THE Fine PRINT

Gökçe

March 2021

89

DIGITAL BANKING IS COMING THROUGH!

Cryptocurrency Statement by Ministry of Treasury and Finance

Always on the Agenda: Personal Data Protection Law

DIGITAL BANKING IS COMING THROUGH!

Ministry of Treasury and Finance announced that digital banking licenses will be enabled as a further development within Economic Reform Package published on 12 March 2021. Pursuant to Economic Reform Action Plan **(Action Plan)** accordingly published on 23 March 2021, it is understood that Banking Regulation and Supervision Agency **(BDDK)** is in charge of establishing the economic, technological and legal infrastructure of digital currency, and it is planned to set forth regulations in this regard until 31.12.2021.

Digital banking, in short, is a banking activity that provides banking services only in a digital environment without branches. Even though it is a new development in our country, digital banking has a wide range of application in practice in many parts of the world. The total value of the 10 most valuable digital banks of the digital banking industry, which show progress significantly within recent years, reached 36 billion 950 million USD as of August 2020.

Therefore, significant changes are expected to be made in Banking Law and its secondary legislation. Entrepreneurs and investors are also expected to show great interest and apply for digital banking licence by commencement of this practice in Turkey. It is an object of curiosity how market actors will act after this progress, which is in particular important for domestic *fintech* initiatives.

Cryptocurrency Statement by Ministry of Treasury and Finance

Ministry of Treasury and Finance **(Ministry)** made a press release on 1 March 2021. In the statement, Ministry shared the worldwide concerns towards cryptocurrencies and stated that the progress on the matter and the situation in Turkey have been closely followed. It was expressed that Ministry works in cooperation with the Central Bank, BDDK, Capital Markets Board **(SPK)** and other related bodies.

Following Ministry's statement, Lütfi Elvan, Minister of Treasury and Finance, announced that a roadmap has been prepared within this framework. It was further indicated that works on **(i)** technological infrastructure, **(ii)** legal infrastructure, **(iii)** financial infrastructure will be carried out with regards to digital currencies. This statement reveals that especially the actions on the Turkish Lira equivalent of digital currency, and the statement relating to the serious concerns about cryptocurrencies reveal the attitude of Ministry towards cryptocurrencies.

Currently, there is no specific Turkish legislation regulating cryptocurrencies. However, the use and scope of application of cryptocurrency is increasing worldwide day by day. Turkey is, in particular, one of the countries where the use of cryptocurrency and the interest in it is highest. According to the Action Plan published on 23.03.2021, Central Bank is assigned with constituting the economic, technological and legal infrastructure of digital currency. Regulations are planned to be made until 31.12.2021.

These developments demonstrate that cryptocurrencies are closely monitored by the state. But at the same time, we see that a negative perspective on cryptocurrencies is beginning to emerge and the use of cryptocurrencies to be issued by the state, rather than decentralized cryptocurrencies, is more significant on the agenda.

You can reach the statement of Ministry here and Action Plan here (Only available in Turkish).

For further information please contact us at contact@gokce.av.tr

Always on the Agenda: Personal Data Protection Law

President Erdogan also addressed Personal Data Protection Law **(Law)** at the Human Rights Action Plan Meeting. Erdogan stated that efforts are underway to bring Law into line with European Union standards as well as emphasizing the right to privacy in his speech. It is also on the agenda that the efficiency of Personal Data Protection Authority will be enhanced. Furthermore, it was expressed that the opportunity of applying to administrative jurisdiction against administrative fines imposed by Board will be available.

The calendar in relation to this matter was also announced in Action Plan dated 23.03.2021. The due date of the action has been determined as 31.03.2022 for the necessary changes which will be made on Personal Data Protection Law on the basis of the provisions of EU General Data Protection Regulation **(GDPR)** related to abroad data transfers. Progress is expectantly awaited.

Verbis Deadline Is Postponed, Again!

Personal Data Protection Board (Board) decided to postpone the deadline for Data Controllers' Registry System (Verbis) by considering that data controllers have been struggling to fulfill the obligation to register Verbis due to Covid-19 outbreak. Board's underlying decision dated 11.03.2021 and numbered 2021/238, was published in the Official Gazette dated 16.03.2021.

As per Board's underlying decision, all data controllers, who are under obligation to register with Verbis, should register until 31.12.2021. Data controllers under obligation to register with Verbis are as follows together with the re-determined deadlines.

Data Controllers	Verbis Deadline
Data controllers with **more than 50** employees or whose total annual balance is higher than **25 million TL** and Turkish non-resident data controllers	31.12.2021
Data controllers with **less than 50** employees and whose total annual balance is lower than **25 million TL**, but processing of sensitive personal data is the major commercial activity	31.12.2021
Data controllers considered as public institutions and organizations	31.12.2021

You can reach the full text of the decision here (Only available in Turkish).

For further information please contact us at contact@gokce.av.tr

Personal Data Protection Board approved Amazon's transfer of personal data abroad

As per KVKK, personal data may be transferred abroad if **(i)** there is an explicit consent of the data subject, or **(ii)** the existence of one of the exceptions of explicit consent referred in Law and adequate protection must be provided in the country where data will be transferred. If there is no adequate protection, data controllers both in Turkey and in the relevant country abroad must give written undertaking and obtain an approval from Board.

Board has not announced the countries which provide adequate protection yet. Thus, the only method that could be followed in the absence of an explicit consent is to obtain Board's approval with a written undertaking. In this context, Board announced on 9 February 2021 for the first time that it allowed TEB Arval Araç Filo Kiralama A.Ş. to transfer data abroad. This was the first time that Board allowed the transfer of personal data abroad since Law came into force. Following this announcement of Board, while it was an object of curiosity about the way Board would follow in relation to the data transfer abroad, Board released another announcement on 4 March 2021. Board allowed abroad transfers by approving the applications of the undertakings made by Amazon Turkey Perakende Hizmetleri Ltd. Şti. and Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti. with this announcement.

