"**) drafted by the Information Technologies and Communications Authority (**"Authority"**) was published on the official website of the Authority on 01.06.2021. The guideline provides information on the current state of digital games, what digital privacy is, how to protect against threats in digital games, threats in online games, and what cyber-bullying is. Some of the key issues organized by the Guideline are as follows:

1 - Privacy

With the Guideline, the definition of the concept of Digital Privacy has been made. Accordingly, Digital Privacy refers to how people shall behave in digital environments, which data shall be shared with whom and which shall not. The Guideline covers the contents such as Personal file, photo, video, real identity information, account, bank information, address information, etc.

2 - Risks to be Encountered in Digital Games

- Risks arising from communication with people who want to steal personal and financial information,
- Risks caused by malicious people who want to take advantage of computer security vulnerabilities,
- Risks posed by criminals seeking victims on the Internet and in the real world,
- Risks posed by Trojan horses, computer worms, spyware and viruses.

3 - Methods of Protection from Digital Damages

In order not to be the target of cyber attacks in digital games and not to deal with the consequences, it is recommended to use methods such as using anti-virus programs and downloading games from safe sources, to choose reliable platforms and content producers when acquiring games from digital media, and to ensure that the information requested on digital platforms does not contain information that can be used against you or your close environment outside that platform, not sharing the passwords requested for the game with third parties, even if the game manufacturer gives confidence

02 - Personal Data Protection Authority Rendered a Decision Regarding an Insurance Company Giving Service Conditional on Explicit Consent

The Personal Data Protection Board (**"Board"**) rendered a decision dated 20.04.2020 and numbered 2021/389 (**"Decision"**) regarding an insurance company (**"Data Controller"**), based on the fact that the insurance company provided its services with the condition of explicit consent.

Pursuant to the Decision, it is stated by the data subject that an individual pension contract was issued by the subject insurance company for the data subject, the data subject was obliged to consent to the processing of personal data by being presented with a confirmation box while trying to access the insurance policy information on the website of the insurance company, and taking any action without filling the confirmation box was not possible. For these reasons, the data subject has notified the insurance company to the Personal Data Protection Authority (**"Notice"**).

As a result of the Notice, the Board made the following evaluations:

- Personal data processing activities by the Data Controller must be carried out in accordance with the Communiqué on Principles and Procedures to be Followed in Fulfillment of the Obligation to Inform (**"Communiqué"**);
- When the privacy notices provided in the separate links on the website of the Data Controller are examined, it is determined that the texts are identical;
- There is no information in the privacy notice regarding which of the Article 5 or Article 6 of the Personal Data Protection Law numbered 6698 (**"PDPL"**) should be based on as a legal reason;
- The legislation under which the personal data is transferred should be clearly and separately stated in the privacy notice, and the privacy notice should be kept up to date;
- In cases where the legal reason for the processing of personal data is explicit consent, the obligation to inform and obtaining explicit consent should be fulfilled separately and a separate explicit consent text should be formed;
- It should be clearly stated on which subject the express consent declaration is requested by the Data Controller, the data subject should be aware of his/her behavior, and it should be his/her own decision, and in this context, the provision of the service should not be conditional on the explicit consent of the data subject;

- In the cases where the parties are not in an equal position or one of the parties has influence over the other, then it should be carefully evaluated whether the consent is given freely or not;
- In the event that one of the conditions clearly stipulated in the law exists, then it is possible to process personal data without seeking the explicit consent of the data subject;
- If it is possible to carry out the data processing activity on a basis other than explicit consent, basing it on explicit consent would be deceptive and abuse of rights, and this would be contrary to the principle of "compliance with the law and good faith" regulated within the PDPL.

In the light of its evaluations, the Board decided that if there are other processing conditions present which are mentioned in the Article 5 of the PDPL, then it is against the principle of "compliance with the law and good faith" stated under Article 4 of the PDPL to request the explicit consent of the data subject; and taking into consideration that the Data Controller has a large customer base in terms of the service provided, the faults of the Data Controller, its economic situation and the content of injustice, an administrative fine of TRY 250.000,- shall be imposed on the Data Controller who did not fulfill its obligations under paragraph 1 of Article 12 of the PDPL. The Board further decided to instruct the Data Controller to regulate the explicit consent and privacy notice presented to the data subjects separately, and to revise the same in order the texts not to include ambiguous expressions and to harmonize them with the provisions of the PDPL and the Communiqué, and to inform the Board accordingly.

03 - Personal Data Protection Authority Rendered a Decision on a Hospital's Data Breach Notice

The Personal Data Protection Board (**"Board"**) rendered a decision dated 20.04.2021 and numbered 2021/407 (**"Decision"**) regarding the data breach notice of a data controller hospital (**"Data Controller"**).

In the Decision, within the scope of the data breach notice submitted by the Data Controller, it was stated that (i) the breach was carried out with the instruction of the physician working in the hospital, by removing the files of the patients out of the hospital by the hospital staff; (ii) the employee who attempted to extract the file was detected 17 days after it was videotaped; (iii) all but one of the employees involved in the breach was given a training on protection of personal data prior to occurrence of the data breach; (iv) the Personal Data Protection Authority (**"Authority"**) was notified to the Board 25 days after the breach occurred, due to the reasons included in the breach notification regarding late notification.

The Board detected the following after evaluating the breach notice submitted by the Data Controller:

- The data breach occurred when the bags containing the personal data and special categories of personal data belonging to the patients of the physician working in the hospital were taken out of the hospital by some hospital staff, upon the physician's instruction;
- Sufficient administrative measures have not been taken to ensure data security, since unauthorized persons could enter the archive room where patients' records were kept, and those persons could remove personal data and special categories of personal data of patients from the archive without permission;
- Of the 789 lost patient files, only 54 were retrieved and the fate of the others were unknown, indicating that the measures to reduce the risks for the loss of files were not sufficient;
- Employees were not given any or adequate training on the protection of personal data;
- The fact that the breach was detected 17 days after its occurrence showed that the Data Controller did not prepare or follow the personal data security policies and procedures well, and also failed to use the existing security measures in the hospital effectively;
- The breach was reported to the Authority 25 days after its detection;
- The breach was not reported to any of the data subjects, except for one person who visited the hospital.

In the light of the detections it has made, the Board imposed an administrative fine of TRY 450,000,- on the Data Controller on the grounds that the Data Controller did not take the measures to ensure the data security stipulated in Article 12, paragraph 1 of the Personal Data Protection Law numbered 6698 ("**PDPL**"); again, considering that the Data Controller has not fulfilled the 72-hour notification obligation specified in Article 12, paragraph 5 of the PDPL and the decision of the Board numbered 2019/10 on the Personal Data Breach Notification Procedures and Principles, and bearing in mind the unfair content of the misdemeanours committed by the Data Controller, the fault of the data controller and its economic situation, the Board decided to impose a further administrative fine of TRY 150.000,- on the Data Controller.

04 - The Personal Data Protection Board Decision on the Obligation to Register with the Data Controllers' Registry for Economic Enterprises Belonging to Foundations, Associations and Trade-Unions Has Been Published in the Official Gazette

The Personal Data Protection Board Decision No. 2021/571 and dated 09/06/2021 on the Obligation to Register Economic Enterprises Belonging to the Data Controllers Registry of Foundations, Associations and Trade-Unions has been published in the Official Gazette dated 24 June 2021.

Pursuant to the Decision of the Personal Data Protection Board ("**Board**") dated 22/04/2020 and numbered 2020/315 and the amended Decision dated 02/04/2018 and numbered 2018/32, it has been provided exception to "associations, foundations and trade-unions established in Turkey that process personal data only in accordance with the relevant legislation and purposes, limited to their fields of activity".

Afterwards, it was stated that there were hesitations regarding the registration obligation of economic enterprises belonging to foundations, associations or trade-unions in some written requests for opinion conveyed to the Authority, aAnd as a result of the evaluation, the exceptions have been amended. In this context, it has been decided that:

1. The expression "associations, foundations and trade-unions established in Turkey that process personal data only in accordance with the relevant legislation and purposes, limited to their fields of activity" in the Decision dated 22/04/2020 and numbered 2020/315 and the amended Decision dated 02/04/2018 and numbered 2018/32" has been amended to "associations, foundations and trade-unions established in Turkey that process personal data only in accordance with the relevant legislation and purposes, limited to their field of activity, that do not have any economic enterprises affiliated to them".
2. Those associations, foundations and trade-unions established in Turkey, that process personal data only in accordance with the relevant legislation and purposes, limited to their fields of activity, that have any economic enterprises affiliated to them, shall register in the Registry, and during their registration with the Registry, information about the activities of economic enterprises should be entered only.

05 - The Personal Data Protection Authority Published an Announcement on the Obligation of Business Partnerships to Register with the Data Controller Information System

Within the framework of the announcement (“**Announcement**”) published on the website of the Personal Data Protection Authority (“**Authority**”) on 25.06.2021, it is stated that there were hesitations in the opinion requests delivered to the Authority, about the registration obligations of business partnerships, consortia and ordinary partnerships in the Data Controllers’ Registry (“**Registry**”).

Pursuant to the Announcement, the main purpose of the obligation to register with the Registry is to carry out the personal data processing processes in a transparent and accountable manner and to provide the highest level of control over the personal data of the data subjects.

In this extend, the Authority stated the importance of reflecting the personal data processed during the activities carried out by structures such as business partnerships, consortia and ordinary partnerships to the Data Controllers’ Registry Information System (“**VERBIS**”).

In the light of this information, the Authority announced that the Personal Data Protection Board rendered a decision dated 09.06.2021 and numbered 2021/569, stating that “the partners forming the partnership, who are obliged to register with the Registry, should also input data regarding the personal data they process within the scope of the partnership activities, along with their own activities, during their registration to VERBIS”.

06 - Personal Data Protection Board Rendered a Decision Regarding the Data Controller Taking Additional Measures

Personal Data Protection Board ("**Board**") rendered a decision dated 06.05.2021 and numbered 2021/470 ("**Decision**") regarding the unredeemed access request of a data subject working in a data controller company ("**Data Subject**") to the employer Data Controller ("**Data Controller**"), for the access to personal data regarding meal card account activities.

