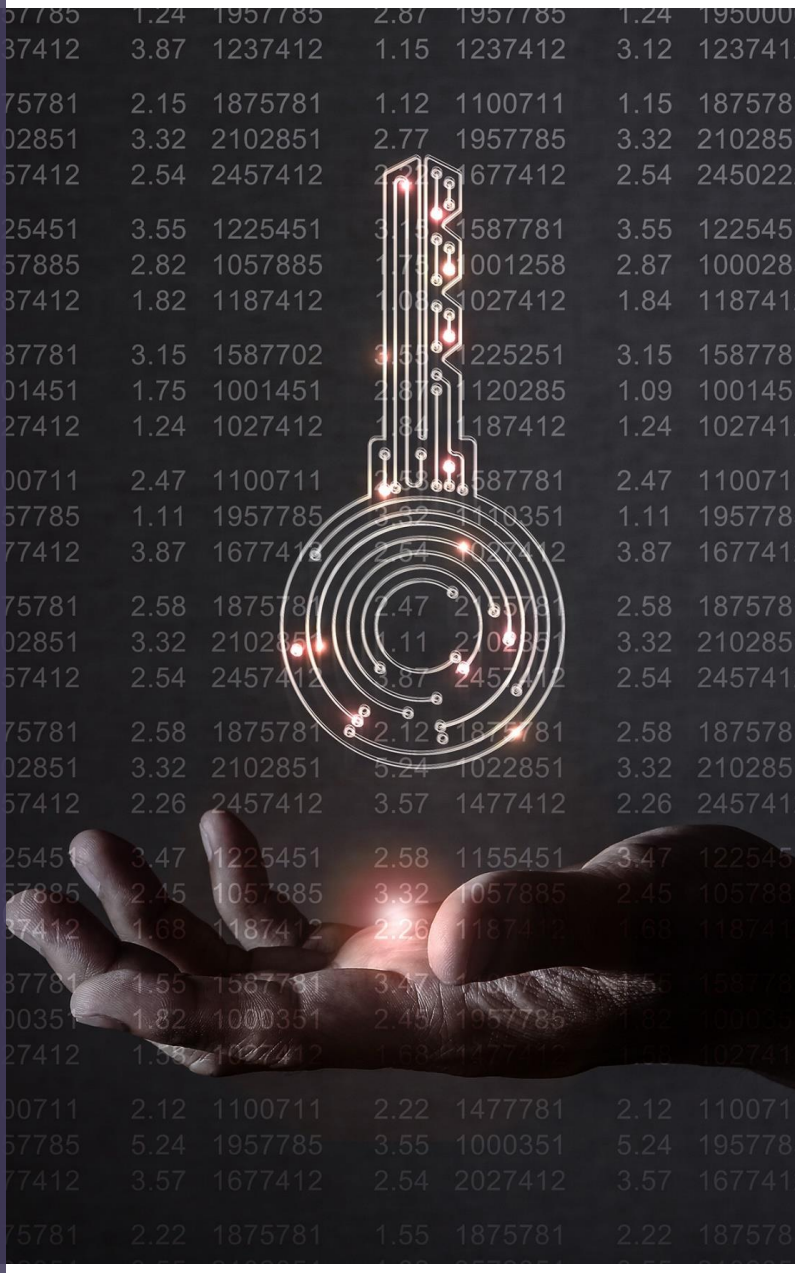
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

MARCH 2020

DECISION SUMMARIES OF THE MONTH AND NEWS

Decision Regarding the Disclosure of Personal Data to Third Parties by a Lawyer as Data Controller

Decision No: 2020/26 **Decision No:**14.01.2020

Subject: Decision Regarding the Disclosure of Personal Data to Third Parties by a Lawyer

In the bill of complaint submitted to the Authority, the data subject stated that he/she was called and received messages about the execution proceedings initiated by the data controller due to his/her debt to the bank, that the messages with the same content were sent to his brother, but when the data controller applied to the lawyer, the lawyer stated despite the evidence, he did not contact anyone other than the data subject.

