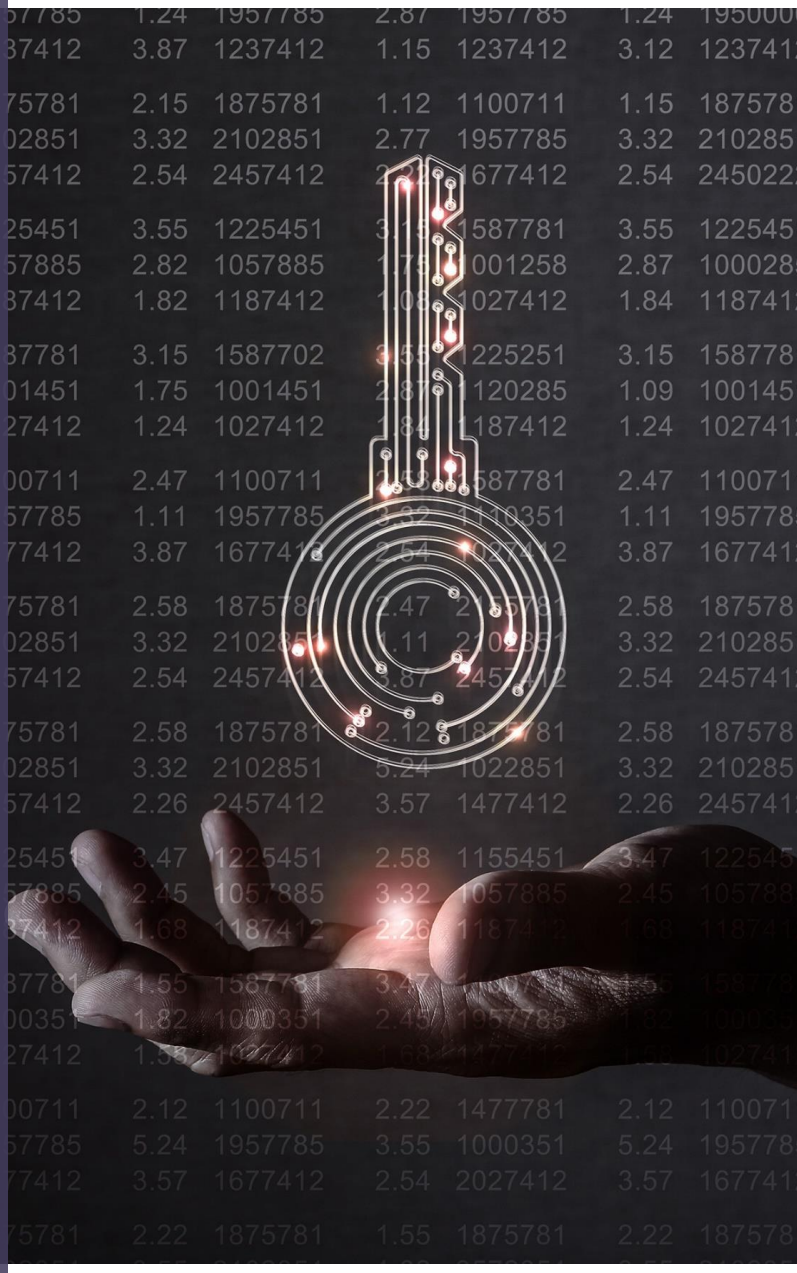
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR NEWSLETTER

DECEMBER 2020

DECISION SUMMARIES OF THE MONTH AND NEWS

Board Decision Regarding the Failure of a Bank to Fulfill an Instruction Given by a Board Decision

Decision Number: 2020/765 **Date of Decision**: 08.10.2020
Abstract: Board decision regarding the failure of a bank to fulfill an instruction given by a Board decision

According to the decision;

The Board instructed the data controller bank;

- Due to the fact that the bank failed to respond to the application made by the data subject to exercise their rights within the scope of the Law on the Protection of Personal Data within the legal period of 30 days;

- That the information text published on the Bank's website is not in compliance with the communiqué published by the Authority; since the reasons for the processing of personal data are not specified in the text and general expressions are used for the purposes of processing personal data, upon the complaint of the data subject, the text on the website of the data controller titled as "Your Personal Data is Under Protection!" to be brought into compliance with the provisions of the Communiqué on Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform.

