THE Fine PRINT

Gökçe

June 2023
115

The Day of Days Has Come: MiCA Published in the Official Journal of EU

The Report Chatbot Applications and ChatGPT Example is Published

Amendments in the MASAK Regulation

Latest Legal News:

The Final Stage of the EU Legislative Process for the AI Act

Recent Developments in the Digital Euro Project

EDPB Updated the Guidelines on Use of Facial Recognition Technology within Law Enforcement Activitie

The Day of Days Has Come: MiCA Published in the Official Journal of the EU

The crypto legislation “Markets in Crypto Assets” (**MiCA**), which was adopted by the European Commission in the past months, was published in the Official Journal of the European Union dated 09.06.2023. MiCA, which has been on the agenda for a long time, has become one of the most detailed and broad regulations published in the crypto asset area with its publication.

The countdown has begun for the actors operating in the field of crypto assets with the enforcement of regulation, different provisions of which will enter into force on different dates. Many obligations for cryptocurrency service providers will enter into force as of 31.12.2024. One of the reasons that make MiCA such a significant regulation is that MiCA will not only regulate crypto asset activities in EU countries but will also set an example for the rest of the world to regulate this field.

MiCA is a regulation that has been worked on since 2018, when crypto assets started to gain popularity and the economic volume of the sector increased. The EU initiated studies on the relevant regulation, due to the following reasons mainly; crypto assets are difficult to follow or cannot be tracked due to distributed ledger technology, can be used anonymously, new users are included in the sector every day, and the possibility of damage to these users increases due to fluctuating market conditions.

Examination of MiCA reveals that the main objectives of the regulation are protection of consumers and investors, transparency, supervision, energy use, prevention of manipulation, offences and money laundering.

The scope of MiCA includes crypto assets that were not previously considered under other regulations. As an example, security tokens covered by the Markets in Financial Instruments Directive (**MiFIDII**) are not considered within the scope of MiCA. In addition, it is stated that the European Securities and Markets Authority will make statements and publish decisions regarding which crypto assets will remain within or outside the scope of MiCA in the coming period.

There are various services related to crypto assets covered by MiCA. Considering these services, it is seen that MiCA categorises services similar to MiFIDII. In MiCA, which stipulates various obligations to be fulfilled, such as obtaining a licence for many services, many services such as storing and managing crypto assets on behalf of third parties, operating a trading platform for crypto assets, transferring crypto assets on behalf of third parties, and receiving and transmitting orders are regulated. Following the publication of MiCA, a regulation similar to the ones brought to the financial markets with MiFIDII was brought to the crypto asset sector.

In addition to the wide scope of services, the regional scope of MiCA will also affect the crypto asset sector worldwide. In case the services within the scope of MiCA are offered in EU countries, they will be considered within the scope of MiCA even if the location of the offering party is outside the EU.

Under the MiCA, several obligations, specifically licensing, are imposed on crypto asset service providers. In addition, the cost of meeting these obligations has also brought controversy. Since many new crypto asset service providers have entered the rapidly growing sector in recent years and service diversity has increased. However, it is not known how many of these service providers can fulfil the obligations in MiCA.

Moreover, after the bankruptcy of some of the biggest actors of the sector in recent months and the victimization of many people due to this reason, it was once again revealed how essential the provisions regarding audit and transparency introduced by MiCA and the obligations imposed on service providers are. It is aimed to create a much safer environment in the crypto asset sector in the upcoming period with MiCA.

As MiCA enters into force, similar developments may occur in Turkey in the coming days. Since Turkey has also enacted regulations similar to the EU directives in areas such as financial markets and banking. In addition, it can be stated that Turkey acts in parallel with the EU in recently regulated areas such as the protection of personal data. The EU's behaviour towards the crypto asset area after MiCA will affect Turkey's approach to this area.

You can reach the full text of MiCA published in the Official Journal of the EU here.

The Report Chatbot Applications and ChatGPT Example is Published

One of the most noteworthy issues of recent years is certainly the developments in artificial intelligence. The use of artificial intelligence has spread to almost all areas and the emergence of many applications, specifically ChatGPT, has mobilised the authorities in many countries.

Authorities are closely observing the developments in artificial intelligence in Turkey. The Digital Transformation Office of the Presidency of the Republic of Turkey published a report titled "Chatbot Applications and ChatGPT Example" (**Report**) on 13 June 2023.

The Report consists of two main sections: "Chatbot Application" and "ChatGPT Example". Chatbots, as of the first part of the Report; is defined as a software that could be used in almost every area of business life and saves time by establishing fast communication with users.