As a result, the Authority asked the data controller lawyer for his/her defense and in the defense of the lawyer, it has been stated that:

• In accordance with the profession of lawyers, learning/obtaining the personal data of individuals is not a data processing activity and nobody's data is processed by them as a law firm,

• In accordance with the provision of 1/b of Article 28 of the Law, lawyers should also be considered as judicial authorities and exempted from the scope of the Law,

• The relevant person's information such as Turkish Identity Number, address and assets have been publicized by giving them to the bank,

• The phone number subject to the examination has been provided to the data subject from the person who came to the law firm and wants to get information about the debt, the phone number was entered in their system in this way and deleted from the system upon application,

• It was stated that the data subject did not give any instructions to the bank not to share the data with third parties and it was conveyed to the Authority that there was no information and document related to the data subject in question in the context of the Law.

As a result of the examination made by the Board,

• That the act of processing the contact information and other relevant information by the lawyer to collect the debt of the data subject to the bank is data processing activity,

• That within the scope of the law, in order for a data to be accepted as personal data, it is required to have a specific or identifiable natural person, and in the message sent to the brother of the data subject, the name of the data subject, the bank to which he/she owes and the information about the debt of the execution file, that is, personal data of the data subject is contained,

• In the aforementioned event, in order to protect the rights and interests of the Bank, who is the client of the data controller lawyer, within the framework of the legal legislation, is authorized to process the information of the debtor in accordance with the law, and to notify the relevant units and authorities pursuant to Article 5 of the Law; however, sharing the personal data of the data subject to a third person cannot be considered under Article 5 of the Law,

• That obtaining the phone number from the person who comes to the law office cannot be under the scope of Article 5 of the Law, and the processing of the phone number of the data subject is not lawful,

• It is an act contrary to the obligations regarding data security to transmit the data of the data subject to an unidentified person and to an unknown number.

• That the data processing activity of the lawyer, which is the founding element of the judiciary and which it performs on the data obtained by betting by its profession, cannot be accepted and the defense that it is within the scope of the exemption pursuant to Article 28 of the Law, in case the data processing is related to the investigation, prosecution, judgment or execution proceedings, the exception may be mentioned and with the conviction that the message to his brother as a deterrent mechanism for the data subject to pay his debt cannot be considered in this context, as a result of obtaining an unknown number by a third party with an unknown identity the contact person's data is shared with this number, an administrative fine of 50,000 TL was imposed on the data controller acting in violation of Article 12 of the Law.

Decision on Missing to Fulfil the Request of the Data Subject

Decision No: 2020/13 **Date of Decision:** 26.12.2019

Subject: About the rejection of the request for access to the phone call records made with the data subject in connection with the transactions regarding the brokerage agreement signed between the data controller company and the data subject

The data subject made an application to the Authority and requested that the matter be examined within the scope of the KVKK upon the rejection of the request of the telephone conversation records to be given to himself/herself made with the data subject based on the agreement signed with the data controller within the scope of the brokerage activity.

With the examination of the relevant situation, it has been decided that;

• That the right of the person to request information regarding the processed personal data within the scope of the Paragraph 1 / b of the Article 11 of the Law also includes the right to access the related data, that this would allow him/her to have full knowledge of how his/her personal data is processed so that he can exercise his rights over his personal data, however, this right does not allow access to the recording system/medium where the data is processed, the delivery of the recording medium to the data subject or the acquisition of the data itself, but to the extent allowed by technical/physical facilities and that the content of the data is reasonably accessible to the data subject,

• That the recordings related to the sound recordings requested by the data subject from the data controller will not be realized by the direct delivery to the data subject; but can be realized by granting them access requested sound recordings to their record documents, which will allow them to fully understand the content of the data,

based on the paragraph 5 of the Article 15 of the Law, it has been decided that the call record documents regarding the phone call records subject to the complaint application to the data subject by taking the data security obligations into consideration and to inform the Board about the transactions.