After the instruction is communicated to the data controller bank,

- The following statement has been added to the information text: *"Within the framework of the relationship you will establish for the products and services you will purchase from our bank; your personal data are processed based on the following legal reasons"* along with the provisions in Articles 5 and 6 of the Law No. 6698;

- The processed personal data are not categorically included, only the provisions of the law are listed as stated above;

- Even though some additions have been made to the purposes of data processing, in general, the relevant amendments have not been made to bring the text into compliance with the Communiqué as stated in the instruction;

- Even though the bank states that specific and separate information texts are available for the data subject natural persons in other activities such as social responsibility projects and corporate branding and advertising activities, the bank is unable to submit any document to prove this to the Authority;
- In addition, it has been evaluated by the Board that in the credit card application or consumer loan application, an overall information text titled "Protection of Personal Data" is submitted to the data subjects and in this context, the provision of *"the requirement to fulfill the obligation to inform during the acquisition of personal data and on an activity basis"* included in the instruction of the Board is not complied with;
- Due to the fact that the information text published by the data controller is not regulated in accordance with the provisions of the Communiqué on Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform and the instruction given by the Board Decision is not fulfilled, it was decided to impose an administrative fine of TRY 120,000 on the bank.

Board Decision Regarding the Failure of a Bank to Fulfill an Instruction Given by a Board Decision

Decision Number: 2020/766 **Date of Decision**: 08.10.2020
Abstract: Board decision regarding the failure of a bank to fulfill an instruction given by a Board decision

The Board instructed the data controller bank;

- Due to the fact that the bank failed to respond to the application made by the data subject to exercise their rights within the scope of the Law on the Protection of Personal Data within the legal period of 30 days;
- For the reasons that instead of the bank's information text on the internet, a link is given to the 20-page Personal Data Processing and Protection Policy by the data controller, and a detailed examination is required to find the relevant parts in the document because the purposes of transferring the listed personal data are not specified, the Board has instructed the data controller bank that the privacy policy text will not substitute for information, the necessary arrangements for the information during the acquisition of personal data and on an activity basis shall be made, the text should be brought in compliance with the Communiqué on Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform.

After the instruction is communicated to the data controller bank,

- It has been stated to the Board that unlike the privacy policy on the website, that necessary conditions are met by listing the data on a categorical basis in the information text transmitted, providing clear and comprehensible statements about in which environments and in what way the data was obtained, why it was processed, transferred, on which legal grounds it was transferred to which institutions and persons, and how long the data were processed and stored,

- However, there is no information in accordance with the Communiqué which personal data processing condition is based on the personal data processed in this information text,

- Under the title "For Which Legal Reason Do We Process Your Personal Data?", the conditions in the 5th article of the Personal Data Protection Law are listed,

- It has been determined that for sensitive personal data, the information is given that it is processed only based on consent.

In this context, it has been emphasized by the Board that it is contrary to the requirement *"... to provide detailed information on the personal data processing conditions on which personal data processed by the data controller..."* included in the instruction communicated to the data controller.

- In addition, it has been evaluated by the Board that in the response of the data controller bank, the Board's instruction does not include the statement of *"fulfilling the information during the acquisition of personal data and on an activity basis ..."* and that the bank does not submit any supporting documents; it has been determined that the information texts submitted during the credit card application and housing loan application are not specific to these applications and are an overall information text.

- It was decided to impose an administrative fine of TRY 120,000 on the bank due to the fact that the information text prepared by the data controller after the instruction was not prepared in accordance with the provisions of the Communiqué on Principles and Procedures to Be Followed in Fulfillment of the Obligation to Inform and the instructions given by the Board Decision were not fulfilled.

Public Announcement on "Publicization"

In the announcement made by the Personal Data Protection Authority on 16.12.2020, it was stated that one of the processing conditions in Article 5 of the Law on the Protection of Personal Data is *"to be made available to the public by the data subject himself"*; it has been stated that the concept of publicization means the personal data of the data subject is disclosed to the public by themselves. However, the announcement emphasized that this statement should be interpreted narrowly.

