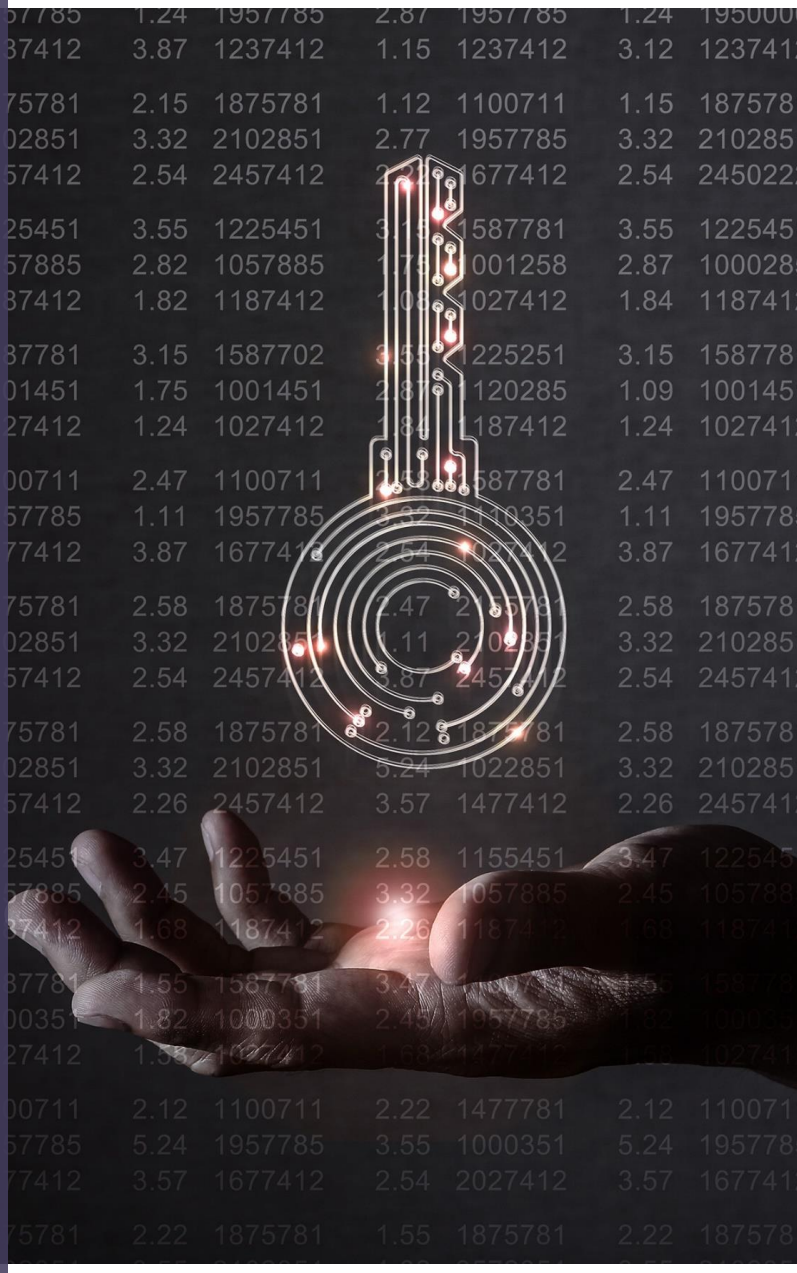
CottGroup®
Holistic Business Services

VeriSistem
a CottGroup® company



KVKK & GDPR
NEWSLETTER

OCTOBER 2020

NEWS

Public Announcement on the Transfer of Data Abroad

In the public announcement published on 26.10.2020, the Turkish DPA provided general information regarding the transfer of personal data abroad. In the announcement, it is stated that the personal data processed before the publication date of the Law ("KVKK") will be brought into compliance with the provisions of the Law within 2 years from the date of publication; regarding the transfer of personal data abroad; by evaluating international conventions of which Turkey is a party, transferring of personal data between Turkey and the countries with reciprocity condition, the relevant legislation and practice of the country where the personal data will be transferred, the countries with adequate protection will be specified and announced by the Board in accordance with paragraph 3 of Article 9 of the Law. The Turkish Personal Data Protection Board is currently working on announcing adequate countries.