Pursuant to the Decision, the Data Subject requested from the Data Controller to be forwarded the account movements of the meal card allocated to him/her by the Data Controller. In order to provide the requested information to the Data Subject, the Data Controller has requested certain information to verify the identity of the Data Subject. Due to the Data Subject's request to have her/his personal data sent to the e-mail address with the extension gmail.com, the infrastructure of which is abroad, by making a risk assessment, within the framework of additional security measures the Data Controller stated that the phone number sent to the e-mail address with the @gmail.com extension is required to be called to access the aforesaid data. The Data Subject has applied for complaint ("**Complaint**") to the Personal Data Protection Authority ("**Authority**") on the grounds that the additional security measure introduced is contrary to the law and access to her/his personal data is prevented.

The Board evaluated as follows regarding the request received by the Authority:

- Within the framework of Article 11 of the Personal Data Protection Law numbered 6698 ("**PDPL**") the Data Subject has the right to request information about herself/himself and to access personal data, and these rights allow the Data Subject to be informed about how her/his personal data is processed;
- Pursuant to Article 12 of the PDPL, the Data Controller must take all necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of personal data, unlawful access to personal data and to ensure the storage of personal data;
- Within the scope of the Communique on the Principles and Procedures for the Request to Data Controller ("**Communique**"), the Data Controller is obliged to take all technical and administrative measures necessary in order to conclude the application to be made by the Data Subject effectively, in accordance with the rule of law and good faith;

- Within the framework of the technical and administrative measures included in the Guideline on Personal Data Security, the Data Controller shall correctly determine the possibility of the risks that may arise regarding the protection of personal data and the losses to be caused in case of the occurrence of the risks and take appropriate measures;
- While not preventing the Data Subject from accessing her/his personal data, the Data Controller stated that she/he sent the file requested by the Data Subject to her/his e-mail address in an encrypted manner in order not to cause a disproportionate burden to the Data Subject and that this password shall immediately be shared with the Data Subject when called with the phone number included in the subject e-mail;
- As stated by the Board in its Decision dated 31.05.2019 and numbered 2019/157, in case of using the g-mail.com service, the infrastructure of which is abroad, the Data Controller's sending of the file containing the personal data by encrypting shall have the purpose of providing high level of security and;
- Pursuant to Article 12 of the PDLP, these additional security measures taken by the Data Controller to prevent unlawful access to personal data of the Data Subject are not in violation of the PDPL, but the meticulous implementation of the PDPL.
- In the light of its evaluations, the Board decided as follows:

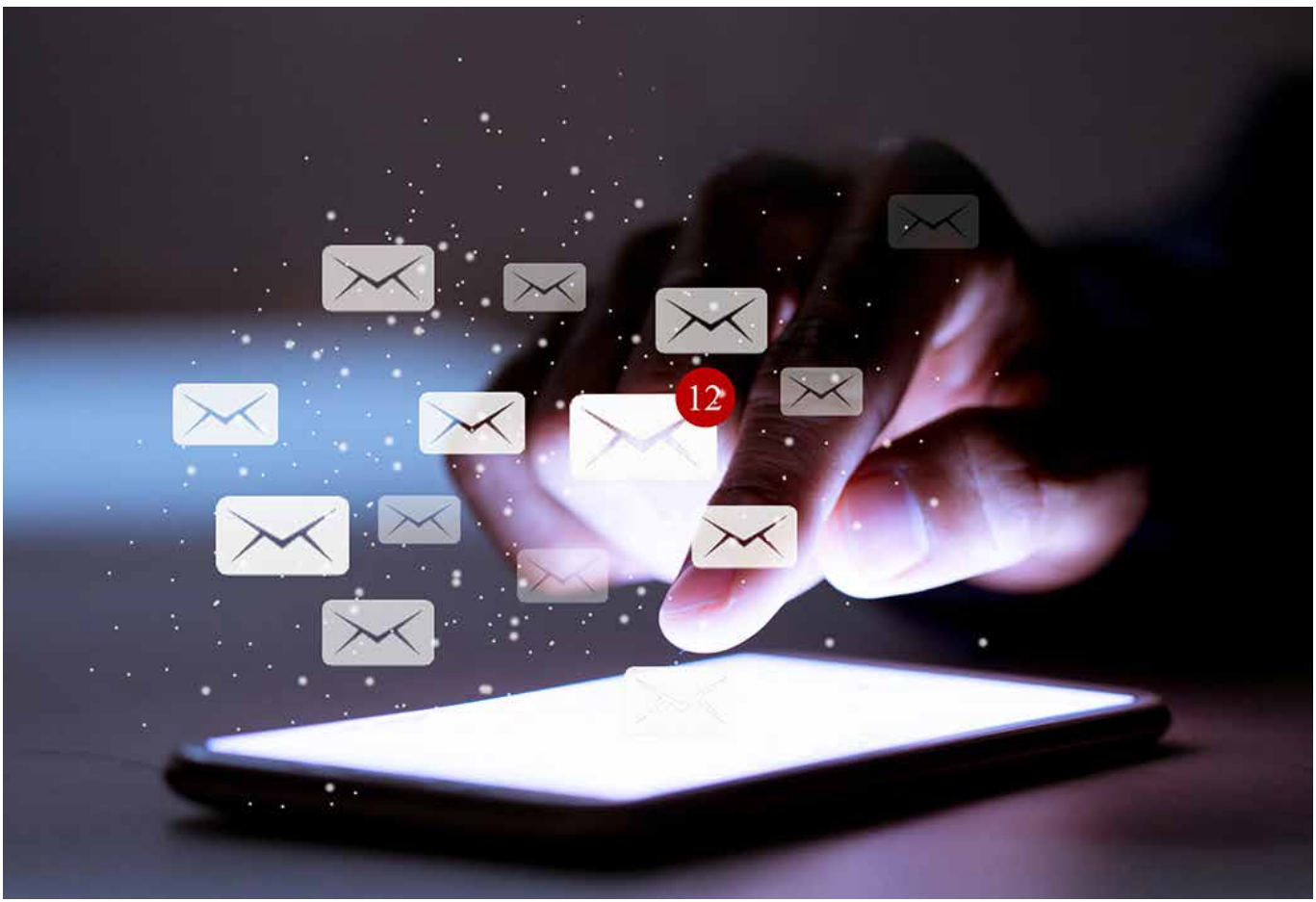
Pursuant to subparagraph (b) of paragraph 1 of Article 12 of the PDPL, the precautions taken by the Data Controller in order to fulfill the obligation to take all technical and administrative measures to ensure the appropriate level of security in order to prevent unlawful access to personal data are reasonable; the necessary explanation regarding the security measure taken is made to the Data Subject and therefore the Data Subject's right of access to personal data is not prevented; and thus there is no action to be taken against the Data Controller within the scope of PDPL.

July

01 **The Regulation On The Applicant's Identity Verification Process In The Electronic Communications Sector Has Been Published In The Official Gazette.**

01 - The Regulation on the Applicant's Identity Verification Process in the Electronic Communications Sector Has Been Published in the Official Gazette

"The Regulation on the Applicant's Identity Verification Process in the Electronic Communications Sector" ("**Regulation**") has been published by the Information Technology and Communication Agency in the Official Gazette dated 26.06.2021 and numbered 31523. The Regulation regulates the procedures and principles regarding the process to be applied for the verification of the applicant's identity in case of electronic documentation of the following issues: subscription contract, GSM number porting application, qualified electronic certificate application, registered e-mail application and SIM change application in the electronic communication sector. The regulation entered into force on 31.12.2021.



August

01 The Communiqué On International Bank Account Number Has Been Published.

02 The Regulation On The Reconciliation Procedure Applicable In Investigations Regarding Anti-Competitive Agreements, Harmonious Act And Decisions, And Abuse Of Dominance Has Been Published In The Official Gazette.

03 The Amendments Have Been Made In The Decision Regarding Taking Regulatory Measures On Some Issues Regarding User Rights In The Postal Industry.

04 The Presidential Circular On The National Artificial Intelligence Strategy Has Been Published İn The Official Gazette.

05 The National Artificial Intelligence Strategy, Co-Developed With The Presidency Of The Digital Transformation Office And The Ministry Of Industry And Technology Has Been Published.

06 Terms And Interdiction Imposed On Digital Banks

01 - The Communiqué on International Bank Account Number Has Been Published

The "Communiqué on the International Bank Account Number" ("**Communiqué**") has been published by the Central Bank of the Republic of Turkey in the Official Gazette dated 05.08.2021 and numbered 31559. Within the scope of the Communiqué, the amendments have been made to the Communiqué on International Bank Account Number (Number: 2008/6) published in the Official Gazette dated 10/10/2008 and numbered 27020. The purpose of this Communiqué is to determine the principles and procedures regarding the application of the international bank account number by the payment service providers:

1 - <u>The Definition of Payment Service Provider</u>

The definition of payment service provider has been added to the first paragraph of Article 3 of the Communiqué:

"(e) Payment service provider: Institutions listed in the first paragraph of Article 13 of the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions dated 20/6/2013 and numbered 6493,"

In addition, the phrase “Bank Code” in Annex 1 of the Communiqué has been amended to “Payment Service Provider Code” and the phrase “bank codes” has been amended to “codes”.

2 - The Structure and Creation of IBAN

By amending the fourth article of article 4 of the Communiqué, it is stipulated that the payment service provider codes to be used while creating the IBAN would be determined by the Central Bank of the Republic of Turkey.

Payment service providers other than banks can also create IBANs for customer accounts subject to money transfer; It is not obligatory for payment service providers other than banks to create an IBAN for customer accounts subject to money transfer, unless there is a contrary provision in the system rules of the payment system they participate as a participant within the scope of Law No. 6493.

3 - Displaying the IBAN

It is obligatory that, payment service providers that create an IBAN are required to show the IBAN in the documents that they would create for their customers regarding the accounts subject to money transfer in written and electronic form, and on the documents containing the account number.

4 - Use and Verification of IBAN

It is obligatory to verify and use the recipient’s IBAN for money transfers to accounts in countries in the European Economic Area. However, this obligation is not sought in transactions between payment service providers and financial institutions that make cross-border payments abroad, and transactions where the customer’s declaration is received that the IBAN of the recipient would not be reported despite the request.

In summary, it is aimed to determine the issues related to the implementation of the international bank account number by the payment service providers

02 - The Regulation on the Reconciliation Procedure Applicable in Investigations Regarding Anti-Competitive Agreements, Harmonious Act and Decisions, and Abuse of Dominance Has Been Published in the Official Gazette

"The Regulation on the Reconciliation Procedure Applicable in Investigations Regarding Anti-Competitive Agreements, Harmonious Act and Decisions, and Abuse of Dominance" ("**Regulation**") has been published by the Competition Authority ("**Authority**") in the Official Gazette dated 15.07.2021 and numbered 31542.