According to the announcement, for any data to be accepted as public it should be determined that the data subject has a will to make the data public and for what purpose the data subject has made his personal data public.

In cases where personal data are disclosed to the public for a reason other than the will of the data subject person, it will not be possible to speak of a publicization under the Law.

In addition, the fact that the data is made public by the data subject will not enable the data controllers to process this data except for the purpose of making it public.

For this reason, it is important to observe the above principles and the general principles of the Law in personal data processing activities carried out based on the sub-clause d (publicization) of paragraph 2 of Article 5 of the Law.

The Turkish Personal Data Protection Board has published its decision dated 07.11.2019 and numbered 2019/331 regarding the subject. You can access the decision here. (The link is in Turkish.)

Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş. - Data Breach Notification

With the data breach notification made by Otokur Otomotiv İnşaat Turizm Sanayi ve Ticaret A.Ş., it was reported to the Authority that,

- The after-sales services manager working within the data controller received data in reports by abusing his authorization, this situation was realized upon the complaint of a customer and the breach was detected as a result of checking the logs,
- The aforementioned breach occurred on 16.12.2020, ended on 19.12.2020 and was determined on 18.12.2020,
- The number of people affected by the breach is 17,092, and the personal data affected by the breach are identity, contact, customer transaction data and notes on the customer card.

The aforementioned data breach was published on the website of the Authority on 22.12.2020.

Ficosa Otomotiv San. ve Tic. A.Ş - Data Breach Notification

With the data breach notification made by Ficosa Otomotiv San. Ve Tic A.Ş., it was reported to the Authority that,

- A ransom attack was performed on the servers of the data controller on 16.12.2020 and the files were encrypted, the breach was detected by noticing that there was a problem with the logs,

- Personal data affected by the breach are name, surname, e-mail and/or phone number, but the investigation on IT side is ongoing,
- Employees, customers, suppliers and service providers were affected by the breach,
- The estimated number of people affected by the breach is 976, but the exact number of people and records are not identified due to the ongoing investigation.

The aforementioned data breach was published on the website of the Authority with the decision of the Turkish Personal Data Protection Board dated 22.12.2020 and numbered 2020/987 and the investigation on the subject still continues.

UiPath SRL - Data Breach Notification

With the data breach notification made by UiPath SRL, it was stated that,

- The data controller kept a file containing the registration information of the users participating in the UiPath Academy ("*Academy*") for the administration of the Academy which enables the users to learn the UiPath software; the data controller's employee uploaded the file in question to a vendor's software platform to keep track of users, and an unauthorized user accessed the file due to an accidental misconfiguration of the file permission settings,
- The data breach was detected on 01.12.2020 when a third party notified the data controller that the affected file was available on a public website,
- The breach may have affected the name and surname, username, e-mail address, the name of company of the user's employer, the country of the user, the country of the user, the UiPath Academy certification level given by the data controller and the UID code information that is no longer used by the company,
- The group of people affected by the breach are users, and 4,692 of them who referred to Turkey as their own country were affected by the breach.

The aforementioned breach was announced on the website of the Authority with the decision of the Turkish Personal Data Protection Board dated 22.12.2020 and numbered 2020/984 and it was stated that the investigation on the subject still continues.

Ficosa International Otomotiv San. ve Tic. A.Ş - Data Breach Notification

In the data breach notification made by Ficosa International Otomotiv San. ve Tic. A.Ş, it has been stated that,

- Ransomware attacked the controller's server in 16.12.2020 and encrypted the files,
- The breach was identified upon noticing there was a problem in the logs,
- The breached personal data consist of names, last names, e-mails, and/or phone numbers, yet the IT investigation is ongoing,
- The breach affected approximately 1084 people including employees, customers, vendors, and service providers, yet the exact number of affected people and logs are not identified as the investigation is still ongoing.
- The aforementioned data breach was published on the website of the Authority on 29.12.2020, and the investigation on the subject continues.

Additionally, the notified data breach took place in Turkey and affected Ficosa International Otomotiv San. ve Tic. A.Ş as the company servers are abroad.