Decision Regarding the Processing of the Data Subject's Mobile Phone Number Without Any Data Processing Requirements and Sending an Ad/Informational Message to the Related Number by an Educational Institution

Decision No: 2020/20 **Date of Decision:** 14/01/2020

Subject: About the complaint regarding the processing of the mobile phone number of the relevant person without any terms of data processing and sending an advertisement / informative message to the relevant number

Following the examination of the complaint application made by the data subject to the Board due to the failure of the data controller to respond to the data subject, on messages sent to the mobile phone without the explicit consent of the data subject by an educational institution for informative & advertising purposes;

Although the letter sent by the Authority to the Educational Institution regarding the request of the relevant information and documents has been delivered to the permanent employee of the workplace, considering that the data officer did not respond to neither the data subject nor the Authority, when the existing information and documents are evaluated; the Board decided to impose an administrative fine of 50.000 TL on the Educational Institution, which processed the data illegally by sending messages with information and advertising purposes to the mobile phone number of the data subject without having the explicit consent of him/her or the processing conditions listed in the relevant article of the Law, and it was considered that the Educational Institution failed to take the necessary administrative and technical measures in this context.

Decision on the Delivery of a Credit Card to Third Parties by a Bank Without the Consent of the Data Subject

Decision No: 2020/32 **Date of Decision:** 16/01/2020
Subject: Delivery of the credit card to third parties without the consent of the data subject

Since the renewed credit card was delivered to third parties without the consent of the data subject and his/her personal data was revealed, the data subject requested the Authority to take necessary actions about the Bank.

In the examination made by the Authority, it has been understood that the courier was to make the distribution to the principal address of the data subject in the first place, which is registered in the system of the Bank; yet, the courier was unable to deliver it; that SMS notification could not be made due to the person's phone being out of service and delivery was made to a person at the secondary address of the data subject registered in the Bank system; whereas, since the relevant the phone number of the data subject was out of service, no information could be sent; after the data subject contacted the customer service, the card was delivered to the secondary address registered in the system, which is the former workplace of the data subject.

As a result of the evaluation of the relevant application, following points have been identified,

• The Bank, which keeps information about the data subject and credit card in the current event, is the data controller; The Courier, who delivers the credit card in a sealed envelope, is not a data controller, since he does not have access to the card information and cannot process this data,

• The courier company is the data controller; since it is obliged to record the receiver and sender information in a complete and accurate manner,

• The courier is in violation of his contract with the Bank regarding the identification of the persons to whom the credit card will be delivered and this may be the subject of a dispute regarding the Law of Obligations,

• Although there is a defense that the necessary information is not updated by the data subject, the necessary attention is not paid to make the necessary checks by the courier during delivery.

• The bank does not make sufficient and reasonable efforts to take administrative and technical measures to be taken during the card delivery and to keep the personal data up to date,

It was decided to impose an administrative fine of 50,000 TL to the Bank.

Gratis – Data Breach Notification

According to the data breach notification made by Gratis İç ve Dış Tic. A.Ş.; in the breach which was realized between 04.03.2020 and 06.03.2020 and identified on 06.03.2020, it has been reported to the Authority on 09.03.2020, that an e-mail was sent to the Company's e-mail by an unidentified person about the seizure of the e-mails and passwords of the members of the Company's website, 2092 people were affected by the said data breach; the affected personal data were identity, communication information and customer transaction information. The data subjects can obtain information on the data breach by sending an e-mail to info@gratis.com and calling 0 850 210 69 00. The relevant breach has been announced on the web page of the Authority and the investigation on the subject is continuing.

Türk Ekonomi Bankası A.Ş. – Data Breach Notification

According to the data breach notification made by Türk Ekonomi Bankası A.Ş, the breach which occurred between 01.01.2018 and 28.01.2020 and identified on 02.03.2020, it has been performed by bank employees by sharing query results information of Risk Center Report of The Banks Association of Turkey with third parties via their personal phones, there may be 2317 non-bank customers and 6917 bank customers affected by the breach. However the exact number of the people affected by the breach could not been identified, the affected personal data are information about the credibility of the persons concerned (credible, non-credible), it has been reported to the Authority on 05.03.2020 that the data subjects can obtain information on the data breach from the Call Center of Customer Satisfaction Department (by dialing 0850 200 0 666), by sending e-mail to the address kvkkbasvuru@teb.com.tr and through web site http://www.teb.com.tr. The relevant data breach has been announced on the web page of the Authority on 09.03.2020 and the investigation on the subject is continuing.