The Regulation regulates pursuant to Article 43 of the Law No 4054 on the Protection of Competition ("Law"); the procedures and principles regarding the process to be applied for the reconciliation for those who accept the existence and scope of the violation among the undertakings, or the associations of undertakings; about which an investigation has initiated regarding the prohibited actions in the Articles 4 and 6 of the Law. The regulation had entered into force on the date of its publication.

The procedures and principles regulated by the Regulation are as followings:

1 - <u>Procedure for Initiating Reconciliation Negotiations</u>

The reconciliation procedure is either ex officio initiated by the Board of the Competition Board ("**Board**") after the commencement of the investigation and then the parties are invited to the reconciliation negotiations; or the parties agree to initiate reconciliation negotiations and after, the Board accept the request. Upon the acceptance, the Competition Authority ("**Authority**") initiates reconciliation negotiations as soon as possible.

2 - General Principles Regarding Reconciliation Negotiations

- Acceptance of the reconciliation negotiations does not mean the parties have accepted the violation.
- Parties may withdraw the process until the submission of reconciliation text.
- If there is more than one reconciliation party, it is essential that these negotiations to be held separately.
- The negotiations are recorded by official report and this report is kept as internal correspondence in the Authority.
- Parties can get information about the content of the claim, the nature and scope of the violation, the main evidence that constitutes the basis of the violation (provided that it does not include any trade secrets), the range of administrative fines and the discount that may be applied to the fine as a result of the reconciliation; all provided that the security of the investigation is not compromised.
- The parties of the reconciliation have the obligation to keep the information and documents confidential, that they have accessed within the scope of the negotiations until the final decision.

3 - Interim Decision of Reconciliation and Reconciliation Text

Following the completion of reconciliation negotiations, the Board make an interim decision determining the scope and nature of the violation, the maximum penalty that can be imposed, the rate of reduction that can be made, and precise the time period to send the text to the Authority. Issued in the interim decision cannot be discussed. When the reconciliation party accepts the interim decision, it presents the reconciliation text by adding additional provisions foreseen in the Article 8 of the Regulation. Administrative fines and reconciliation text cannot be subject to a lawsuit. The reconciliation text is kept as internal correspondence in the Authority.

4 - Final Decision

The final decision regarding the administrative fine and the determination of violation is made by the Board, within 15 days after entrance of the reconciliation text to the Authority's records.

Briefly, by this Regulation, it is purposed to determine the procedures and principles to be followed in the reconciliation and in the reconciliation negotiations, when the alleged violations have been accepted by the parties in the investigations opened regarding the prohibited actions in the Law. The regulation had entered into force on the date of its publication.

03 - The Amendments Have Been Made in the Decision Regarding Taking Regulatory Measures on Some Issues Regarding User Rights in the Postal Industry

It was decided to amend the Decision on Taking Regulatory Measures on Some Issues Regarding User Rights in the Postal Sector, dated 23.09.2019 and numbered 2019/DK-SRD/206, via the Decision of the Information Technologies and Communication Board (**"Board"**), dated 03.08.2021 and numbered 2021/DK-SRD/212.

Within this scope;

It has been added as follows to come after the first article of the Board Decision dated 23.09.2019 and numbered 2019/DK-SRD/206:

"To be able to digitally issue the documents proving the service delivery within the knowledge and approval of the sender; to share the said documents and necessary informational texts with users (sender and recipient) via SMS, website link or similar methods, to provide this opportunity to the users, if the said document is physically requested"

04 - The Presidential Circular On The National Artificial Intelligence Strategy Has Been Published In The Official Gazette!

"The Presidential Circular on the National Artificial Intelligence Strategy", ("**Circular**") has been drafted by the Presidency of Digital Transformation Office and the Ministry of Industry and Technology has been published in the Official Gazette dated 20.08.2021 and numbered 31574.

In this respect, it was announced that "National Artificial Intelligence Strategy (2021-2025)" has been drafted by the Presidency of the Digital Transformation Office and the Ministry of Industry and Technology in cooperation with the public, private sector, non-governmental organizations and universities, and the "National Artificial Intelligence Strategy Steering Committee" ("**Steering Committee**") has been established under the chairmanship of the Vice President with the participation of the President of Digital Transformation Office and the relevant Deputy Minister of the Ministry of Industry and Technology; in order to further the activities that Turkey will carry out in the field of artificial intelligence until 2025, to determine the strategic priorities, goals, targets and measures in this field and to implement them.

The objectives and procedures of the Steering Committee drafted by the Circular are as follows:

1 - Objectives of the Committee;

- Effective execution of activities to be carried out within the framework of national policies for the production and dissemination of artificial intelligence technologies
- High-level monitor the strategy and manage the processes in the Strategy Document
- Provide the necessary coordination

2 - Procedures regarding the Committee;

- The Steering Committee will meet at least once every three months,
- It shall meet separately upon invitation,
- Secretariat services will be carried out jointly by the Presidency of Digital Transformation Office and the Deputy Minister of Industry and Technology.

In order to assist the activities of the Committee; sub-committees, technical committees, advisory and working groups may be organized. Relevant public institutions and organizations as well as universities, non-governmental representatives, professional associations and private sector representatives can be invited to the Committee meetings; they will be able to take part in sub-committees, committees, advisory and working groups.

In summary, the details regarding the National Artificial Intelligence Strategy and the National Artificial Intelligence Strategy Steering Committee, which will execute this document, were determined via the Circular.

05 - The National Artificial Intelligence Strategy, co-developed with the Presidency of the Digital Transformation Office and the Ministry of Industry and Technology Has Been Published

"National Artificial Intelligence Strategy 2021-2025", which was drafted in cooperation with the Digital Transformation Office of the Presidency of the Republic of Turkey and the Ministry of Industry and Technology announced on 24.08.2021. With the publication of the National Artificial Intelligence Strategy (**"NAIS"**), which is the first national strategy document of our country on artificial intelligence (**"AI"**), Turkey has taken its place among the countries that have an AI strategy. NAIS was drafted as per the Eleventh Development Plan and Presidential Annual Programs, in line with the "Digital Turkey" vision and the "National Technology Initiative". In this regard, the vision of NAIS has been determined as "creating value on a global scale with an agile and sustainable AI ecosystem for a prosperous Turkey".

The Strategy was designed around 6 strategic priorities. These priorities are as follows:

- Training AI experts and increasing employment in the domain
- Supporting research, entrepreneurship, and innovation
- Facilitating access to quality data and technical infrastructure
- Regulating to accelerate socioeconomic adaptation
- Strengthening international cooperation
- Accelerating structural and labor transformation

Within the scope of these strategic priorities, 24 objectives and 119 measures were determined.

The high-level targets to be achieved in 2025, the end of the implementation period of the NAIS, are as follows:

- The share of AI in its GDP will be increased to 5%.
- Employment in the field of artificial intelligence is to be increased to 50,000.
- Employment in the field of artificial intelligence in central and local public institutions, and organizations shall be increased to 1,000 persons.
- The number of graduates in the field of AI will be increased to 10,000.
- AI application developed by the local ecosystem will be prioritized in public procurement and commercialization will be supported.

- The number of graduates in the field of AI will be increased to 10,000.
- AI application developed by the local ecosystem will be prioritized in public procurement and commercialization will be supported.
- Active contribution will be made to the regulatory studies and standardization processes of international organizations in the field of reliable and responsible AI and cross-border data exchange.
- It will be ensured that Turkey is among the top 20 countries in the rankings of international artificial intelligence indices

The Artificial Intelligence principles adopted within the scope of these goals are as follows:

- Proportionality
- Safety and Security
- Fairness
- Privacy
- Transparency and Explainability
- Responsibility and Accountability
- Data Sovereignty
- Multi- Stakeholder Governance

In summary, the roadmap for work on the field of artificial intelligence until 2025 has been determined by the Strategy Document. Implementation process of the Strategy that will be coordinated by the "Steering Committee", will be chaired by the Vice President. The governance mechanism embraces AI Ecosystem Advisory Group and working groups as well, where all relevant stakeholders will be represented.

06 - Terms and Interdiction İmposed On Digital Banks

"The Draft Regulation on Operating Principles of Digital Bank and Service Model Banking ", ("**Draft Regulation**") has been drafted by the Banking Regulation and Supervision Agency ("**BDDK**") and has been published in the Official Website (www.bddk.org.tr) on 19.08.2021. The Draft Regulation regulates the conditions for providing the operating principles and banking services of branchless banks, which only serve through digital channels, as a service model to demanding businesses and innovative enterprises in order to encourage financial innovation in the banking sector, increase financial inclusion and facilitate access to banking services.

The terms regulated with the Draft Regulation are as follows:

Terms and Interdiction İmposed On Digital Banks

- Activity Interdictions;
- Customers of digital banks will only consist of financial consumers and SMEs.
- The total of unsecured cash loans that digital banks can extend to a certain customer who is a financial consumer cannot exceed 4 times the average monthly net income of the relevant customer.
- The draft regulation also includes provisions against digital banks setting aggressive pricing policies, such as imposing extremely low prices on financing products compared to other banks or imposing excessively high interest rates on deposit products. In addition, digital banks will announce the committed continuity percentage values on the basis of each distribution channel for the electronic banking services they offer, so that they can be seen on the home page of their internet addresses.
- Terms;
- The minimum capital required for the establishment of digital banks will be 1 billion Turkish Liras, and the BRSA can increase this amount.
- Digital banks will be required to set up at least one physical office to handle customer complaints. Units to be established to handle customer complaints will not be used as a branch other than for this purpose.

Principles On Service Model Banking

The service bank can only provide service model banking services to domestically resident interface developers.

In summary, the terms and principles of Digital Banks and Service Model Banking has been determined. Banks other than digital banks that have obtained operating license are not required to make a separate application within the framework of this Regulation in order to transfer their activities to digital.

According to the Draft, Regulation will enter into force as of 1/1/2022.