The Personal Data Protection Office in Poland (UODO) Imposed a Penalty of Reprimand for Revealing the List of Quarantined People

The Personal Data Protection Office in Poland launched an ex officio investigation regarding a waste management company revealing personal data of the quarantined people to unauthorized recipients, including their address, and imposed a penalty of reprimand to the company in question.

UODO has undertaken a detailed investigation to clarify the situation. It requested information from the company about whether risk analyses of privacy were conducted when the personal data of the people quarantined due to the COVID-19 threat were processed and the regarding procedures were established.

In its explanation, the company stated that it conducted an analysis for possible loss or unauthorized disclosure in data processing activities, adding that the lists in question contain only the administrative addresses and not the names, last names, or other identifiable information of the persons.

Upon their investigation, UODO concluded that the name of the location and street, the building number, and the data revealing the persons quarantined constitute personal data under GDPR. Additionally, according to UODO, the data revealing the persons are quarantined are subject to sensitive personal data.

At the same time, UODO decided that there was a breach of data privacy due to the employee who is responsible for examining the list leaving it open on their desk and causing another employee to take a picture of the list in question.

UODO emphasized the measure that employees signing the statements and files regarding the provisions in the risk analysis is an inadequate measure on its own. Additionally, the company that conducted risk analysis should take into account both the sensitive personal data processed and human factors as the controllers are human (lack of attention, neglect, carelessness, etc.). UODO stated one-time and cursory analysis is inadequate.

It was confirmed that the company did not notify the breach to authorities within 72 hours as well as to the people in question even though the breach poses major risks as the data processing interacts with sensitive personal data.

In the light of these findings, stating that the GDPR provisions were violated, UODO imposed a penalty of reprimand to the company and instructed it to notify the data subjects about the data breach.

The Swedish Authority for Privacy Protection Issued a Penalty Fine Due to Illegal Video Surveillance

The Swedish Authority for Privacy Protection issued a penalty fine of SEK 200,000 to Gnösjö Municipality for their unlawful video surveillance in LSS housing.

The agency received a complaint from a relative of a person who resides in a disabled nursing home (LSS Housing) about illegal surveillance conducted on the resident.

The agency initiated an audit regarding the activities operated in LSS Housing and concluded that the resident in question was indeed being monitored in their own bedroom against GDPR and Swedish Video Surveillance Act.

The Social Welfare Committee responsible for accommodation in LSS Housing in Gnosjö stated that the data subject is suffering from a disease that causes extreme difficulties for both themselves and personnel, and the video surveillance was carried out to prevent any possible harm.

The agency concluded in their evaluation the Social Welfare Committee could achieve their purpose by using means that are less violating LSS residents' privacy.

The agency reached a conclusion in their decision that there is no legal basis for video surveillance, the data controller did not conduct an impact assessment, and the data subjects were not informed about the surveillance. The agency issued a penalty fine of SEK 200,000 to the Social Welfare Committee for the mentioned reasons.

The Belgian Data Protection Authority Fines for Unlawful Processing of Video Images

The Belgian Data Protection Authority fined EUR 1,500 against those who illegally process personal data through a video surveillance system. Also, they decided that the location of the cameras of this video surveillance system constituted a data security breach.

Two complainants had filed a complaint to the Authority regarding the video surveillance system of their two neighbors and the images stored by the system. The complainants demanded uninstallation of the video surveillance system.

The two defendants had set up a video surveillance system by five security cameras recording 24/7 on their private property. The way the cameras were mentioned in the complaint that they were positioned in such a way that the complainants were absolutely recorded while they were entering their homes, driving cars, or performing any action around their private property. The footage was used by the defendants in an environmental planning dispute between defendants and complainants.

The Authority determined that the images were not processed lawfully under GDPR and were not within the scope of legitimate interests. Although the aim was to protect private property, it was concluded that viewing public areas was beyond the legitimate interest and damaged the rights and freedoms of the data subjects.

Besides, since the data are obtained unlawfully, the Authority concluded that data processing was also contrary to the use of images to resolve the dispute that arose later.

The Authority imposed a fine of EUR 1,500 and reprimand to the defendants for the reasons listed above.