Doğa Sigorta A.Ş. – Data Breach Notification

According to the data breach notification made by Doğa Sigorta A.Ş., it has been reported to the Authority on 06.03.2020 that the breach which occurred on 28.02.2020 and identified on the same day was realized by hacking the test server of the company's web page; the breach, where the estimated number of affected people are 300, the personal data categories relevant to the breach are identity, communication, license plate, vehicle license and finance data, the data subjects can obtain information on the data breach through www.dogasigorta.com. The relevant violation was announced on the web page of the Authority on 09.03.2020 and the investigation on the subject is continuing.

Dutch DPA (AP) Imposed 525.000 EUR Fine To Tennis Association KNLTB, Due To Selling Personal Data Of Its Members

In 2018, the KNLTB tennis association unlawfully provided personal data of a few hundred thousand of its members to two sponsors for a fee.

Sponsors were provided with personal data such as name, gender and address; one of the sponsors reached more than 50.000 members and the other one reached more than 300.000 members to provide different offers.

Although KNLTB claims to have a legitimate purpose on the transfer of these data, AP decided that KNLTB has no legal ground to share these personal data with sponsors.

Polish DPA Fines 20,000 PLN to School Processing Biometric Data of Students

In Poland, a school processes the biometric data of 680 students in the sensitive personal data by obtaining consent from the parents or legal successors of the students without any legal basis to determine that the students pay the food fees at the canteen entrance, and it uses alternative identification systems (with electronic cards or by name and contract number) for 4 students.

It is stated in the lunch rules on the school website that students without biometric identity have to wait at the end of the queue until all students with biometric identity enter the canteen, and after all students with biometric identity enter the canteen, students without biometric identity are allowed to enter the canteen.

According to the President of the Data Protection Authority, students with biometric identity are clearly supported, and students are treated unequally and differentiated.

This school, which processes biometric data of students in the canteen and acts unequally in this regard, has been imposed a fine of 20.000 PLN by the Polish DPA.

Icelandic Supervisory Authority (SA) Fines 20,643 EUR to National Center of Addiction Medicine

National Center of Addiction Medicine, which is also a rehabilitation center, is an NGO that operates a family services center and social center in Iceland. When a former employee went to the Center to take his/her personal belongings, it was found in the delivered boxes to the person that there were records of 252 elderly patients with health records and the names of approximately 3,000 people who started rehabilitation due to alcohol and substance abuse.

In the examination conducted by the Authority, it was decided that the breach occurred as a result of the failure to implement appropriate data protection policies and appropriate technical and organizational measures to protect the data by the data controller, and an administrative fine of 3.000.000 ISK (20.643 EUR) to be imposed.

The Icelandic SA noted that when determining the penalty, the nature of the violated health data and the scope of data processing are taken into account, that the National Center of Addiction Medicine operating as a nonprofit healthcare provider, has made substantial efforts to improve the processing of personal data before the data breach occurred.

A School by Icelandic SA Has Been Fined of 8.945 EUR

In the e-mail sent by a teacher in Breiðholt Secondary School, in which examination appointments were to be shared; a data breach occurred by sharing a document with 57 people, about a different group of students of 18 in total, regarding their welfare levels, study performances, social conditions, problems and even the physical illness of a student and another student's mental health problem, instead of the relevant document.

In the examination made by the relevant Authority, it was concluded that the breach occurred as a result of the failure to apply appropriate data protection policies and appropriate technical and organizational measures to protect the data by the data controller, and an administrative fine of 1.300.000 ISK (8.945 EUR) was imposed to Breiðholt Secondary School.

Suggestion of Penalty by the Danish DPA for Two Municipalities

In the investigations made by the Danish DPA as a result of the reporting of data breaches occurred with the theft of computers of both municipalities, it has been determined that the fact that computers are not protected by passwords by both municipalities causes data breach and this breach poses an unnecessary risk for citizens.

It has been found that in the first breach, due to the lack of security from the computer stolen from the Gladsaxe City Hall, the data of 20.620 citizens including sensitive data were affected, in the second breach approximately 1.600 people working in the municipality were affected, including sensitive data, when the computer of an employee in the Hørsholm municipality was stolen from his car.

The Danish DPA notified the municipalities to the police, as it determined that the municipalities did not meet adequate security requirements in accordance with the GDPR, and proposed fines of 100,000 DKK to Gladsaxe Municipality and 50,000 DKK to Hørsholm Municipality.