September

01 **Audio and Video in Civil Procedures**

02 **The Disclosure of Personal Data on a Social Networking Site**

03 **The Access of Lawyers to Enforcement Proceedings of 3rd Parties**

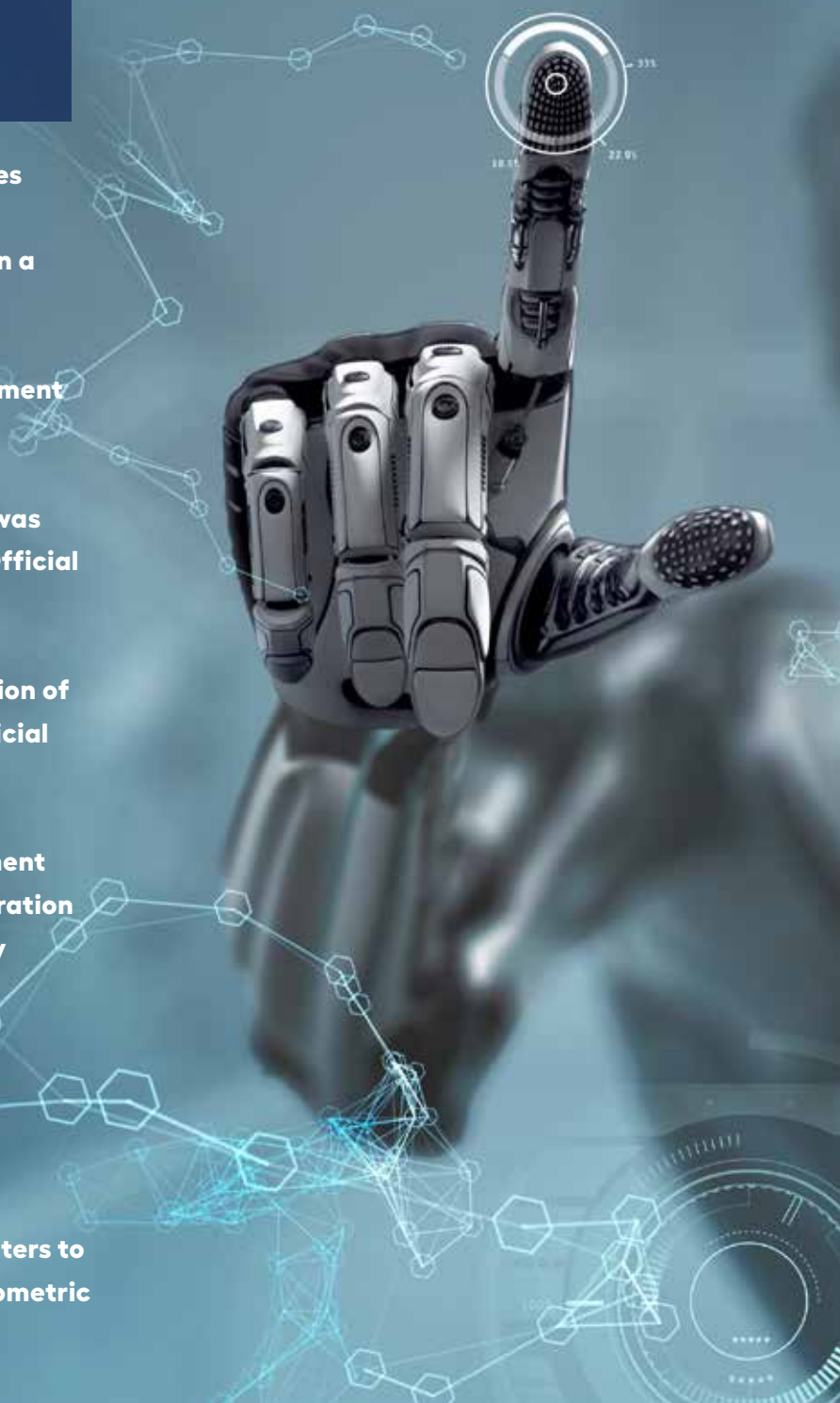
04 **The "Medium-Term Programme" was Approved to be Published in the Official Gazette!**

05 **Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence.**

06 **The Communiqué on the Amendment of the Communique on the Registration of Devices with Electronic Identity Information has been Published in the Official Gazette!**

07 **Digital Turkish Lira Cooperation Platform**

08 **Guiding Principal Decision on Matters to be Considered in Processing of Biometric Data.**



01 - Audio and Video in Civil Procedures

The Regulation on the Execution of Hearings by Transmission of Audio and Video in Civil Procedures Is Published in the Official Gazette.

The Regulation on the Execution of Hearings by Transmission of Audio and Video in Civil Procedures ("**Regulation**") is published in the Official Gazette dated 30.06.2021 and numbered 31527.

The Regulation, which entered into force on 30.06.2021, the date of its publication, based on the 5th paragraph of Article 149 of the Code of Civil Procedure numbered 6100, regulates procedures and principles regarding the participation of the party or attorney and those concerned from their place of residence, through simultaneous audio and video transmission in civil proceedings, in other words, the e-Hearing System.

Pursuant to the Regulation, e-Hearing refers to the "attendance and procedural actions of the party or his/her attorney in the civil proceedings from their place of residence by means of simultaneous transmission of video and audio; allowing the hearing of the witness, expert and other concerned parties" and the e- Hearing System refers to "the system which was established and secured by the Ministry in integration with the National Judiciary Informatics System, in order to carry out hearing procedures by simultaneously transmitting audio and video".

In the implementation of the Regulation, besides the principles of disposition, being brought by the parties, adherence to the request, principles of publicity and procedural economy, the obligation to act honestly and telling the truth, the right to be heard, the ex officio application of Turkish Law, the duty of the judge to enlighten the case, and the principles regarding the conduct and administration of the proceedings, the principles of ensuring information security, protection of personal data, principles of ensuring service quality and ensuring national and international standards are also taken into consideration. In accordance with the Regulation, the safe and simultaneous transmission of video and sound in the e-Hearing System and the video and sound to be of a quality that shall allow the person to be understood visually and audibly are of the essence.

Within the framework of the Regulation, the court may decide to hold the hearing via the e-Hearing System at the request of one of the parties or ex officio. Likewise, the court may decide to hear the witness, expert, or specialist via the e-Hearing System at the request of one of the parties or ex officio. The parties must submit their e-Hearing requests to the court at least two business days before the hearing, and the judge must accept or reject the request at least one business day before the hearing. The judge's decision on the e-Hearing request is final.

The Regulation regulates that the place where the parties shall attend the e-Hearing should be far from all kinds of external factors and should allow them to understand all the visual and auditory expressions of the relevant person and to listen to the relevant person clearly. The court shall identify the attorney of the party participating in the e-Hearing by using secure electronic signature or mobile signature, UYAP (National Judiciary Informatics System) records and similar methods. Identification of the other persons who shall attend the e-Hearing shall be made by issuing a report by the assigned officer at the place allocated for the e-Hearing. In addition, it has been regulated that the identification of the persons who shall attend the e-Hearing from their location due to illness, age or disability shall be made using secure electronic signature or mobile signature.

Pursuant to the Regulation, the e-Hearing is subject to the same procedures and principles as the hearing order held before the court and brings out the same legal consequences. However, declarations of waiver, acceptance, and settlement made through the e-Hearing System which conclude the case shall become valid by being renewed before the court on a new hearing date determined by the court and by signing the hearing report.

The Regulation, as a rule, regulates that recordings and images cannot be taken during the e-Hearing, but recording can be made by the court in cases where the trial makes it compulsory. Pursuant to the relevant article of the Regulation, Article 286 of the Turkish Penal Code numbered 5237 titled "Recording of sound or images" shall be applied to the person who violates the mentioned recording ban. The e-Hearing records taken when deemed necessary by the court shall be kept in the Central Registry System for 2 weeks and shall be irreversibly deleted at the end of such period. These records shall not be published without the explicit consent of the court and the persons concerned. Within the framework of the Regulation, the procedures and principles regarding the technical criteria of the systems and devices to be used for the effective, efficient and safe execution of the e-Hearing System shall be determined by the Ministry of Justice and the provisions of the Regulation shall be executed by the Minister of Justice.

02 - The Disclosure Of Personal Data On A Social Networking Site

The Constitutional Court rendered a decision concerning an allegation that the right to demand for the protection of personal data within the scope of the right to respect privacy has been violated due to the disclosure of personal data on a social networking site.

The Constitutional Court ("**Decision**") dated 15.06.2021 and numbered 2018/24439 published in the Official Gazette dated 29.07.2021 and numbered 31552 pertains to a claim of an applicant having a political role (the "**Applicant**"); where the Applicant alleged that the Applicant's right to request for protection of personal data within the scope of right to respect privacy was violated due to the fact that the full address of the Applicant and his spouse's company, the general assembly minutes containing the identity numbers and signatures of his spouse and other relatives, the subscription information of the applicant's spouse's company and the company's photos on the social networking site have been shared on a social networking site, namely Twitter.

The Applicant in the individual application, stated that (i) the mentioned personal information shall be deemed personal data, and the applicant suffered the consequences of the disclosure of such personal data to the public, (ii) although it was clearly stated before the courts of first instance that this situation is against the rights of protection of personal data and respect for privacy, which are guaranteed under the Constitution; the Applicant's rights of protection of personal data, respect for privacy and right to a fair trial were violated since the case was evaluated within the scope of freedom of expression.

The Constitutional Court, as a result of its evaluation based on the national and international legal regulations, decided that;

- The Applicant's information published on Twitter were within the scope of information relating to an identified real person and accessing to, use of and processing of this information should be examined in terms of the right to request for the protection of personal data within the scope of the right to respect privacy,
- Article 20/3 of the Constitution secures the right to request the protection of the personal data for everyone; this constitutional guarantee corresponds to the right to respect privacy, protected under Article 8 of the European Convention on Human Rights; considering the related international documents and comparative law and in light of the relevant provision of the Constitution, all the information about a specific or identifiable real person should be considered as personal data,
- Within the scope of the protection of privacy, the government has a positive obligation to protect all individuals within its jurisdiction against risks that may arise from the actions of both public authorities and other individuals, as well as the person himself in terms of the right to request the protection of personal data,
- Courts of first instance evaluated the concrete case within the scope of the freedom of expression by emphasizing that the parties are politicians and the messages on the social networking site are a way of criticism; but did not evaluate (i) to what extent and how the personal data of the Applicant was seized, (ii) for what legitimate purpose it was shared on the social networking site and (iii) to what public purposes it does serve ,
- For these reasons, it shall be resolved that the Applicant's right to request the protection of personal data which is regulated under Article 20 of the Constitution was violated since it is understood that the courts of first instance did not fulfil their positive obligation to conduct diligent legal proceedings,
- A fundamental right was violated due to a court decision within the scope of an individual application, and the Decision should be sent to the relevant court for a retrial for the elimination of the violation and its consequences,
- The claim for compensation should be refused since it is understood that there is a legal benefit in retrial and also the retrial shall provide the necessary legal benefit and sufficient remedy.