Under the "Chatbot Application" section of the report, the definition, background, varieties and functions of chatbots with examples of the companies that use chatbots are covered in detail. In addition, the Report includes many subheadings, including the potential benefits of chatbot applications for businesses and customers, security and privacy, how they protect user data, potential attack risks and precautions. The "Chatbot Application" section is summarised as follows:

- Chatbots are subject to various classifications. However, they are basically classified as (*i*) rule-based chatbots and (*ii*) artificial intelligence chatbots.
- According to their functions, chatbots are categorised as (*i*) business management, (*ii*) gaming, (*iii*) music, (*iv*) assistant and (*v*) education chatbots.
- According to the interface used, chatbots are divided into three categories: (*i*) menu/button-based chatbots, (*ii*) keyword recognition-based chatbots, and (*iii*) content-based chatbots.
- The Report includes the purposes of use of chatbots and the benefits they provide for businesses and customers.

- In the sub-heading "Potential Attack Risks for Personal Assistant Chatbots", it is stated that the chatbot architecture consists of 4 modules: (*i*) client module, (*ii*) communication module, (*iii*) response generation module and (*iv*) database module. In this chapter of the Report, potential attack risks for each module are included.

- Regarding the security and data protection in Chatbots; (*i*) authentication and authorisation, (*ii*) end-to-end encryption, (*iii*) self-destructing messages, and (*iv*) user contact data, backend side methods are included in the Report.

The second part of the Report focuses on ChatGPT. In this section, ChatGPT is examined in detail under many subheadings, specifically what ChatGPT is, how it works, its usage areas and disadvantages. ChatGPT is defined in the Report as "artificial intelligence developed to fulfil various functions, specifically to provide detailed answers to all queries of users".

The bullet points under the heading "ChatGPT Example" of the Report are briefly as follows:

- The benefits of ChatGPT are outlined in the Report, as increasing efficiency, providing an improved accuracy model and cost savings. However, ChatGPT's limited capabilities such as disinformation, inability to multiply large numbers and inaccuracy in some information are counted among its disadvantages.

- It is stated that ChatGPT has many different fields of use, specifically e-commerce sites, education and entertainment.

- The Report includes detailed explanations on the security risks of ChatGPT such as phishing e-mails, data theft, malware, malicious website and botnet attacks.

With the digital transformation, the importance of chatbots, which are used effectively in various fields such as communication, marketing, entertainment and education, is increasing every day. Moreover, the growth in the chatbot market and the developments in this field with new language models such as ChatGPT developed with artificial intelligence technology are quite noteworthy. Compliance with the regulations enacted in ChatGPT in particular and chatbot technology in general is very essential in terms of minimizing legal risk.

You can reach the full text of the Report here (*only available in Turkish*).

Amendments in the MASAK Regulation

The legislation concerning the prevention of money laundering and terrorism was amended on 27 May 2023. A summary of the amendments is below.

Amendments Regarding the Electronic Notification System. Law on the Prevention of Money Laundering numbered 5549 (**Law**) regulated that notifications to be made to the entities determined by the Turkish Financial Crimes Investigation Board (**MASAK**) shall be delivered electronically, and responses to these notifications can be requested in electronic form.

Accordingly, the Regulation on the Principles and Procedures of the Financial Crimes Investigation Board's Electronic Notification System (**Regulation**) was published by MASAK, specifying that electronic notifications are the primary method for notifications within the scope of the Law for the entities determined by MASAK. The Regulation was amended in the Official Gazette on May 27, and "investment financing companies" and "payment and electronic money institutions" were added as entities that are obligated to use MASAK's system. These organizations are required to open an account in the system established by MASAK to receive electronic notifications.

Although the Regulation came into force upon its publication, these organizations are required to open an account by August 1, 2023. You can reach the full text of the amendments in the Regulation here (*only available in Turkish*).

Amendments Regarding the Appointment of Compliance Officers. Entities determined by MASAK are required to comply with the provisions outlined in the Regulation on the Obligations for Compliance with the Prevention of Money Laundering and Financing of Terrorism (**Compliance Regulation**).

As per the Compliance Regulation, the type of entities determined by MASAK are required to appoint a compliance officer assistant. Certain conditions specified in the Compliance Regulation for the appointment of a compliance officer assistant would not be required until 1 June 2023. These conditions included having worked as a manager, expert, or auditor in one of the entities specified in the Compliance Regulation, or as a manager or expert at MASAK for at least five years. However, as per the amendments in the Compliance Regulation published in the Official Gazette on 27 May 2023, these conditions for the compliance officer assistant will not be required until June 1, 2024. In other words, the enforcement of the relevant provisions has been postponed for 1 year.

You can reach the full text of the amendments made in the Compliance Regulation here (*only available in Turkish*).

The Final Stage of the EU Legislative Process for the AI Act Has Begun

The European Parliament accepted its stance on AI regulation by an overwhelming majority on June 14, clearing the door for interinstitutional discussions to finalize the world's first comprehensive law on artificial intelligence.

The AI Act is a flagship endeavour aimed at regulating this revolutionary technology based on its potential for damage. It takes a risk-based approach, prohibiting AI applications that represent an unacceptable danger and enforcing stringent rules for high-risk use cases.

The main focus of the last-minute attempts to amend the wording agreed at the parliamentary committee level was where to draw the line regarding the kinds of AI applications that should be prohibited. It is reported that the purpose of plenary changes is to send a political statement rather than to change the text.