Administrative Fine to Google by Swedish DPA

In 2017 the Swedish Data Protection Authority (DPA) made an audit concerning how Google handles individuals' right to have search result listings for searches that includes their name and the DPA concluded in its decision that a number of search result listings should be removed and ordered Google to do so, accordingly.

In 2018, due to indications that Google had not fully complied with the order that was given previously, the DPA initiated a follow-up audit.

This audit has yet to be completed and the Authority fined Google with an administrative fine of approximately 7.000.000 EUR on the grounds that it did not fulfill its obligations regarding the right to request listing as a search engine operator.

Croatian DPA (AZOP) Imposed a Fine of 20.000.000 EUR to a Bank

With the rejection of request to access to personal data of approximately 2.500 customers using a loan at a bank, it is claimed that "the right of the data subject to access his/her personal data" has not been fulfilled according to article 15.3 of GDPR.

Citizens frequently requested information from the Bank; however, it was found that the Bank prevented the applicants from exercising their rights for more than a year.

It was found that the Bank is aware of the protection of fundamental rights guaranteed by the regulation; it has been determined that the Bank acted intentionally and deliberately on the breach of the obligation, and the Bank was given an administrative fine of 20.000.000 EUR considering that this situation led to a serious breach.

Announcements by Data Protection Authorities Made Within the Scope of Covid-19 Outbreak

Regarding the Covid-19 outbreak, European Data Protection Board (EDPB), Data Protection Authorities (DPAs) in France Ireland, Italy and Turkey have made announcements about the measures to be taken in this context, the points to be taken into consideration for the protection of personal data, and in which scope the health data and other personal data can be processed by the relevant parties

These announcements briefly include:

European Data Protection Board

EDPB explained that GDPR includes the necessary arrangements for employers and health authorities to process the health data of individuals and in this context, there are some requirements for the data to be processed without explicit consent of the persons.

In this context, employers can process data to protect public health and interests or to comply with other legal obligations. In addition, data such as mobile location data can be processed by applying additional privacy measures, such as anonymous processing. If it is not possible to process the data anonymously, the activity should be performed if necessary and appropriate and proportionate.

Following this announcement, on 19.03.2020, EDPB elaborated the subject, by making explanations in terms of compliance with the law, answered questions about collecting location information and processing employee data. You can access the related text via this link.

France DPA (CNIL)

The French Data Protection Authority ("CNIL") declared that it is not appropriate for organizations to take measures that only health institutions can take and implement. For example, practices such as measuring the body temperature of the employees regularly or conducting surveys to people in this direction should be avoided.

In this context, the measures that organizations can take are to conduct studies to raise awareness of employees and to encourage remote working.

In accordance with the French legislation, an employee must inform his/her employer if he or she is suspected of contact with the virus to ensure the safety of himself/herself and others. In other words, the employer should not get this information compulsively from the employee.

Finally, CNIL has announced that health data can only be collected by the health authorities and that it is the responsibility of public authorities to take such precautionary measures.

Ireland DPA (DPC)

According to the statement of Ireland DPA ("DPC"), the legislation on protecting personal data is not ahead of public health, but the processing of health data and other special personal data within the scope of measures taken for coronavirus should be proportionate and based on a purpose. The measures taken in this context should be in line with the instructions of public health authorities and other relevant authorities and these authorities should be informed.

According to the announcement, organizations must fulfill some obligations. Namely; personal data should be processed within the framework of Articles 6 and 9 of GDPR. In addition, the subjects should be informed by providing transparency, a complete confidentiality about the data should be provided, only as much data as necessary should be processed, and the measures taken in this regard should be accountable.

Italian Data Protection Authority (Garante per la protezione dei dati personali)

According to the announcement issued by the Italian Data Protection Authority, it has been stated that they switched to digital working methods within the framework of the measures taken by the Italian government and will not accept visitors until April 3. It has been declared that the documents to be sent to the authority should only be transmitted by digital means, not physically.