03 - The Access of Lawyers to Enforcement Proceedings of 3rd Parties

The Personal Data Protection Board Rendered a Decision on the Access of Lawyers to Enforcement Proceedings of 3rd Parties.

The Personal Data Protection Board (**"Board"**) rendered its decisions dated 20.05.2021 and numbered 2021/511-512-513 (**"Decision"**) on the notices received with regard to the fact that the attorneys have unlawfully accessed the personal data in the files of enforcement proceedings without a power of attorney and the personal data in the files of enforcement proceedings where the debtors are the creditors, which were illegally transferred to the attorneys of creditors through the personnel working at the enforcement offices and the Ministry of Justice (**"Notices"**).

The Notices alleged that the attorneys of the creditors, acting as the data controllers, having access to the enforcement files without a power of attorney, and the personnel in the enforcement distribution offices transferring the personal data contained in the enforcement proceedings files to the attorneys of the creditor attorneys shall constitute a violation of the Personal Data Protection Law numbered 6698 (**"PDP Law"**); and requested that the Board should detect the violation in question, and take initiatives before the Ministry of Justice, acting as the data controller, to correct the violation and to apply the necessary administrative measures.

The Board initiated an ex officio investigation in line with the Notices received. As a result of the information requested from the Ministry of Justice and the attorney of the creditor both acting as the data controller, within the framework of the investigation, it is stated that;

- The right of the creditor or her attorney to question the debtor's assets, rights and receivable stems from the Enforcement and Bankruptcy Law numbered 2004 (**"Enforcement and Bankruptcy Law"**);
- Pursuant to the Attorneyship Law numbered 1136 (**"Attorneyship Law"**), it is understood that an attorney or an intern may review casefiles and legal action files without a power of attorney, otherwise, the attorney would be liable to the client for not duly performing her duties;
- Attorneys or interns would not be in breach of the PDP Law since it is clearly stipulated in the laws that they could examine the debtors' files where the debtors are the creditors, to ensure that their clients receive their receivables.

The Board, as a result of the examinations carried out on the relevant provisions of the Enforcement and Bankruptcy Law and the Attorneyship Law, and based on the legal ground of "explicitly stipulated in the laws" regulated in Article 5/2-a of the PDP Law, rendered that;

- The attorneys representing the creditors can examine the execution proceedings without the need to present a power of attorney and that the relevant authorities are obliged to provide the attorneys with the necessary feasibility in this regard;
- The attorneys of creditors may inquire about all the properties, rights or receivables of the debtors including the enforcement files where the debtor is the creditor, through the National Judicial Network Information System (**"UYAP"**);
- In order for the creditors' attorneys to fulfill their duties, the personnel in the enforcement offices may transfer to the attorney the personal data contained in the enforcement proceedings files of the debtors;
- In the light of these evaluations, there is no action to be taken within the scope of the PDP Law regarding the Notifications received by the Board.

04 - The "Medium-Term Programme" Was Approved To Be Published İn The Official Gazette!

The "Medium-Term Programme (2022-2024)", prepared with the conjunction of the Ministry of Treasury and Finance and The Ministry of Development, was approved to be published in the Official Gazette!

The Medium Term Programme (**"MTP"**), which initiated the central government budget process, has been published with the President's Decision in the Official Gazette dated 5 September 2021 and numbered 31589. The MTP is designed to cover topics related to public policies including macroeconomic policies, principles, and goals, and income and expenditures related to the upcoming 3 years. Additionally, updates related to the global and Turkish economy along with macroeconomic goals and future economic and social policies that would be followed in relation to these updates are also included. Financial Technologies (**"FinTech"**) are one of the topics covered in these updates. Within this context;

Macroeconomic Goals and Policies: Financial Stability

An increase in savings in the financial system, developments in capital markets that will lead to ease accessibility financing, and the provision of support to financial stability in order to promote financial literacy is aimed. Within this objective;

- Legislation regulating information systems that contribute to the development of the financial technology ecosystem in Turkey while putting it in a place to be one of the leading countries in the digitalisation of the financial industry will be updated.
- Key financial technology companies that provide support services to the financial ecosystem in Turkey will be included in the scope of the audit, minimizing the risks arising from third parties and expanding the use of domestic and national products and services.
- In line with the first phase pilot findings of the Digital Lira Research and Development Project, the findings of the studies on the technological, economic and legal structures of digital money will be evaluated, while further pilot tests with wider participation will continue to be conducted.
- FinTech institutions operating in the field of payments will be provided with access to payment systems and public databases operated by the Central Bank.
- A regulatory sandbox related to payments which will support the Istanbul Finance Centre to become a global authority in the FinTech area will be set up.
- A Finance and Technology Centre will be set up in the İstanbul Finance Centre to support FinTech enterprises.

Briefly, with the publication of the Medium Term Programme, the path to be followed in the area of financial technologies was drawn and the precautions to be taken in this area were established.

05 - Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence

The Personal Data Protection Authority published the guide titled "Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence" ("**Guide**") on 15.09.2021. The Guide has been prepared by taking into account the studies "Guidelines on Artificial Intelligence and Data Protection" of the Directorate General of Human Rights and Rule of Law of the Council of Europe, "Recommendation of the Council on Artificial Intelligence" of the Organisation for Economic Co-operation and Development ("**OECD**"), and "Ethics Guidelines for Trustworthy AI" of the European Commission.

Firstly, the Guide refers to the necessity of managing the artificial intelligence techniques and applications properly, which have made great progress, within the scope of the protection of personal data, since such techniques and applications have started to affect many areas of life directly. In this framework, artificial intelligence studies and applications should comply with the Personal Data Protection Law numbered 6698 and its secondary legislation (all together the "**PDP Legislation**").

The Guide, after stating the general recommendations, sets certain recommendations on the protection of personal data in artificial intelligence applications, carried out by developers, manufacturers, service providers and decision makers in the field of artificial intelligence.

The Guide, under the "General Recommendations" concerning the artificial intelligence application and development processes, recommends that:

- the fundamental rights and freedoms of the data subjects should be respected and the right to the protection of human dignity should be paid regard;
- the data collecting activities should be based on the principles of compliance with the law, proportionality, accountability, transparency, correct and up-to-date status of personal data, specific and limited use of personal data, and data security approach;

- a perspective focusing on the prevention and reduction of potential risks when processing personal data while taking into account the human rights, the functioning of democracy, and social and ethical values should be adopted;
- The control of the personal data processing activity by the data subjects should be possible;
- A privacy impact assessment should be implemented when necessary;
- Compliance with the PDP Legislation from the initial stage and constituting a compliance program specific to each project should be maintained;
- Strict technical and administrative measures regarding the special categories of personal data should be taken;
- The use of personal data should be by anonymizing the data as much as possible;
- The data controller and data processor roles of the stakeholders should be determined from the beginning, and legal relation between the same should be established as compatible with the PDP Legislation

In the Guide, under "Recommendations for Developers, Manufacturers and Service Providers" section, concerning the artificial intelligence application and development processes recommends that:

- A special attention should be paid to personal data privacy in a way that is consistent with national and international regulations;
- Appropriate risk prevention and mitigation measures should be considered to protect fundamental rights and freedoms;
- The data subjects should be prevented from being exposed to discrimination or other negative effects and prejudices at all stages of personal data processing;
- Data minimization principle should be applied;
- The risk of causing adverse effects on individuals and society, that could arise from the out-of-context algorithms should be taken into consideration diligently;
- Relevant academic institutions, neutral experts and organizations should be collaborated within the design phase of human-rights based ethical and socially oriented artificial intelligence application;

- The data subjects should be given the right to object to personal data processing activities which are based on technologies that affect their opinions and personal development;
- Risk assessments based on the active participation of data subjects who are likely to be affected by practices should be promoted;
- Mechanisms should be designed to prevent data subjects from being exposed to a decision that will be affected by processes based on automated personal data processing;
- Alternatives that have less interference with personal rights should be provided to ensure the freedom of choice of users;
- Accountability in accordance with the PDP Legislation for all stakeholders throughout the artificial intelligence in lifecycle should be ensured;
- The users should be provided with the right to stop the processing of personal data and the possibility of deletion, destruction, or anonymization of their personal data;
- Mechanisms should be designed to inform the data subjects and obtain approval in necessary situations in accordance with the PDP Legislation.

Finally, the Guide, under the "Recommendations for Decision Makers" section, regarding the artificial intelligence application and development processes, mentions that:

- Special attention should be paid to the principle of accountability at all stages;
- Risk assessment procedures should be adopted application matrices should be created for the protection of personal data;
- Action should be taken for codes of conduct and certification mechanisms;
- The freedom of individuals not to trust recommendations offered by artificial intelligence applications should be preserved;
- Supervisory authorities should be applied in the case the fundamental rights and freedoms of data subjects are significantly affected;
- Cooperation between supervisors and competent bodies should be encouraged;

- Individuals, groups, and stakeholders should be informed about the social dynamics of artificial intelligence and shaping decision-making mechanisms, and their active participation in these discussions should be ensured;
- Open software-based mechanisms should be encouraged to create a digital ecosystem that supports the processing of personal data in accordance with the PDP Legislation;
- Digital literacy and educational resources shall be invested and trainings should be encouraged to raise awareness about artificial intelligence and personal data privacy.

06 - Registration of Devices with Electronic İdentity Information has been published in the Official Gazette

The Communiqué on the Amendment of the Communiqué on the Registration of Devices with Electronic Identity Information has been published in the Official Gazette! The Communiqué on the Amendment of the Information Technologies and Communication Authority's ("**Authority**") Communique on the Registration of Devices with Electronic İdentity Information, has been published on the Official Gazette dated on 15 September 2021, numbered 31509.

The first article, determining the purpose of the communiqué, was updated to specify;

- The recording of electronic identity information so that devices with electronic identity information that are imported, manufactured, or brought with passengers from abroad can benefit from the electronic communication service,
- The prevention the provision of electronic communication services to lost, illegal or stolen devices,
- The procedures and principles regarding the devices whose electronic identity information is copied to other devices, disposed, exported, and/or reported to be in financial debt by the operators or benefiting from the international permanent data roaming service.