You can reach the full text of the announcement here (Only available in Turkish).

Summaries of Personal Data Protection Board's Recent Decisions

We compiled below some of Personal Data Protection Board's **(Board)** decisions, published in March within the scope of Personal Data Protection Law **(Law)** and secondary legislation.

The decision summary on an employer who illegally processed personal data and sensitive personal data of an employee without fulfilling the disclosure obligations

In the complaint petition filed to Board the complainant employee stated that he requested information from the data controller company in which he works within the scope of Law but he has not received an adequate response. He stated that no information was given regarding who accessed his personal data and how long it was stored, that he was not informed by the data controller and he was obliged to approve a comprehensive deed of consent. The complainant further stated that the fingerprints of the company employees were taken by force without explicit consent and that he was not informed about the transfer and measures.

Board in its decision ruled and included, that;

• The matters that must be incorporated in privacy notices pursuant to Law art.10 and Communique on Procedures and Principles to Fulfill Disclosure Requirement **(Communique)**,

• The deed of consent indicated by the complainant was issued as a privacy notice and explicit consent text, yet as per Communique art.5/1-f the data controller must fulfil disclosure obligations and carry out explicit consent procedures separately and the disclosure was not made duly in terms of manner,

• It could not be said that the text fulfilled the disclosure obligations in respect of content, due to after listing the processed categories of personal data the expression that "including the listed personal data but not limited to those" was mentioned and which personal data would be processed (categorically) was left ambiguous, the purposes of processing were also listed consecutively, and there was no explanation as to the purposes of data categories, the statement that "transferred to other third parties deemed appropriate and/or abroad" was included and within this context to whom the transfer would be made was left to the data controller in an ambiguous way,

• The consent obtained is not valid in the event that the employer does not effectively provide the employee with the opportunity of not giving explicit consent and the processing of sensitive personal data was not proportionate.

Based on the assessment mentioned above, Board decided to impose **(i)** an administrative fine of TRY 50,000 due to the failure to fulfil disclosure requirements and **(ii)** an administrative fine of TRY 200,000 for not taking the necessary technical and administrative measures towards ensuring the appropriate security level on the data controller.

You can reach the full text of the decision here (Only available in Turkish).

The decision summary on the request to remove the news from the website of the newspaper in which the news belonging to the person whose sentence was executed due to the crime she was convicted

The data subject stated that the website of the data controller newspaper contains information about the crime that she was convicted of and that the news was from 2009. She expressed that still having access to such news has a negative impact on her. Thus, she requested from Board to impose an administrative fine and suspension of data processing activities on the data controller on the grounds that she applied to the data controller and got rejected.

Board made detailed statements on freedom of expression and freedom of the press in its decision. Even though the news belongs to the year 2009, it has been concluded that it is one of the exceptional circumstances referred in Law by reason of the fact that it is up-to-date as of the date of publication and is a matter of public concern. Thus, Board has ruled that there was no action to be taken within the scope of Law.

You can reach the full text of the decision here (Only available in Turkish).

“Remote” but “Safe”?

Employees have started to be able to easily work from outside the workplace by virtue of the technology which in recent years has been developed faster than expected. Many businesses switched to remote working model due to the pandemic last year. Employees in many workplaces started to work from home or anywhere outside the workplace in our country as well, without the need of being present at the workplace.

Although there is a great deal of advantages of remote working especially during the pandemic period, the problems that businesses may encounter when adequate safety measures are not taken are more than predicted. This has made digital security, information security and data security more important to businesses nowadays than physical security, which had been more focused for many years.

The necessary precautions taken by employers and employees has a critical importance in today’s world. The issue should be addressed carefully from the perspectives of both employers and employees. Regulation on Remote Work **(Regulation)**, which was published by Ministry of Family, Labour and Social Services on 10 March 2021, also imposes various responsibilities on both employers and employees, similar to those mentioned below. The importance of information security is highlighted by forming a framework of how employer and employee will act in terms of information security.

First and foremost, employers need to establish a digital security strategy and remote work security procedures. The rules that employees working remotely have to comply with must be determined; which data can be accessed remotely, how to control access devices, remote connection procedure and other similar issues should be linked to clear rules. When remote access to the databases of businesses is made available, security weaknesses would be inevitable to happen. In order to minimize this, required network security should be provided and proactively prepared for possible cyberattacks.

Employees should be more careful than ever before and give importance to safety while working remotely, at least as much as employers. Employees must act in accordance with the rules and procedures set by the employer and avoid actions that may violate information security. It should not be connected to unsecured Wi-Fi networks and the devices used should be protected against harmful software. Strengthening passwords used in accounts and devices, not using devices used allocated to work for personal purposes are examples of measures that employees can take themselves. Another issue that needs to be taken into consideration is fake and harmful content sent to corporate e-mail addresses. Many workplaces are exposed to such similar attacks. Employees should not open e-mails that they are not sure are safe, and should seek support from experts in any suspicious case so as to prevent damage.

As can be seen, employers and employees should fulfil their obligations equally as long as remote working models continue to be implemented.

For further information please contact us at contact@gokce.av.tr

THE Fine PRINT
Gökçe
March 2021
89

Answers. Not theories.

Gokce Attorney Partnership

Editors:

Prof. Dr. Ali Paslı
ali.pasli@gokce.av.tr

Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr

Elif Aksöz
elif.aksoz@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
contact@gokce.av.tr
0 212 352 88 33