- E-Mail to: protocollo@gpdp.it
- PEC mail to: protocollo@pec.gpdp.it
- Complaint application form mail to: cyberbullismo@gpdp.it

Turkish Data Protection Authority (KVKK)

On 27.03.2020 Turkish Data Protection Authority ("KVKK") explained what needs to be known in the process of struggling against Covid-19 in the scope of KVKK with a public announcement and answered frequently asked questions. In the announcement it has been stated that the measures to be taken to prevent the spread of Covid-19 virus should comply with the general principles of law and should not cause irreversible harm in terms of fundamental rights and freedoms. In this context, the principles of lawfulness, transparency, confidentiality and data minimization should be taken into account during data processing activities. In this context, the principles of lawfulness, transparency, confidentiality and data minimization should be taken into account during data processing activities. In addition, the Authority announced that decisions on this issue should be taken in accordance with the instructions of the Ministry of Health and other authorized public institutions and organizations.

With these explanations, the Authority answered important questions in terms of health institutions, employers and employees and obligations to the institution. You may access further information on the subject via this link.

In the announcement made by Turkish Data Protection Authority dated 23.03.2020, it has been declared that regarding the obligations to the Authority, for the processes to be fulfilled within certain deadlines, the extraordinary situation that the entire world is going through will be taken into consideration.

Besides, in the announcement dated 18.03.2020, KVKK has announced that the applications to be made to the Board should not be made by in person delivery, but via courier, regular mail, registered e-mail or via modules on the web page of the Authority.

Modules on the web page of the Authority are as follows:

- Complaint Module: https://sikayet.kvkk.gov.tr
- Data Breach Notification Form: https://ihlalbildirim.kvkk.gov.tr
- VERBIS Applications: https://verbis.kvkk.gov.tr
  (Application form should be sent via registered e-mail or regular post.)

INFORMATION GUIDE

Coronavirus (COVID-19) Pandemic and Its Relation with KVKK

Affecting the whole world, the Covid-19 pandemic led organizations to initiate certain precautions in line with the suggestions of the state authorities, to save and secure public health and prevent further spread of the virus. Due to the Covid-19 virus, within the scope of these precautions, the possibility of unauthorized access to personal data has emerged, including health data of employees or third parties. Organizations should be very careful to avoid possible violations which might directly impact the rights and freedoms of persons when taking relevant preventive measures. In this process, organizations can follow the methods in the precautions to be taken, which are elaborated as follows:

1. Remote Working

In order to ensure business continuity, an organization may go for the option of shift to remote working in this period. In such case, if organizations do not already have sufficient technical infrastructure, certain difficulties may be faced. For example, within the scope of this measure taken to protect public health, the personal phone numbers of people who do not use the company phone for communication between people, other employees, business partners, customers, suppliers etc., can be shared with third parties. While this transfer/sharing of information has a legitimate aim, it is well known that it must be based on the explicit consent of individuals. In cases where people do not give explicit consent or withdraw their explicit consent, providing a company line to the person would be an appropriate solution.

2. Visitors

Even though the most appropriate method during interim period is not to accept visitors, in cases where visitors are deemed necessary, questions regarding whether the visitors or the people with whom they have a close relationship show coronavirus symptoms or whether these people have recently traveled can be directed to the visitor and the method of preserving this information by the organization can be followed.

It should not be preferred to obtain health data from individuals, in particular; since it is not within the authority of the organization in accordance with KVKK. Organizations that have decided to implement a precaution in such way should keep this data anonymously or obtain and store it by the workplace doctor (occupational physician) and by applying for the explicit consent of individuals. The data which are not kept anonymously must be stored by workplace doctor in a locked cabinet with no access allowed, and when the purpose to store the data is not applicable any longer, it must be destroyed by the appropriate method. Organizations that do not have a workplace doctors should carry out this activity through a single person they have authorized. Taking measures regarding coronavirus is duty of authorized bodies under all circumstances and the most applicable way in this regard would be not to obtain such data by the organizations in the first place.

3. Collecting Information About Employees and Their Relatives

Recently, organizations have been requesting information on whether the employees and their relatives have shown any of the symptoms of coronavirus in practice, or whether they have recently traveled, in a similar manner to the prevention described for visitors. The purpose of this request is to follow the 14-day protection period of the relevant employee, along with the health of the other employees within the organization. In this context, the information whether the employees or their relatives show the symptoms should be kept anonymously by the organization, the purpose of this information should be to only follow the 14-day protection period. For this reason, only the date when the risk occurred and how the risk occurred should be reported to the organization by the employee, and the identity information of the data subjects or information that can identify them should not be transmitted.