Within the scope of the AI Act, the EU legislators established a tiered approach for AI models that do not have a specified goal, known as general goal AI, with tougher regulation for foundation models, and huge language models on which other AI systems can be constructed.

The first layer concerns generative AI, such as ChatGPT, for which the European Parliament intends to mandate the labelling of AI-generated material and require the disclosure of copyrighted training data.

Reporters were told that the Parliament wants to anticipate the legislation's two-year application time, if not for all forms of AI, at least for foundation models or generative AI, considering the disruptive consequences these models are currently having.

The list of prohibited practices was extended to subliminal techniques, biometric categorisation, predictive policing, internet-scrapped facial recognition databases, and emotion recognition software is forbidden in law enforcement, border management, workplace and education.

An additional layer was introduced for AI applications to fall into the high-risk category, while the list of high-risk domains and use cases in law enforcement and migration control was refined and expanded. Popular social media recommender systems have been classified as high-risk.

Risk management, data governance, and technical documentation requirements for high-risk AI providers were strengthened. Assessments of the potential effects on fundamental rights and the environment were made subject to new regulations.

The Commission was given the important task of resolving conflicts between authorities, but an AI Office was set up to help collaborate on cross-border issues.

The members of the European Parliament will now engage in trialogue conversations with the EU Council of Ministers, which represents European governments, and the European Commission.

According to the interpretations, high-risk categories, basic rights, and foundation models are expected to be the key topics of debate. On the other hand, technical solutions to problems like governance, innovation, and AI definition are probably in order.

It is considered to be essential for companies operating in the field of AI to initiate compliance processes already, within the scope of the fiction designed by the EU.

You may access the details of the vote at the European Parliament session on 14 June 2023, and the AI Act here.

Recent Developments in the Digital Euro Project

In recent years, the increase in the use of cryptocurrencies has raised the risk of reducing the effectiveness of the European Central Bank's (**Bank**) monetary policies. Accordingly, the project of issuing a "digital euro" in July 2021 was put on the agenda by the Bank in order to strengthen the monetary and payment systems. The digital euro refers to the electronic version of the euro banknotes and coins currently in use. Moreover, the digital euro was intended to enable individuals and private companies to hold accounts directly with Bank for the first time.

Following the announcement of the relevant project, one of the curious issues was what the legal status of the digital euro would be and whether the digital euro would replace cash. In the statement made by Bank; it was stated that the digital euro complements cash, and that cash will continue to exist in European Union countries using the euro currency. In addition, it was intended to provide the digital euro with the status of a legal payment instrument.

In recent months, the European Parliament has published a report on the relevant subject. In the report published by the European Parliament dated 19 April 2023 (**Report**), the issue of Central Bank Digital Currency (**CBDC**) was discussed. CBDC refers to digital currencies issued by the authorised central bank in accordance with the applicable legislation.

Report contains details on the eagerly awaited regulations in EU and provides insights into the digital euro project. Report includes ten key issues that the digital euro may possibly face, and under each heading, the importance of the issue, whether it has been sufficiently researched, and what should be done if it has not been adequately analysed. In addition, the Report underlined the necessity for Bank to continue its research on the digital euro.

You can reach the full text of Report published by the European Parliament here.

The meeting on the draft legislation on the confidentiality and distribution of the digital euro, which was scheduled to be held by the European Commission on 28 June, has been postponed. The draft legislation was expected to prohibit the payment of interest or surcharges on the use of the digital euro. However, the draft legislation aimed to make the digital euro primarily a retail payment option, not only for banks, and to ensure that it is accessible to public. In addition, it was expected that it would not be mandatory to accept digital euros unless a special agreement was concluded in advance; digital euros were expected to be convertible into banknotes and coin.

The European Commission has not yet announced a new date for the meeting on the digital euro draft legislation. Nevertheless, in case the draft digital euro legislation is provided with the green light when the meeting takes place, it will completely change the dynamics in the relevant sector.

EDPB Updated the Guidelines on Use of Facial Recognition Technology within Law Enforcement Activities

The final guidelines on the application of facial recognition technology in law enforcement have been released by the European Data Protection Board (**EDPB**) on May 17. The initial version of the guidelines was published and opened to public consultation in 2022. Guidelines assess the risks posed using facial recognition systems in terms of the protection of personal data and provide recommendations for implementers.

The final version of the Guidelines, which are similar to the guidelines from May 2022, include some additional clarifications:

- Guidelines stipulated that they explicitly cover the processing of biometric data solely through the use of facial recognition technologies.
- Guidelines emphasized the principle of accountability and highlighted that logging is merely one of the fundamental elements of this principle.
- Guidelines stated that a central safeguard to the fundamental rights at stake is effective supervision by the competent data protection supervisory authorities.

You can reach the latest version of the guidelines here.

THE Fine PRINT
Gökçe
June 2023
115

Answers. Not theories.

Gokce Attorney Partnership

Editors:

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

Doç. Dr. 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
info@gokce.av.tr
0 212 352 88 33