The Swedish Authority for Privacy Protection Announced the Deficiencies in Healthcare Providers Accessing the Patient Data

The Swedish Authority for Privacy Protection inspected eight healthcare providers regarding the governing and restriction of personnel's access to electronic health records.

The agency firstly investigated whether the authorization of personal data access in the electronic health records was provided to authorized persons upon necessities and risk analysis conducted.

The healthcare providers should have conducted a detailed analysis and evaluation of the risks and necessities regarding the personnel's access to the information in the health records. Yet, the agency stated that seven of the healthcare providers did not conduct any risk evaluation and only one of them carried out one analysis which has deficiencies.

The agency reached a conclusion that seven of the healthcare providers did not limit their access authorization to the patient information to an extent strictly necessary, which was a sign of insufficient measures taken by the providers for the privacy of the personal data in the electronic records system.

Additionally, the agency set up a guideline summarizing the results of their current inspection regarding the obligation of conducting a risk and necessities analysis.

In their guideline, the agency pointed out the importance of healthcare providers conducting a risk and necessities analysis. The agency stated that the purpose of the guideline is to help healthcare providers with the necessary analysis before giving them access authorization to health records. Within this context, the agency explained their purpose is assuring the authorization of the healthcare providers is correctly done and guaranteeing the privacy right of the patients.

Estonian Data Protection Inspectorate Decides to Immediately Terminate 3rd Party Access to Prescription Information in E-pharmacies

Estonian Data Protection Inspectorate imposed a fine of EUR 100,000 on three pharmacy chains for displaying another person's prescription in an e-pharmacy environment without the person's consent.

The Inspectorate stated that "We considered it necessary to urgently suspend the display of valid prescriptions to third parties in e-pharmacy environments on the basis of personal identification codes, as there is no legal basis for such display."

The inspectorate emphasized that it may be possible to buy a medicine for another person under normal circumstances, but in such cases, the pharmacist must ensure whether or not the consent of the prescription holder is present.

When the inspectorate examined the e-pharmacy portal, they noticed that the accessing users could quickly access the prescription information of other people using the chat window. During the login stage, it was determined that the users choose whether they wish to see their own prescription information, or someone else's prescription information and that the information is accessible when they have entered another person's identification number. They decided that this activity does not comply with GDPR.

Estonian Data Protection Inspectorate issued a warning covering the Apotheka, Südameapteek and Azeta.ee e-pharmacies.

The Irish Data Protection Authority Announces Decision on Twitter Investigation

The Irish Data Protection Authority ("DPC") announced the result of its investigation against Twitter International Company.

DPC stated that Twitter acted in violation of Article 33 (1) and Article 33 (5) of GDPR as the violation was not reported and documented in due time. DPC imposed an administrative fine of EUR 450,000 to Twitter, which they declared as effective, proportionate and deterrent.

The draft decision within the framework of the investigation was submitted to other Relevant Supervisory Authorities in May 2020 in accordance with Article 60 of GDPR. It was the first "big technology" case in which Article 65 ("Dispute Resolution") has been implemented since GDPR came into force and was conducted in cooperation with all EU Supervisory Authorities.

The European Data Protection Board has published its 65th decision on its official website.

The Swedish Authority for Privacy Protection Imposed a Penalty Fine of SEK 300,000 on a Housing Company

The Swedish Authority for Privacy Protection imposed financial a penalty fine of SEK 300,000 on a housing company named “Uppsalahem” due to their illegal video surveillance in an apartment.

The agency received a complaint about video surveillance done in an apartment belonging to Uppsalahem. The complainant claimed that there was a security camera facing their apartment’s front door.

The agency confirmed the company had indeed set up a surveillance camera monitoring the floor the complainant lived in. The monitored zone clearly covered two apartment doors, one belonging to the complainant and the other to another resident who claimed that they had experienced disturbance and harassment.

The housing company stated that the purpose of the video surveillance was to prevent any problems that might arise in the stairwell over time.

The agency stated in their decision that the relevant video surveillance violates privacy by monitoring people in their apartments and issued a penalty fine of SEK 300,000 against the housing company, who announced that they ceased the video surveillance in question upon the decision.