In addition to the determination of adequate countries, the details of data transfer to inadequate countries are included collectively in the announcement of the Authority. Accordingly, it was stated that these two principles should be followed in data transfer to inadequate countries by summarizing the undertakings and Binding Corporate Rules ("BCR"). You can access further information on the Commitments and Binding Corporate Rules through our article via the link and the Information Guide section of KVKK&GDPR April Newsletter.

In addition, the Authority explained the role of regulations in other laws; in this context, it has been emphasized that other provisions of the law are reserved in data transfer abroad and if they are included in our domestic law in accordance with Article 90 of the Constitution, international agreements have the force of law, that is, data transfer is considered among the reserved cases in accordance with international agreements.

In summary, the Authority declared that although it carries out instructive and guiding studies on the implementation of the Law, it imposes administrative sanctions as a law enforcer when necessary and carries out its studies and examinations in line with the regulations allowed by the Law and announced that the process to allow is being carried out in accordance with the mandatory provision of the Law regarding transfer abroad.

Decision of the Constitutional Court on Corporate E-mail Address Dated 14.10.2020

The applicant had a corporate e-mail account during his work as a lawyer for a law firm. Problems started to occur in the team where the applicant worked, and a few of the team members submitted a petition to the top management and stated that the team manager did not approach the applicant objectively and favored him. As a result of the case, an interview took place between the applicant and the management. The management made an examination on the applicant's corporate e-mail address and terminated his employment as a result of this examination. The applicant claimed that due to the examination of the content of his corporate e-mail account and as a result of this his employment contract is terminated based on the correspondences through his e-mail, he claimed that his right to demand protection of personal data and freedom of communication were violated.

The court stated that the authority of the employer to supervise the communication of the employee should be examined within the scope of the positive obligations of the state in the context of the right to demand protection of personal data and freedom of communication. Accordingly, the concrete case has been evaluated within the framework of the general principles determined for the employer to audit and monitor the corporate e-mail account. In cases where there is no full and clear notification in advance that the communication made through the e-mail account can be controlled, it is a situation that can be foreseen by the employer that the employee can make personal correspondence via corporate e-mail.

Reasonably, employees expect that their rights and freedoms will not be intervened in the absence of clear information. It has been understood that the courts of instance resolving the dispute arising from private law business relations, did not carry out a fair trial by observing constitutional guarantees and that positive obligations were not fulfilled. The Constitutional Court concluded that the right to demand protection of personal data and freedom of communication were violated for the reasons explained.

Vatan Bilgisayar Sanayi ve Ticaret A.Ş. - Data Breach Notification

According to the data breach notification made by Vatan Bilgisayar, it is stated that the breach occurred at 01.30 on 05.10.2020 and detected at 17.04 on 05.10.2020 with a warning e-mail from a security company, the breach occurred as a result of testing whether the username (e-mail) and passwords that are considered to have been acquired from another source are valid on the website of the data controller, and that successful usernames and passwords have been

published on a website, login attempts were programmatically tested with the API under a web service used in the mobile interface of Vatan Bilgisayar, the personal data affected by the breach are www.vatanbilgisayar.com member usernames (e-mail addresses) and these users have passwords on www.vatanbilgisayar.com, 27,143 members of vatanbilgisayar.com were affected by the breach, data subjects can receive information about the data breach from the e-mail address kisiselverim@vatanbilgisayar.com.

The relevant data breach has been announced on the web page of the Turkish DPA on 09.10.2020 and the investigation on the subject is continuing.

Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co. - Data Breach Notification

With the data breach notification reported to the Turkish DPA by Hanon Automotive Climate Sys. Manufacturing Industrial and Commercial Co. it is stated that the breach occurred as a result of a ransomware attack that encrypts the files on most of the organization's global servers on 04.10.2020, the personal data affected by the breach, the number of persons and records, data subject groups and the possibility of the breach to have negative consequences for the data subjects are not yet known, the evaluation studies regarding the effect of violation are continuing.