Furthermore, the communiqué was expanded to address;

- Devices with electronic identity information that operators provide services on their networks through their IMSI's,
- Devices with electronic identity information that receive permanent international data roaming service and communicate without audio communication,

- Devices with electronic identification information used in the 112 in-vehicle emergency call system (e-Call).
- The other amendments that were brought with the new communiqué can be summarized in the following manner;

IMEI registration applications for imported or manufactured exchange devices

The IMEI numbers of the devices to be exchanged and intended for exchange must be notified to the Authority by the manufacturer or importer, also notifying that they are intended for exchange. After the controls, the IMEI numbers of the two devices will be changed, provided that they belong to a device of the same brand.

Incorrectly reported IMEI numbers

In order to correct incorrectly registered IMEI numbers, the necessary corrections must be made by the relevant public institution and forwarded to the Authority electronically within the first six months after the registration of the device.

Devices that have not received electronic communication services for seven consecutive years

A new article has been added for devices that have not received electronic communication services for seven consecutive years. Within the scope of this article, it is stated that if these devices do not receive electronic communication for seven years after being registered in the Mobile Device Registration System (MCKS), the request for re-registering their IMEI numbers will be made via MCKS, again through the importer or manufacturer of the device. If the importer or manufacturer of the device has ceased to operate, it is possible for the user to re-register their device if they apply to the Authority with the necessary documents proving this.

07 - Digital Turkish Lira Cooperation Platform

The Central Bank of Turkey has announced a press release in relation to the creation of the Digital Turkish Lira Cooperation Platform within the scope of the Ar-Ge Project! On 15 September 2021 the (**"Central Bank"**) of Turkey announced on its 2021-40 numbered press release that The Central Bank of Turkey "Digital Turkish Lira Cooperation Platform" was established considering the bilateral memorandum of understandings signed with ASELSAN, HAVELSAN and TÜBİTAK-BİLGEM. It was also stated in the press release that the platform is planned to be expanded with new participations in the light of relevant pre-application tests.

In the light of this release;

- Within the scope of the first phase implementation studies, the prototype "Digital Turkish Lira Network" will be established, and narrow-scope and closed-circuit pilot application tests will be carried out with the acknowledged technology stakeholders.
- Afterwards, in line with the results obtained, more comprehensive tests on topics such as blockchain technology, use of distributed structures in payment systems, integration with instant payment systems, that may further diversify and develop the Ar-Ge Digital Turkish Lira project, are planned to be conducted.

The Central Bank of Turkey has not made an official and financial announcement regarding the use and validity of the Digital Turkish Lira yet. Following the capacity measurements of different technological alternatives are completed and the architectural setups are finalized, the question of whether the existing technologies can meet the economic, legal, and financial requirements of the Digital Turkish Lira is to be deduced. The results of the first phase will be shared with the public in 2022, following the completion of the tests

08 - Guiding Principal Decision on Matters to be Considered in Processing of Biometric Data

The Personal Data Protection Authority ("**Authority**") published the "Guiding Principal Decision on the Matters to be Considered in Processing of Biometric Data" ("**Principal Decision**") on its website on 16.09.2021.

The Principal Decision primarily states the relevant article of the Personal Data Protection Law No. numbered 6698 ("**PDP Law**") on the special categories of personal data and the definition of biometric data under Article 4 of the European Union General Data Protection Regulation ("**GDPR**").

Afterwards, the Principal Decision provides a definition of the biometric data as the "data that is impossible for people to forget, does not change for life, and is effortlessly owned without the need for any intervention" based on the definitions stated under the judicial decisions before the adoption of the PDP Law.

According to the Principal Decision, while biometric data such as the fingerprint, retina, palm, face, hand shape, and iris of a person constitute the physiological biometric data; biometric data such as the person's walking and driving style, and the way of pressing the keyboard constitute the behavioural biometric data.

As stated by the Principal Decision, in the processing of biometric data, existence of the biometric data processing conditions and complying with the general principles under Article 4 of the PDP Law should be a must.

The Principal Decision also emphasizes the importance of making evaluations within the frame of the concrete case apart from fulfilling the conditions stipulated under the PDP Law on determining whether the biometric data is processed.

At this point, in the light of the Personal Data Protection Boards' ("**Board**") Decision numbered 2019/81 and the Summary Decision numbered 2019/165, it is stated under the Principal Decision that the Board has certain judgement on the matters of explicit consent and proportionality, but different judgements can be made in different cases where the concrete case requires to do so, to the extent that it is in compliance with the PDP Law.

Pursuant to the Principal Decision, in accordance with the general principles set forth under Article 4 of the PDP Law, and the conditions set forth under Article 6 of the PDP Law, data controller shall only be able to process biometric data in compliance with the following principles:

- The core principles of the fundamental rights and freedoms shall be preserved while processing biometric data;
- The method used for processing biometric data shall be suitable for achieving the purpose of processing and the data processing activity shall be suitable for the purpose to be achieved;
- The biometric data processing method shall be necessary for the purpose to be achieved;
- A proportion shall be established between the purpose to be achieved by the data controller and the tool;
- The biometric data shall be stored for a required period and shall be destroyed without any delay/immediately after such requisite disappears.
- Data Controllers shall fulfil their obligation to inform the data subjects in accordance with Article 10 of the PDP Law, but limited to the purpose of processing and
- Explicit consent shall be obtained from the data subjects, if required in accordance with the PDP Law.

Apart from these principles, data controller;

- Shall record and document that all the principles listed in the Principal Decision are met;
- Shall not collect genetic data while collecting biometric data, if not necessary;
- Shall provide justification and documentation as to preference of certain type or types of biometric data;
- Shall state the retention periods and their reasonings in the Personal Data Retention and Destruction Policy in accordance with Article 4/1-d of the PDP Law.

It is stated under the "Biometric Data Security" title of the Principal Decision that the data controllers processing biometric data shall pay attention to the regulations related to the personal data security, stated under the regulations, communiques, and the board decisions. Within this frame, it is mentioned that the measures specified in the Board's Decision numbered 2018/10 on "Adequate Precautions to be Taken by Data Controllers in the Processing of Special Categories of Personal Data" shall be taken. Finally, the Principal Decision, apart from the measures stated under the Board Decision numbered 2018/10, specifies the technical and administrative measures required to be taken by the data controller as follows.

Technical Measures:

- Cryptographic methods shall be used for storing of the biometric data in cloud systems, and encryption and key management policies shall be introduced;
- Derived biometric data shall be kept in a way that does not allow recovery of the original biometric feature;
- The use of biometric data in testing environments shall be limited to necessity, if possible synthetic data shall be used for testing, biometric data shall be deleted latest by the end of the tests;
- Measures that warn the system administrator and/or delete biometric data and provide reports in case of an unauthorized access to the system shall be implemented;
- Certified equipment, licensed and up-to-date software shall be used, and open-source software shall be preferred within the system;
- Lifetime of the devices that process biometric data shall be monitorable;
- Logging and access authorizations regarding processing of biometric data shall be defined; and
- Periodic hardware and software tests for the biometric data system shall be conducted.

Administrative Measures:

- An alternative system shall be provided without any restrictions or additional costs for the data subjects whose biometric data cannot be processed;
- An action plan shall be established for the cases where an authentication by biometric methods cannot be fulfilled;
- Access authorizations shall be defined, access control matrixes shall be established and documented;
- Tailor made trainings on the processing of biometric data shall be given to the personnel involved in the processing of biometric data and such trainings shall be documented;
- A formal reporting procedure shall be established for the employees to report possible security gaps in the systems and services and
- An emergency procedure shall be implemented to be used in the event of a data breach and everybody concerned shall be announced.

October

01 **The Constitutional Court Rendered A Decision Concerning An Allegation That The Right To Demand Protection Of Personal Data.**

01 - The Constitutional Court Rendered A Decision Concerning An Allegation That The Right To Demand Protection Of Personal Data

The Constitutional Court Decision dated 07.09.2021 and numbered 2018/30296 published in the Official Gazette dated 14.10.2021 and numbered 31628 (**"Decision"**) pertains to an applicant's claim that her right to request the protection of personal data within the scope of the right to respect for privacy has been violated. The claims of the applicant (**"Applicant"**) within the scope of the Decision are as follows:

- Personal data such as communication, message records, e-government and banking passwords on the mobile phone of the Applicant being accessed through spyware installed without the Applicant's consent and knowledge,
- Within the scope of the Applicant's spouse presenting the said data as evidence before the divorce case despite the Applicant's request, no research being conducted during the investigation and prosecution regarding which data were accessed by the spouse and between which dates,
- The justification of the Court of Instance that spouses accessing information about the other spouse not being protected under Article 20 of the Constitution.

The Applicant, within the frame of such allegations requested that since the use of personal data obtained without consent in the divorce case will not make the spouse's act comply with the law, it should be rendered that the right to respect for privacy and freedom of communication has been violated. Criminal proceedings were carried out by Ezine Criminal Court of First Instance upon the request of the Applicant regarding the spouse being charged for the crimes of violating the confidentiality of communication and privacy of the Applicant, and the spouse was acquitted. Bursa Regional Court of Justice, acting as the appeal court, decided to affirm the Ezine Criminal Court's decision. Thus, the Applicant filed an individual application before the Constitutional Court.

As a result of its evaluation based on the national and international legislation, the Constitutional Court decided that:

- Article 20/3 of the Constitution secures the right to request the protection of the personal data for all individuals; considering the wording of the article, it provides assurance against all kinds of interventions and limitations on personal data within the scope of the right to request the protection of personal data; this constitutional guarantee corresponds to the right to respect privacy protected under Article 8 of the European Convention on Human Rights; considering the related international documents and comparative law and in light of the relevant provision of the Constitution, all the information about a specific or identifiable real person should be considered as personal data,

- In the concrete case, the essence of the Applicant's complaint is that the unlawful access to the information contained in the Applicant's phone, and therefore the Applicant's personal data should be evaluated in terms of the right to protection of personal data within the scope of the right to respect privacy in line with the allegation that the obligation to establish an effective judicial system is not complied with regards to the criminal complaint,
- Within the scope of the protection of privacy, the government has a positive obligation to protect all individuals within its jurisdiction against risks that may arise from the actions of both public authorities and other individuals, as well as the person himself/herself in terms of the right to request the protection of personal data; in this sense, the state should fulfil its obligation to establish an effective judicial system and to use appropriate tools for the resolution of disputes,
- It is clear that the information on the applicant's phone serves as personal data and that illegally obtaining and disclosing such personal data is regulated as a crime under the applicable legislation, in this regard an effective criminal investigation clarifying all aspects of the incident should be carried out and the conclusion reached relating to the incident should be stated with specific reasoning relating to the facts by considering the Applicant's complaints,
- The Ezine Criminal Court in its justification stated that the accused acted in order not to lose the evidence and that the data obtained were only used as evidence in the divorce case, thus no research was done on (i) which personal data of the Applicant were obtained and (ii) whether changes were made to these data or not, (iii) how long the data were accessed and (iv) the court of instance did not evaluate whether the method, scope and purpose of obtaining personal data accessed is legitimate or not, by installing a software program on the Applicant's phone, which is an important element of the Applicant's privacy,
- Due to these facts, it is not possible to state that the reasoning of the court of instance is relevant and sufficient to protect the Applicant's right to personal data protection,
- A fundamental right of the Applicant to demand the protection of personal data within the scope of the right to respect for privacy has been violated due to a court decision within the scope of an individual application, and the Decision should be sent to the relevant court for a retrial for the elimination of the violation and its consequences.