In addition to this, besides obtaining information from the individuals, the practices of health screening the employees in some workplaces (measurement of fever, detection of symptoms) have been started. These practices should definitely be performed by a workplace doctor and the person showing the symptoms should contact the workplace doctor only and direct.

4. Situation of Employees Who Have Positive Coronavirus Test Results or Showing Related Symptoms

As mentioned above, most important point on the subject is that only the workplace doctor shall with the person who has positive test result or shows the symptoms and the doctor shall guide the employee. Organizations that do not have a workplace doctor should also perform these activities through a doctor or an authorized institution.

Even in the presence of a person who has a positive test at a workplace, the name of the person should not be announced in order to prevent the exclusionary actions of individuals, and general information should be provided to the people. The best thing to do here is to guide the person who has a positive test to alert those he/she has a close relationship with.

In addition, when it is realized that there is a positive case of virus among the employees, employees circle of close relationships ora third person who has the coronavirus, this situation must be reported promptly to authorized institutions according to Article 61 of Public Health Law in Turkey. Detailed information on this subject is provided below.

However, according to the statement made by the competent authorized bodies and institutions, patients who have positive test results are going to rest at home or in medical institutions / hospitals with medical reports. The conditions for obtaining and keeping the report or test result obtained from the authorized institution by the employer will be in the same scope as the sick reports. In other words, additional security measures should be taken to keep these reports and this activity should be carried out through the workplace doctor.

5. Employees Working in Public Places Who Are to Meet a Person Showing Symptoms

For example, if people working in public places, such as a courier, a customer representative or a driver, meet a person who shows symptoms during their work, it will be appropriate to inform the competent authorities and take the precautions announced by the competent authorities in order to make the environment suitable for finding, in which the person is exposed. This matter takes place clearly in Article 57 and 61 of Public Health Law in Turkey. As follows, contagious diseases are listed and obligation of notification to authorized institutions is regulated with Article 57. Among the people who have obligation the report to authorized institutions in Article 61 can be listed employees working in public places, health care personnel and the employees who encounter with such diseases due to nature of their work.

It should not be forgotten that it is the duty of the authorized institutions and organizations to take precautions against Covid-19 virus, but individuals also have a great duty. In this context, it is appropriate to take precautions to protect public health as an organization, but it should be ensured that individuals are not exposed to an exclusionary policy while taking precautions, and a balance should be set between their rights and freedoms and public health and safety.

Technical Aspects to be Considered During Working Remotely

Due to the Covid-19 Corona virus epidemic, which is on the agenda of the whole world, many companies switched to remote working. However, some companies could not start working remotely, from homes due to lack of technical infrastructure, while some companies switched to working from home without being aware of the systems that they had to set up in their technical systems and without taking the necessary precautions.

Among the frequently asked questions published by Turkish Personal Data Protection Authority (KVKK) and ICO2 on the subject, the question "What kind of security measures should be taken to work from home?" has been answered stating that data protection is not a barrier to working from home and that usual security measures should be applied during working remotely, as well.

So, what aspects should companies take into consideration when working remotely?

One of the biggest issues experienced during the pandemic was that companies did not have equipment appropriate for handling operations remotely from home. It has been much easier to switch work from home for companies whose computers are portable and communication devices can also be used remotely. In this context, there were those who tried to carry the monitors, and those who could not carry their computers and expected to use their personal computers at home for business purposes. The lesson learned by companies was that screened devices should be provided to people according to the nature of the job. Because the first rule of working remotely is that the quality of work shall be appropriate for working from home.

Besides, requesting the use of personal computers in their homes for business purposes due to lack of equipment would constitute a huge deficit in ensuring cyber security, since personal computers do not have the same systems as office computers. For example, it will not be possible on personal computers to monitor the systems of people who connect to Office365 accounts. Or, since personal computers' USB ports will not be closed, it will be much easier for employees to export company data.

