THE Fine PRINT

Gökçe

February 2022

99

LONG-AWAITED "TELEMEDICINE REGULATION" ENTERED INTO FORCE!

User Security Criteria by Data Protection Authority

Employee Stock Option Plans (ESOP) and the Practice

Latest Legal News:

Constitutional Court Stayed on its Course: WhatsApp Conversations are in the Scope of Private Life

Will Google Analytics be Banned in Europe?

Long-Awaited "Telemedicine Regulation" Entered into Force!

Regulation on Delivery of Remote Healthcare Services **(Regulation)** was published in the Official Gazette on 10 February 2022 by Ministry of Health **(Ministry)**. Regulation regulates the procedures and principles regarding the scope of remote health service, providing permits to facilities to provide this service, development of remote health information system and audits. Regulation has been expected for a long time by the health sector and technology subjects who desire to serve to this sector.

The definitions of "remote healthcare service", "healthcare facility" and "remote healthcare information system" were entered into the legislation with the Regulation. The general approach of the Regulation is to regulate the ability of healthcare facilities to provide remote healthcare services. On the other hand, the remote information systems are information systems that are available for audio-visual communication in order to provide these remote healthcare services.

The main regulations introduced by Regulation are as the follows:

- The healthcare services were set forth as numerus clausus in the Regulation as medical examination, observation and consultation, services for the provision of psychosocial support services, evaluation of clinical parameters related to remote monitoring of diseases, necessary medical procedures to protect the health of individuals in endemic or epidemic outbreaks, and e-prescription and e-report issuance procedures which can be provided remotely by healthcare facilities provided that their qualifications are suitable for remote healthcare service delivery.
- Health institutions and organizations that seek to provide remote healthcare services are required to obtain a permit from the Ministry. Health institutions that obtained the permit from the Ministry will be able to provide remote healthcare services as a "permitted healthcare facility" in accordance with Regulation.
- Remote healthcare service can only be provided through a remote health information system which is provided by Ministry or in case it is provided by third parties, such system should be approved and registered by the Ministry.
- Before providing the remote health service; it is obligatory to provide various information to the recipient; such as the identity and expertise of the healthcare professional who will provide the healthcare service, that the remote healthcare service cannot be the equivalent of in-person healthcare service, that the nearest emergency service should be consulted in an emergency, the fee and scope of the service and that the recorded personal data will be transferred to Ministry's system.
- The video or audio recording of the remote health service can only be taken with the explicit consent of the parties. Relevant records can be kept for a maximum of twelve months at the remote healthcare facility or in secure data centers permitted by the Ministry.

Nevertheless, there are no detailed provisions in the Regulation on remote health service information systems and the permit to be obtained from the Ministry for such.

Although the Regulation entered into force on the date of its publication in the Official Gazette, a 6-month transition period was envisioned for the health institutions that currently provide remote healthcare services to obtain a permit from the Ministry within the scope of the Regulation. You can find the full text of the Regulation here (only available in Turkish).

You can visit https://gokce.av.tr/en/english-publications/ for similar articles.

User Security Criteria by Data Protection Authority

Public Announcement on Technical and Administrative Measures Recommended to be Taken by Data Controllers Regarding User Security **(Announcement)** was published on Personal Data Protection Authority's **(Authority)** website on 15 February. Announcement provides guidance for the measures to be taken in accordance with the obligation to "take all necessary technical and administrative measures to ensure the appropriate level of security regarding personal data" that is set forth Personal Data Protection Law's **(Law)** Article 12. In Announcement, it is recommended for data controllers to make their own risk assessments and to implement appropriate measures regarding their activities.

It is stated that Announcement was published due to the violations reached to Authority resulting from the failure to take the necessary administrative and technical measures in sectors such as finance, e-commerce, social media, and gaming.

It is possible to gather the recommendations in Announcement under three categories.

Measures regarding passwords:

- Reminding users that the same password should not be used on more than one platform,
- Creating a password policy and ensuring that passwords of the users are changed periodically or reminding the users to change them,
- Preventing newly created passwords from being the same as old passwords (at least the last three), and
- Ensuring that passwords are at least 10 characters long and strong passwords are created from the combination of upper-case and lower-case letters, numbers, and special characters.

Measures regarding IP address/device:

- In case of logging in on devices other than the devices that provide frequent access to the users' accounts, sending login information to the contact addresses of the users via e-mail/SMS or similar means,
- Limiting the number of failed login attempts from an IP (Internet Protocol Address) address, and
- Limiting the IP addresses allowed to be accessed.