November

01 **Pursuant To The Communiqué On Amendments To The Communiqué On Block Exemption On Vertical Agreements The Market Share Threshold Has Been Lowered To 30%.**

02 **Evaluation Of The Right To Be Forgotten In Light Of Search Engines**

03 **Regulation On Internal Systems In Insurance And Private Pension Sectors Has Been Published.**

01 - Pursuant to the Communiqué on Amendments to the Communiqué on Block Exemption on Vertical Agreements the Market Share Threshold has been Lowered to 30%

The Communiqué on Amendments to the Communiqué on Block Exemption on Vertical Agreements (**"Communiqué"**) was published in the Official Gazette dated 5 November 2021 and numbered 31650. With the Communiqué, the second and third paragraphs of Article 2 and article 6/A in the Block Exemption Communiqué on Vertical Agreements numbered 2002/2 (**"Communiqué numbered 2002/2"**) have been amended and Provisional Article 3 has been added. The Communiqué entered into force on the date of its publication.

With the amendment made in Article 2 subparagraphs 2 and 3 of the of the Communiqué numbered 2002/2 pursuant to Article 1 of the Communiqué, the exemption provided by the Communiqué will now be applied on the condition that the market share of the supplier in the relevant market in which the supplier provides the goods and services subject to the vertical agreement does not exceed 30%. In vertical agreements that include the obligation to supply to a single buyer, the exemption will also be applied provided that the buyer's share in the relevant market from which the goods and services subject to the vertical agreement does not exceed 30%.

The following rules will be applied in the implementation of the 30% market share principle specified in the Communiqué:

a) Market share is calculated using the previous year's data.

b) Market share includes all goods and services provided for sale to affiliated distributors.

c) If the market share is initially not more than 30% and then increases above the threshold, not exceeding 35%, the exemption will continue to be valid for the next two years following the year in which the market share threshold was first exceeded.

d) If the market share is initially not more than 30% and then increases above 35%, the exemption will continue to be valid throughout the year following the year in which the market share threshold was first exceeded.

e) The rights provided by subparagraphs (c) and (d) cannot be combined in such a way that the period exceeds two calendar years.

With the added Provisional Article 3, agreements that benefit from the exemption provided by the Communiqué numbered 2002/2 on the effective date, but fall outside the scope stipulated by the amendment made in Article 2 of the Communiqué, within 6 months from the effective date of the Communiqué, compliance with the conditions set out in Article 5 of the Protection of Competition Law numbered 4054 (**"Law"**) must be ensured.

The conditions stipulated under Article 5 of the Law are as follows.

a) Ensuring new developments and improvements or economic or technical development in the production or distribution of goods and the provision of services,

b) The consumer benefiting from such,

c) Competition ceasing in a significant part of the relevant market,

d) Not limiting the competition more than is necessary to achieve the objectives in (a) and (b).

Also, pursuant to the Communiqué, within the 6- month period, Article 4 of the Law regarding the prohibition of "Agreements between undertakings, concerted practices and associations of undertakings with the aim of preventing, distorting or restricting competition directly or indirectly in a particular good or service market, or which have or may cause such an effect, to such decisions and actions" shall not apply.

In summary, the market share threshold in the Communique numbered 2002/2 has been lowered to 30% and the rules to be applied in the implementation of the 30% market share threshold have been determined.

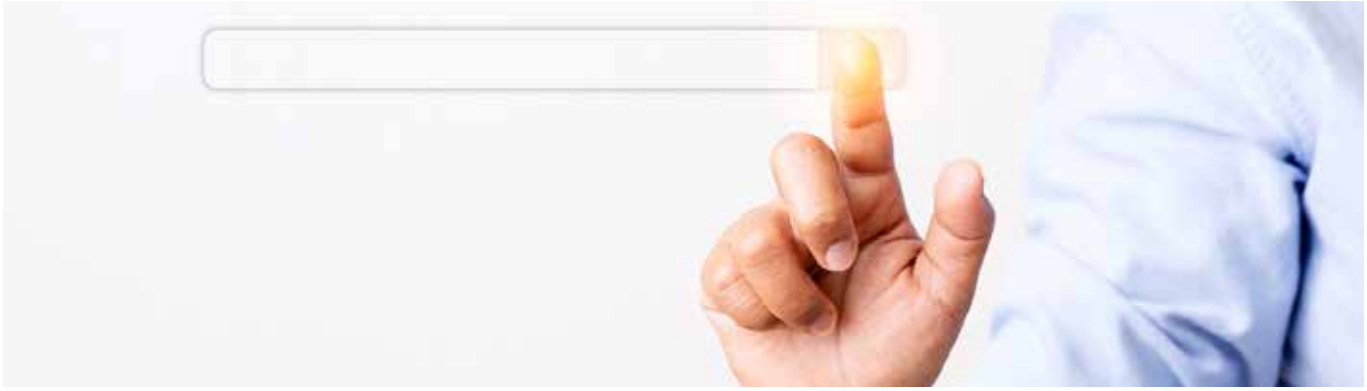
02 - Evaluation of the Right to be Forgotten in light of Search Engines

The Personal Data Protection Authority published the Guide titled "Evaluation of the Right to be Forgotten in light of Search Engines" (**"Guide"**) on 20.10.2021.

The Guide has been prepared to clarify the exercise of the right to be forgotten before the search engines within the framework of the Decision of the Personal Data Protection Board dated 23.6.2020 and numbered 2020/ 481 (**"Decision"**) regarding the requests of individuals to remove from the index, their names and surnames and the results of searches made through search engines.

In the relevant Guide, firstly, explanations regarding the right to be forgotten and its development and the place of the right to be forgotten in international and national law are given.

In the Guide, it is mentioned that data can be easily recorded and stored for many years due to the developing technology, and it is stated that the data of data subjects not being tracked by third parties is important for the individual to continue living her/ his life freely. In this sense, by restricting (partially) access to the personal data of the individual by third parties; the "Right to be Forgotten" comes to the fore as an aspect of the right to protect personal data in order to ensure a dignified life, to prevent exclusion from society, and to start off with a clean slate. The right to be forgotten, which is defined as "the individual's ability to request that the data which has been legally disseminated in the past and of a correct nature be removed from access or not brought up due to the passage of the time", in other words, refers to the right of individuals to request the prevention of access to their personal data.



Although there is no legal regulation that conceptually includes this right under the title of "Right to be Forgotten" in Turkey, it has been stated that there are tools in our law to exercise this right. In this context; the Constitution, the Turkish Civil Code numbered 4721, the Law on the Protection of Personal Data numbered 6698 (**"Law"**), the Judicial Registry Law numbered 5352, and the Law on the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts numbered 5651 contain various tools for the establishment of the right to be forgotten.

Within the scope of the aforementioned Decision; considering that the search engines have a decisive role in the dissemination of data, some procedures and principles have been determined in terms of subjecting the names and surnames of the data subjects and the results obtained from searches to be made through the search engines in a non-indexable technical way. With the Decision, search engines have been accepted as data controllers within the framework of the definition in Article 3 of the Law, considering that they determine the purpose and means of processing the data they collect on the internet belonging to third parties.

Requests regarding the establishment of the right to be forgotten by the data subjects may be asserted to search engines within the scope of data processing conditions, as well as regarding the content processed and disseminated by third parties without the condition of data processing. On the other hand, it is possible for the data subjects to request the removal of links related to their personal data from the search results under certain conditions, such as in cases where their data is incorrect, unsuitable, irrelevant or disproportionate for the purpose of data processing. In this context, since the right to be forgotten is not an absolute right that can be asserted by the data subjects under any circumstance, but an exceptional right, a decision is made by evaluation within the framework of criteria specific to each concrete case.

These criteria have been determined as follows:

- The data subject playing an important role in public life
- Child being the subject of the search results
- The accuracy of the content of the data
- Relevance of knowledge to one's professional life
- The data being of an insulting, humiliating, slandering nature
- The data being sensitive personal data
- Currency of data
- Data causing prejudice about the person
- Data posing a risk on the person
- Whether the data is published by the data subject herself/ himself
- Content's coverage of data processed within the scope of journalistic activity
- Legal obligation to publish data
- The data relating to a criminal offense.

In the continuation of the Guide, the methods of claiming rights of the data subject are taken into consideration, and it is emphasized that within the scope of the requests of the data subject for the right to be forgotten, they should primarily apply to search engines pursuant to the provisions of the legislation.

03 - Regulation On Internal Systems In Insurance And Private Pension Sectors Has Been Published

"Regulation on Internal Systems in Insurance and Private Pension Sectors" ("**Regulation**") drafted by the Insurance and Private Pension Regulation and Supervision Agency ("**Agency**") was published in the Official Gazette dated 25 November 2021 and numbered 31670. The Regulation regulates the procedures and principles regarding the internal control, risk management, actuarial and internal audit systems to be established by insurance, reinsurance and pension companies, specific institutions operating in the insurance and private pension sectors, and insurance and reinsurance brokers regarded as legal entities, and their operations.

The Regulation covers insurance, reinsurance and pension companies established in Turkey, organizations of foreign insurance and reinsurance companies in Turkey, Assurance Account, Insurance Information and Monitoring Center, Pension Monitoring Center, Insurance Arbitration Commission, Turkish Motor Vehicles Bureau, Turkish Natural Catastrophe Insurance Pool, Special Risks Management Center and insurance and reinsurance brokers regarded as legal entities.