The relevant data breach has been announced on the web page of the Turkish DPA on 27.10.2020 and the investigation on the subject is continuing.

Hamburg Data Protection and Freedom of Information Commissioner Imposed a fine of 35.3 Million EUR on H&M for Data Breach

Hamburg Data Protection and Freedom of Information Commissioner imposed a fine on H&M Hennes & Mauritz Online Shop A.B. & Co KG in the amount of 35.3 million EUR for its data breach as the Company spied on hundreds of its employees.

It was noted that the breaching Company was registered in Hamburg with a service center in Nuremberg; that this service center has been keeping detailed records about the private lives of employees since 2014; that records have been permanently stored; that based on these records, audit teams were holding so-called “Welcome Back” talks following a day on which an employee was absent (for instance following a holiday or a compassionate leave); that during these talks, data concerning the diseases and symptoms of an employee were also collected and saved in records in addition to details about the leave (or a holiday).

In addition, certain auditors have collected very comprehensive details about the private lives of employees, including their family issues and religious beliefs; that some of these data were

recorded; that they were accessible to 50 other executives; that sometimes these records could be extremely detailed and they were kept for periods longer than required; that in addition to performance assessment, these data were also used for measures and decisions regarding employment by creating a profile of the employee; and these activities involve a high degree of interference with the employee's rights, and these activities involve a high degree of interference with the employee's rights.

This data breach was revealed when such data were exposed following a configuration error in October 2019. When competent authorities first heard about the collection, they first ordered that the contents be seized and delivered to them and afterwards witnesses were heard so that this practice was confirmed.

It was further noted that responsible parties started to take corrective actions after the breach was discovered; that the Company management apologized and offered to pay compensation to their employees; that competent authorities presented a concept to the Company, showing how the data protection should be enforced; that this concept entails the appointment of a new data security officer, the monthly update of data protection statements, the reinforcement of the whistle-blowing mechanism and a consistent approach to the rights of data subjects.

The competent authority noted that H&M seriously ignored the protection of the employee data in Nuremberg and that therefore, the fine imposed on them was effective and sufficient to deter them from future attempts. Notwithstanding the foregoing, it was emphasized that the Company's efforts to compensate the damages were evidently a positive move and that the provision of data in a completely transparent manner and provision of financial indemnity guarantee clearly indicated that the Company showed the necessary respect and appreciation well deserved by its employees.

The Belgian Data Protection Authority Has Issued a Warning and Reprimand Penalty to a Regional Public Environmental Institution

The Public Environment Institution ("Institution") has the power to fine citizens in matters such as pollution. The Institution imposed such fine on the first plaintiff. However, in the decision imposing the fine, the Institution also referred to the first plaintiff's wife and her husband's father. The Institution noticed that the first plaintiff's National Register contained the name of his spouse (the second plaintiff) and a connection with his spouse. The father of the spouse (third plaintiff) contacted the Institution to defend the first plaintiff in the environmental procedure initiated by the Institution. In its judgment based on the surnames of the second and third plaintiffs, the Institution concluded that there was a family link between the two.

In the first assessment of the Litigation Chamber of the Belgian DPA, it is found that that the Institution's reference to the name of the second plaintiff, the connection of the second plaintiff with the first plaintiff and the family relationship between the second and third plaintiff in its decision with the information obtained from the National Register is contrary to Article 6 of the GDPR and unlawful data processing has taken place. So much so that the provision 1 (e) of Article 6 of the GDPR covers data processing based on the public interest; however, there is no such

public interest for the processing of the data of the persons in question, because the penalty was given to the first plaintiff.

In addition, the family relationship between the second and third plaintiffs mentioned in the judgment is not an exact information but based on an assumption. Furthermore, this information is not an information to be necessarily stated in the concrete case. In this respect, the Authority has determined that the Institution has acted against the principles of the accuracy of data and data minimization included in Article 5 of the GDPR.

The Authority issued a warning and reprimand decision against the Institution for the reasons mentioned above.