Measures regarding the system:

- Establishing two-factor authentication systems and presenting them to users as an alternative security measure from the membership application stage on,
- Protecting applications with HTTPS (Hypertext Transfer Protocol Secure) or in a way that provides the same level of security,
- Using secure and up-to-date hashing algorithms to protect user passwords against cyber-attacks,
- Enabling users to view information on at least 5 successful and unsuccessful login attempts,
- Using technologies such as security codes (CAPTCHA, four processes, etc.) that distinguish computer and human behavior when logging into user accounts, and
- If third party software or services are used for logging into the systems, performing regular security updates and necessary controls of these software and services.

The measures are merely advisory and exemplary. Whether it is included in Announcement or not, every data controller shall take all kinds of measures that are appropriate for their field of activity. Since this obligation is an obligation arising from Law, its importance should be highlighted.

You can find the full text of the Announcement here. (Only available in Turkish)

Employee Stock Option Plans (ESOP) and the Practice

With the increase in competition and opportunities in the business world; companies have been seeking solutions to attract successful and potential employees to their companies and to ensure the continuity of business relations with these employees. One of the first (and not entirely new) solutions that comes to mind is ESOPs. This method has been used frequently for a considerable time, particularly in the USA and Europe. In line with a plan concluded and determined within the scope of the business relationship, ESOP is the name given to the setups that enable the employees to possess the shares of the company or the benefits related to these shares, in addition to/or instead of the wages they are entitled to.

ESOPs

Thanks to ESOP, companies try to ensure the commitment of all employees within the plan (particularly its key employees) to the company and to their job; also to strengthen their motivation. For instance, when a fixed wage employee owns a stake in the company in addition to its salary; it is reasonable to expect the company to be more motivated to grow and increase its earnings. In addition, ESOP is crucial for the development of the company-employee relationship. On the other hand, with ESOP, the company and its founders can also persuade employees to do business with them and make an effective proposal to keep them with the company the longest possible.

It is important to note that by using ESOP, companies limit the amount they allocate to payroll and keep cash flow internally. Although it is not valid for every country, it is also possible that the payments made or the sales of shares, due to ESOP may be subject to tax deductions and exemptions.

There is yet no clear regulation on ESOPs in Turkish law and it has not been adopted in the practice sufficiently when compared to leading countries in the business world. Employee stock options, which became relatively applicable with the entry into force of the Turkish Commercial Code, has become a method preferred mostly by tech companies and startups.

The reasons why startups frequently use this method can be listed as follows; not always having the budget to allocate to high salaries, the difficulty of competing with the leading companies in the sector and the desire to reach the top employees.

Types of ESOP

There are different plans that can be preferred to operate the ESOP setup, and as a result of these plans, there are various rights that companies can provide to their employees.

a. ESOPs which the employee actually owns the shares

In this method, company shares are promised directly to the employee and the employee is made a shareholder in the company. The employee has shareholding rights, primarily financial rights. This method basically consists of three steps.

First, the company grants **(Granting)** that the employee will have the right to own shares of the company, provided that the employee fulfills the specified conditions and/or the employee has worked for the company for a certain period. At this stage, an agreement is signed between the employee and the company and/or the shareholder providing the option, in which the details of the plan and its implementation are drawn up. However, at this stage, no share transfer or capital increase takes place and only a commitment is made for the right.

In the second stage **(Vesting)**; with the fulfillment of the terms and conditions set out in the agreement, which the parties have previously agreed upon (particularly in commercial terms), the employee is entitled to the share option. If the conditions determined by the parties are not fulfilled, the employee cannot be entitled to the share option and cannot proceed to the final stage.

The mechanism determined in the agreement between the parties and its details are very important. In the agreement; details such as the termination of the employment relationship for certain reasons and whether the employee will be entitled in such a case should be prepared very well and detailly.

In practice, there are provisions known as Good Leaver and Bad Leaver.

Good Leaver means the termination of the employment relationship with the company for reasons not usually caused by the fault of the employee. Bad Leaver, on the other hand, means the severance of ties of the employee with the company due to the employee's fault. These concepts will vary for each agreement.