The operations described below have been added in addition to the internal control system, risk management system and internal audit system in the Regulation on Internal Systems of Insurance, Reinsurance and Pension Companies published in the Official Gazette dated 21.6.2008 and numbered 26913, which was repealed with Article 56 of the Regulation. The regulation entered into force on the date of its publication and the transitional provisions are regulated with the Provisional Article 1.

Pursuant to Article 6 and onwards, the qualifications of the Members of the Audit Committee which fulfil duties within the scope of internal systems have been determined and their duties related to each function have been specified. Specific institutions, insurance and reinsurance brokers regarded as legal entities are not required to establish an audit committee within the scope of the exception set out in Article 13.

The purpose of the actuarial unit to be established within the scope of the Fifth Section of the Regulation is to provide assurance to the Agency regarding the general pricing policy of the institution, the actuarial adequacy of reinsurance agreements, the financial situation of the institution, the reliability and adequacy of technical provisions, asset and liability risk management and investment risk for investments made under insurance policies. Within the scope of Article 4/4 of the Regulation, Turkish Natural Catastrophe Insurance Pool, Special Risks Management Center and Turkish Motor Vehicles Bureau are obliged to establish an actuarial unit and function in addition to the units and functions defined in the Regulation.

Within the scope of Article 54 of the Regulation, detailed regulations regarding the reports which need to be submitted to the Agency within the scope of the internal control function, risk management function, actuarial function, internal audit function and the report prepared by the board of directors have been stipulated. With the exception of information regarded as trade secrets and taking into account the matters within the scope of personal data protection, companies and specific organizations are obliged to announce to the public the reports disclosed within the scope of paragraph 2 of Article 55 of the Regulation, in a way that can be easily accessed by the users on their home page.

December

01 The Regulation On Payment Services And Electronic Money Issuance And Payment Service Providers Has Been Published In The Official Gazette.

02 Specialized Courts For The Crimes Regulated, Covered Under The “Law On Payment And Securities Settlement Systems, Payment Services And Electronic Money Institutions”.

03 Communiqué On Procedures And Principles Regarding Personnel Certification Mechanism Published In The Official Gazette.

04 The Competition Authority’s Report On Financial Technologies In Payment Services Is Published.

01 - The Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers has been published in the Official Gazette

The Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers (“**Regulation**”) has been published in the Official Gazette dated 01.12.2021 and numbered 31676.

In the published Regulation, it is seen that detailed regulations have been introduced on processes such as capital, partnership structure, establishment principles, license application and extension processes, data sharing services, technical, infrastructure, information security, risk and internal control processes, remote customer acquisition. In this context, the main regulations are as follows. Within the scope of Article 3 of the Regulation, any quantitative data that can be associated with price such as fees, commissions and interest are defined as competition sensitive data.

Pursuant to Article 4 paragraph 7, the provision of services listed in subparagraph (d) of the first paragraph by the electronic communications operator to its non-adult prepaid or postpaid users is conditional upon the approval of the person’s legal representative for the services. In accordance with Article 8, the payment service provider is obliged to offer the payment account and infrastructure services it offers under similar conditions to other commercial customers, business partners and other payment service providers with which it realizes transactions, in case another payment service provider requests to use it and within 1 month at the latest, it is obliged to convey the decision to reject or accept the request.

Pursuant to Article 11, the application fee for the authorization permit has been regulated as TL 500.000 and the amount of the paid-in capital of the company, free from collusion relating to the provision of services in different categories has been amended.

In Article 14, determining principles for the operating principles of payment institutions and electronic money institutions (**"Institution"**) have been introduced. The activities that the Institutions may not carry out have been detailed in Article 15. In paragraph 4 of the relevant Article, an exception has been made to the prohibition of foreign exchange buying and selling, in payment transactions in which both parties are resident in Turkey and are making transactions through payment service providers located in Turkey. Pursuant to paragraph 5 of the same article, Institutions are allowed to make foreign exchange transactions to persons who are not considered to be resident in Turkey, provided that it is limited to the provision of payment services only.

Pursuant to Article 18, the regulation for the Institution to carry out payment services through representatives has been expanded, allowing Institutions to establish representative relations in relation to their activities abroad, with real or legal persons residing abroad. In the scope of Article 19, it has been regulated that the Institution may cooperate with legal entities residing abroad that have obtained permission from the bank.

In accordance with Article 21 paragraph 2, Institutions have obtained the opportunity to procure information systems, marketing, advertising, corporate resource management, accounting, call center, follow-up activities of the Institution's administrative affairs from external service providers. The minimum equity obligation under Article 33 has been differentiated according to the types of payment services to be provided by the payment institutions.

Within the scope of Article 59, the principles for payment institutions to provide the services regulated in paragraphs f and g of Article 4/1 have been comprehensively regulated. In Articles 60 and 61, rules regarding access to payment account information have been introduced during the provision of the payment order initiation service and the provision of the account information service. In Article 62, a comprehensive regulation has been introduced for the protection of data related to the realization of payment service activities as part of the Institutions' activities.

Pursuant to paragraph 3 of Article 66, it has been regulated that, where both parties of the transaction are resident in Turkey and use payment service providers located in Turkey, the Institution may only perform payment transactions in Turkish Lira. Article 66 paragraph 4, sets the rules regarding transactions that cannot be made in foreign currency by persons residing in Turkey. Within the scope of Provisional Article 1 paragraph 1, regulating the transitional provisions, a 1-year transition period has been defined starting from the effective date, for compliance with all new provisions introduced by the Regulation.

02 - Specialized courts for the crimes regulated, covered under the "Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions"

The Decision of the First Chamber of the Board of Judges and Prosecutors, dated 25.11.2021 and numbered 1230 ("**Decision**") was published in the Official Gazette dated 30 November 2021 and numbered 31675. With the Decision taken, specialized courts have been set up to deal with the cases to be filed for the crimes regulated, covered under the "Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions" numbered 6493 dated 20.06.2013 ("**Law**").

In this context, the courts that will handle cases arising from the Law are as follows.

In terms of crimes falling under the jurisdiction of the criminal court;

- Number 1 in places with two or more criminal courts,
- Ankara 6th and Istanbul 8th Criminal Courts to, since Ankara 6th and Istanbul 8th Criminal Courts were previously designated as specialized courts for crimes related to banking.

In terms of crimes falling under the jurisdiction of the criminal court of first instance;

- Number 2 in places with two criminal courts of first instance,
- Number 3, in places with three or more criminal courts of first instance,

03 - Communiqué on Procedures and Principles Regarding Personnel Certification Mechanism Published in the Official Gazette

The Communiqué on the Procedure and Principles Regarding the Personnel Certification Mechanism (“**Communiqué**”) drafted by the Personal Data Protection Authority (“**Authority**”) was published in the Official Gazette dated 6.12.2021 and numbered 31681.

The Communiqué determines the procedures and principles regarding the certification of persons within the Data Protection Officer Program in accordance with the (TS) EN ISO/IEC 17024 standard.

Persons holding the title of Data Protection Officer within the scope of the Communiqué are deemed to have sufficient knowledge of personal data protection legislation and may use this title throughout the validity period of the certificate. In accordance with Article 14 of the Communiqué, the validity period has been determined as 4 years from the announcement of the exam results. As per Article 4 of the Communiqué the term Data Protection Officer has been included in our legislation.

Pursuant to Article 5 paragraph 2 of the Communiqué, the data controller and/or the data processor appointing a Data Protection Officer does not remove the data controller's and/or data processor's responsibility to comply with the Personal Data Protection Law numbered 6698 and relevant legislation. In accordance with Article 11 of the Communiqué, those who have received a certificate of participation in the last 4 years before the exam date or those who have a valid Data Protection Officer Certificate, and those who meet the conditions determined in the program, are entitled to apply for the Data Protection Officer Certificate Exam.

The Authority shall be responsible for the establishment and management of the Certificate Tracking and Verification Information System (**"SERTABIS"**), in accordance with Article 15 of the Communiqué, allowing public inquiries to ensure that the certification activities are carried out impartially, transparently and effectively. In SERTABIS, the information contained in the certificate of participation, the information of the personnel certification information and the changes in their status, the information on the certificate holders, the dates of the exams held within the scope of the program, as well as certificate dates, certificate numbers, certificate validity periods and certificate status of those who pass the exams, shall be included.

Pursuant to Article 17 of the Communique, complaints or appeals within the scope of the program shall be made to the personnel certification institution. In cases where the complaint or objection application is rejected by the personnel certification institution or no response is given within 30 days from the application, the complainant may apply to the Authority within 30 days from the date of becoming aware of the response of the personnel certification institution and in any case within 60 days from the application date. Pursuant to the relevant article, it is not possible to apply to the Authority without exhausting this complaint or appeal procedure.

Personnel certification institutions shall be accredited by the Turkish Accreditation Agency (**"TURKAK"**) and TURKAK may suspend accreditation completely or partially or narrow the scope of the institution.

04 - The Competition Authority's Report on Financial Technologies in Payment Services is Published

On 08.12.2021, the Report on Financial Technologies in Payment Services (**"Report"**) was published on the website of the Competition Authority (**"Authority"**). The Report has been prepared in order to emphasize the importance of making maximum use of the radical transformation in the financial sector in our country and to reveal the necessity of inter-institutional cooperation in this field. The Report focuses on the issues supporting development of Financial Technologies (**"FinTech"**), exclusionary actions of established enterprises, regulatory framework, market dynamics and market entry of large technology companies. In the Report, the reasons for the emergence of FinTech sector, their effects on the sector, the difficulties faced by the players while marketing their products and services, and the obstacles on the increase in innovation and competitive conditions in the market, exclusionary effects and actions originating from both the market and established enterprises are evaluated. Valuable suggestions from the perspective of competition are made for the development of the FinTech ecosystem taking into consideration the dynamics of the sector.

It is stated that the fact that FinTech companies are highly dependent on the banking infrastructure in their activities, creates a vertical relationship between FinTech companies and banks, and in cases where services are not provided to FinTech companies by banks, Fintech companies are not able to provide products and services they have developed to the consumers. It is evaluated that this market structure, in which FinTech companies receive services from banks in the upstream market and compete with banks in the downstream market, has similar characteristics to markets such as telecommunication and retail. The Authority established a convergence between the telecommunication market and the payment services market and stated that **each bank shall be in a dominant position, taking into account the customer data of companies providing financial services.**