INFORMATION GUIDE

How Should the Organizations Evaluate Mobile Devices within the Scope of Personal Data Protection?

As it is known, it is among the obligations of the data controller organization to ensure the protection of the data on the organization's devices by taking the necessary administrative and technical measures within the scope of the protection of personal data and information security. Even though this topic is elaborated by the Authority under the title of "Ensuring the Security of Media Containing Personal Data" by including among the technical measures within the scope of KVKK, it should be examined from a technical aspect as well as from an administrative perspective.

First, it should be explained that ensuring the security of environments containing personal data does not mean that companies only protect their company computers or servers. In this context, mobile devices are an essential element that is often overlooked and causes many breaches in practice.

Matters that may cause breaches are separated into technical and administrative aspects and examined as follows:

Breaches Arising from the Lack of Administrative Measures:

Employee's Use of Personal Mobile Device for Business Purposes

One of the inconveniences mostly encountered is that the employees use their personal mobile devices for business purposes since the organization does not provide a mobile device to the employee. The use of a personal mobile device will endanger the employee to continue accessing this data in case the business relationship between the employee and the data controller organization is terminated. Although the employee's access to e-mails or company documents can be prevented by mobile device management systems and by closing company accounts, the contact information of the employee's customer, supplier, or company-related persons will not be prevented from remaining on this mobile device or from reaching the employee after the termination of the business relationship.

In such a case, taking a commitment from the employees that the data belonging to the organization will not be kept in personal devices used for business purposes and the related data will not be used for different purposes if they leave their jobs or change their duties, it will be one of the administrative measures that will minimize the risk.

For the aforementioned reasons, it would be appropriate to provide the employee with a separate mobile device and phone line to carry out the business processes, or to inform the employee about the use of the company's fixed lines to communicate with the data subjects with a strict policy.

Employee's Use of Corporate Mobile Device for Personal Purposes

The employee's use of the company mobile device for personal purposes, uploading their personal data to the company device will result in them being responsible for the data that should not be kept by the organization, and keeping the data incompatible with the purpose. For example, if the employee personally adds the contact information of third parties to the directory of the device and obtains visual and audio recordings with this device, it will be incompatible with this purpose.

In addition, as in other devices, the employee's installation of applications with detected vulnerabilities such as WhatsApp, Zoom, which are not under the control of the organization, on the device will also be a cause of a breach.

For this reason, to ensure that the employee does not use the company device or the company phone line for their personal work, it will be a good practice to prepare a strict policy that regulates all the above issues and to inform the employees about this and to ensure that the employees are aware of the device use. In addition, in this context, the use of secure mobile device management systems by providing information to the employee will be a proportionate data processing activity and will prevent breaches that may occur over mobile devices.

Ensuring Mobile Device Security

The management of the devices is as important as their installation. It is necessary to know and manage the information such as which features are open in the devices used or whether the devices are open to access from outside. The following technical issues should be noted for Secure Mobile Device Management.

1. Asset management should be implemented, the type and operating system version information of the devices should be followed.

2. Up-to-date anti-virus applications should be used on mobile devices and disabling this application should be prevented.

3. Employees should be prevented from installing and using applications that are not approved by the organization on mobile devices, and remote version update and patch security measures should be taken for applications.

4. In case of any attack or data breach, device backup policies should be determined, and backups should be secured to detect the data in the device and to prevent data loss.

5. In case mobile devices are delivered to unauthorized persons for maintenance, repair, and similar operations, the data should be inaccessible, and it should be ensured that no malicious software is installed on the device during maintenance.

The use of Mobile Device Management (MDM) Solutions provides great benefits to organizations in ensuring data security, as well as providing additional protection methods to the above-mentioned measures.