In summary, it is necessary to make sure that the necessary security software is installed on the equipment used for remote working, up to date software is used, and no malware is available. Insufficient equipment will make the company vulnerable to both internal and external attacks.

In addition, during work remotely, employees must have as much system access as they need only by task. Unnecessary access authorizations on critical data should be restricted, in particular. Since the network connections in the home may not have the same security measures as in the company, it is very important to ensure that the established communication is encrypted with VPN and that the use of VPN is mandatory.

Unauthorized access to the network can be prevented by using two factor authentication (2FA) for all employees' authentication processes.

Giving the authorities in accordance with the principle of "least privileged access" in the Guidelines for Safe 'Remote Work' published by the National Cyber Incidents Response Center within the scope of corona virus outbreak measures, the importance of the measures are described as follows: Defining a time-out for maximum connection time on systems, temporary establishment of the rules defined during remote work, "source IP" restrictions for remote connections where possible, multi-factor authentication and time-based authorization measures for access, ensure that remote access is not permitted for access to any critical systems that should not be defined according to the risk assessment.

In addition, full disk encryption must be done on the computers used by employees against a possible theft, sensitive data on computers must also be encrypted to minimize the risk of cyberattack. Setting up the software used for virtual conferences alterative to face-to-face meetings to establish a strong encrypted communication will protect the institutions by preventing remote listening.

Finally, in order to maintain the function of all these measures taken as in any case, cyber security awareness training should be provided to all personnel working remotely and thus, precautions should be taken against a possible human error.

Details regarding the subject can be accessed from our article published in our website.

LEGISLATION ANALYSIS

Interpretation of Processing Personal Data in Order to Ensure Public Safety and Public Order According to the Article 28 of the Law

Article 28 – Exemptions:

(ç) personal data are processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorized and assigned by law to maintain national defense, national security, public security, public order or economic security.

*****

Several measures are taken to prevent the further spread of Covid-19 virus, which is described as a pandemic worldwide. These measures require the processing of health data and location information of individuals, in particular. Although the public interest is considered to be superior when the rights and freedoms conflict with the public interest, the practices carried out must be lawful and have a certain limit. In this context, data protection authorities make explanations regarding the data processing activities and the authorized institutions take the necessary steps to carry out a lawful activity. Data processing activities performed aiming to prevent the further spread of epidemic in Turkey, are intended to ensure public safety and public order and will be exempted from the requirements of the Law, if they meet the requirements of Article 28 of the Law. Accordingly, in order for a data processing activity to be exempted from the law within the scope of the Article 28 / (ç) of KVKK;

• First of all, data should be processed to provide national defense, national security, public security, public order or economic security. Data processing activities carried out in order to prevent the spread of the epidemic in the concrete event are aimed at providing public security and public order.

• Secondly; data must be processed by public institutions and organizations authorized by law. This may be an authority granted by any law. In the current situation, the application shall be more clearly understood with the two examples given below regarding the authority given by law:

• According to the Appendix, Article 2 of the Law for Provincial Administration, the contact and location information of the person making the call can be shared by the 112 call center and the relevant governorship and the Information Technologies Authority. The purpose of this application is to reach the person faster. It is also stated in the article that location information will be limited to the time of call and cannot be used for any other purpose. This is an example of the authority given by law.

• It has been observed in practice that private security officers measure people's fever with a fever meter in order to prevent the epidemic. These officers obtain health data of individuals within the scope of KVKK. Private security officers fulfill the duties set out in the Law on Private Security Services, and the duties and authorizations explicitly included in article 7 of the law, are not regulated to cover processing of health data. Although the General Directorate of Security - Private Security Audit Directorate has explained about the use of a thermometer stating that "it is a reasonable practice until the end of this process", this activity cannot be considered within the scope of Article 28 as it is not an authority granted by law.

• Finally, according to Article 28, the activity carried out should be processed by authorized public institutions and organizations within the scope of preventive, protective and intelligence activities. In the current situation, it is fixed that the activities are carried out to prevent further spread of the pandemic and protect people from the epidemic.

Although data processing activities that meet the conditions, we have explained above are exempted, authorized bodies and institutions should not interfere with the privacy of private life and personal data; they should the acquired data in accordance with the purpose of obtaining it.

Follow Us on Social Media...