In the third stage, as a result of fulfilling the terms and conditions determined in the ESOP, the employees acquire the company shares by using these rights they have won **(Exercising)**. To the extent permitted by Turkish legislation, the last stage is exercised by; **(i)** increasing the capital and issuing the new shares or **(ii)** undertaking the transfer of shares to the employee by the existing shareholders.

b. Phantom Stock Option Plans

Sometimes companies and/or shareholders may not want to allocate real shares to their employees. The reasons may be listed as; (i) the operational difficulties that may arise, (ii) the desire to avoid granting shareholding rights to employees (e.g., the right to get informed, participation in the general assembly and voting rights, minority rights), (iii) the desire to stay away from the processes regarding share transfer restrictions, deterioration of the shareholding structure and difficulties in related transactions.

Accordingly, if certain terms and conditions are met, the company may promise its employees a payment indexed to the sales price. In practice, this contingent payment method is called phantom stock option. With this method, instead of directly owning the shares themselves, employees are entitled to financial rights related to these shares (such as dividends) or to payments corresponding to the exit values of these shares.

Conclusion

ESOPs serves purposes such as; improving employee-employer relations, increasing employee loyalty to the company, enabling start-ups to compete with the market, and increasing company productivity and income. ESOPs seem to appear more frequently as the Turkish start-up ecosystem grows day by day. In this context, we are eagerly awaiting whether any legal regulation will come soon.

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

Constitutional Court Stayed on its Course: WhatsApp Conversations are within the Scope of Private Life

The Constitutional Court's **(Court)** decision dated 28 December 2021 **(Decision)** was published in the Official Gazette on February 11. The decision is related to the examination of applicant's WhatsApp conversations by their employer and the termination of his employment agreement based on these conversations.

It is stated in the Decision that the supervisor of the applicant acquired the WhatsApp conversations when the applicant, who sent texts from his business computer, left the computer open. It is also stated that the employer detected insults, slander, and threats in the conversations and thus, the employment agreement of the applicant was terminated immediately without any notice. The applicant applied to the Court with the allegation that his right to respect to privacy and the freedom of communication was violated, following the exhaustion of all legal remedies.

The Court restated the principles on which its previous decisions were based and emphasized that the conflicting interests between employers and employees should be balanced fairly. Accordingly, the evaluation has been made in the context of the employee's right to respect to private life and freedom of communication, along with employer's authority to supervise the employee's communication.

While it was stated that the employer could supervise the communication devices assigned to the employee, it was once again expressed that this authority should be limited to the execution of the work in the workplace and limited to ensuring the order and security of the workplace. It was also underlined that full and clear information should be provided by the employer in advance. Thus, the Court laid down the basic rules regarding the supervision of employee's communication in parallel with its previous decisions.

Considering the Decision, it could be stated that the conditions for employer to audit the communication devices assigned to employees' use in the workplace are as follows; *(i)* employers should inform the employees fully and clearly in advance, *(ii)* the supervision should be balanced with employee's rights and freedoms and *(iii)* it should be based on legitimate purposes. It is essential for employers to implement the necessary measures and to prepare and enforce the privacy and supervision policies regarding the workplace.

The full text of the Decision can be found here.

Will Google Analytics be Banned in Europe?

Data protection authorities across the European Union **(EU)** have been ruling that the use of Google Analytics breaches the General Data Protection Regulation **(GDPR)** recently. So far there are three decisions in this direction and even more cases are under investigation.

This all started when European Center for Digital Rights **(NOYB)** filed 101 complaints in 2020. These complaints were against European companies that transfer data to Facebook and Google and NYOB claimed it is a violation of GDPR since data were transferred to the United States of America **(US)**. And one of the transfer methods, probably the most used, is Google Analytics.

Google Analytics is widely used by website owners to receive statistics on their website traffic. However, when Google acquires the data, data transfers to Google's servers in the US. According to the claim of NYOB this data is vulnerable to US surveillance such as US intelligence agencies since foreigners' data aren't protected with the same standards as US nationals.

European Data Protection Supervisor **(EDPS)** was the first one to rule that using Google Analytics violates GDPR following the European Parliament's use of Google Analytics on their Covid-19 testing website. Following this decision, the Austrian Data Protection Authority (**ADPA)** and French Data Protection Authority **(CNIL)** respectively ruled that websites in their cases breached GDPR by using Google Analytics and making personal data vulnerable to US intelligence agencies. CNIL also added that even though Google adopted certain measures such as encryption, they were not sufficient.

This all shows that companies that use analytics tools or cookies must be very cautious in terms of data transfers outside of the EU in order to comply with GDPR.

You can find the EDPS decision here, ADPA decision here (only available in German) and CNIL decision here (only available in French).

THE Fine PRINT
Gökçe
February 2022
99

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