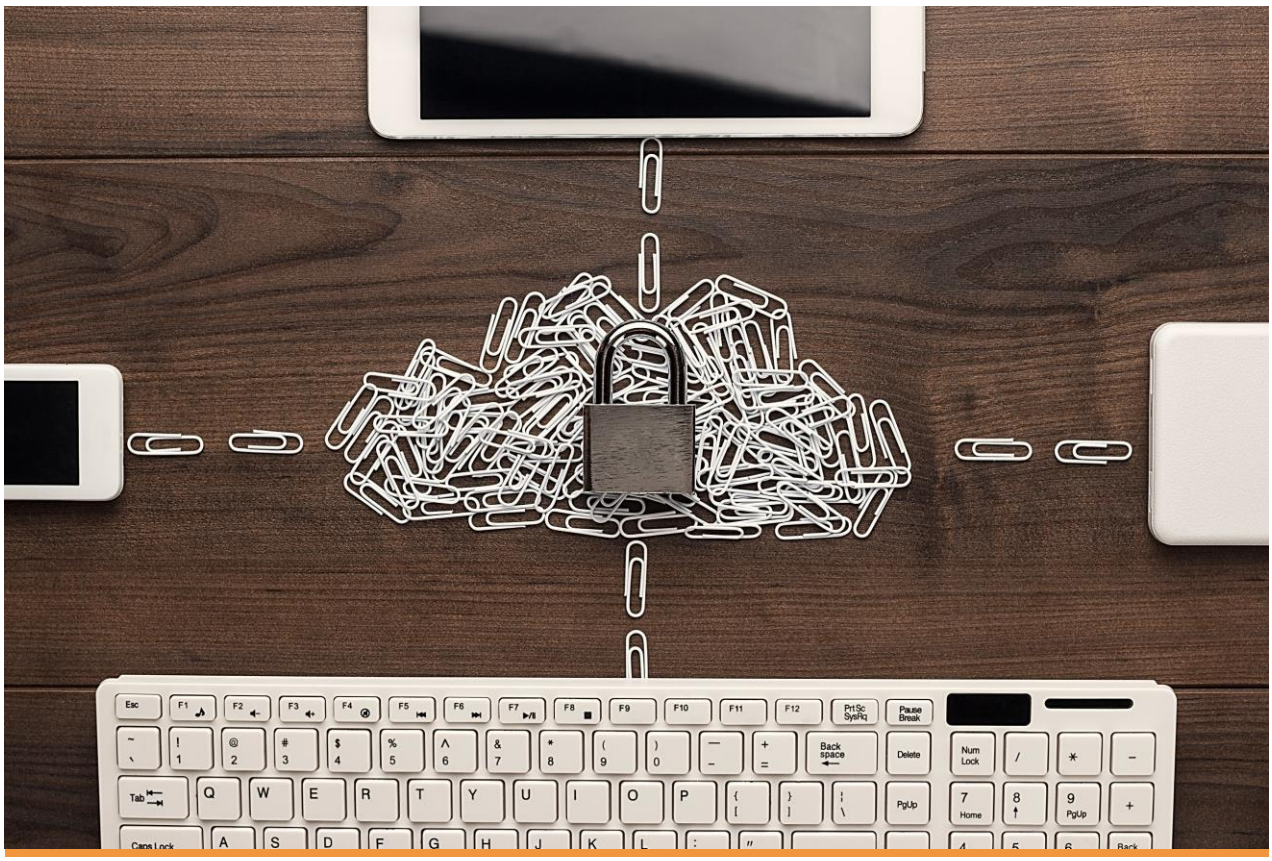
With MDM Solutions, the organization's data, correspondence, e-mails, sensitive documents can be protected, and their transmission can be limited. It is possible with Mobile Device Management Systems to provide password management in devices, prevent data copying, and taking screenshots.

In addition, in case mobile devices are lost or stolen; by locking the devices remotely, the data inside can be secured and even if the SIM cards are inserted into another device, their access can be blocked.

All the threats of breach described above regarding mobile devices, administrative and technical measures to be taken are valid for computers, tablets, and similar smart communication devices controlled by the organization. The point to be considered here is to think in a broader perspective about ensuring the security of environments containing personal data and to make a correct risk analysis.

Kübra Özkahraman | Quality Assurance & Training Responsible

Şeyma Kaplan | Legal Consultant | Attorney



Prepared By

Ece Melis Erkoçak

Hazal Özçelik

Kerem Akdağ

Kübra Özkahraman

Livanur Sever

Onur İzli

Rabia Dağcı

Şeyma Kaplan

Şule Özcan

Follow Us on Social Media...