The Norwegian Data Protection Authority Fines Bergen Municipality

Bergen Municipality has developed a portal called Vigilo to ensure security of children in communication between school and home. In October 2019, the Norwegian Data Protection Authority imposed an administrative fine on Bergen Municipality with the conviction that the personal data processed in the portal containing the communication module were not processed in the ways of sufficient security.

The administrative fine was imposed on the grounds that the municipality did not implement technical and organizational measures to achieve an adequate level of security, and also did not ensure confidentiality and integrity. In the decision, it was stated that especially children are the group with the most sensitive position for data protection and the highest level of privacy concern, but the Municipality did not apply the necessary security measures at the highest level regarding the use of this application by the children. It was stated that personal data that should be confidential, such as address information, are made available to the parents of all children through the portal, and information that should have remained confidential in the context of parent-child relationship was not protected by taking sufficient measures.

The Lithuanian DPA Imposes Fine for Unlawfully Processed Personal Data of the Parents of an Adopted Child

The Personal Data Protection Supervisory Authority of the Republic of Lithuania imposed penalty on the Vilnius City Municipality Administration for GDPR violations.

15,000 EUR has been imposed for the improperly processed personal data of the parents of an adopted child. The fine was imposed due to the violation of Articles 5 (1) (d) and 5 (1) (f) of the

as a result of the failure to take appropriate technical and organizational measures and ensure the accuracy of the personal data processed.

While conducting an investigation, the Authority noticed that the data of the relevant child was updated incorrectly when filling out the education application of the adopted child in the Centralized Application Submission and Population Information System (hereinafter referred to as "IS") of the Municipal Administration, although the IS should update the data monthly. So much so that, when the data in IS was automatically updated, the information of the adoptive parents were incorrectly updated and replaced with the contact data (e-mail address) of one of the biological parents of the child in the Population Register of the Republic of Lithuania.

When processing personal data, the Municipality Administration must comply with the principle of accuracy, which ensures that the data is correct and kept up to date when necessary, and take reasonable steps to ensure that personal data that is inaccurate regarding the purposes for which they are processed are deleted or corrected without delay. Appropriate technical or organizational measures should be taken to realize integrity and confidentiality principles and personal data should be protected against unauthorized or illegal processing, loss and damage.

The Norwegian DPA Fines Odin Flissenter for Performing a Credit Check of a Sole Proprietorship Without Having a Legal Basis for the Processing

The Norwegian DPA fined Odin Flissenter EUR 13,905 for performing a credit check of a sole proprietorship without a legal basis.

An unidentified citizen filed a complaint that Odin Flissenter performed a credit check of a sole proprietorship that did not have a customer relationship or any other connection to the company. Considering the effects of Covid-19, the amount of penalty fine has been slightly reduced.

Credit information of a sole proprietorship is considered as personal data, because the owner is directly affiliated with the company, and the financial situation of the company is directly related to the financial position of the company owner. On the other hand, credit check ratings are built on a compilation of personal data from several different sources and show a score that indicates the likelihood of a person or sole proprietorship performing payment on their own. The credit rating also includes details about the economy of the business organization such as payment descriptions, guarantees (for costs), debts, equity ratio.

The Authority emphasized that; although the data collected by Odin Flissenter is directly related to the financial status of the company owner, such persons may have high privacy concerns regarding the privacy of the data, and that the data was processed outside of the company's operating purposes in the said case. For all these reasons, the Authority imposed an administrative fine of 13,905 EUR on Odin Flissenter.

INFORMATION GUIDE

Administrative Measures - Ensuring Physical Environment Security

In accordance with the Law on the Protection of Personal Data No.6698 ("KVKK"), natural and legal persons engaged in data processing activities are obliged to take administrative and technical measures regarding data processing activities. One of these administrative measures is to ensure the security of environments containing personal data. In addition to the technical measures to be taken to ensure the security of the digital environments where personal data are kept, it is essential to provide the security of physical environment in order to protect the data stored in devices or on paper. Certain monitoring methods can be used to ensure the security of physical environment, and various data recording systems can be set up. While taking this protection measure, the party engaged in data processing activity should not neglect other administrative and technical measures. Although not limited in number, some examples that can be taken to ensure physical environment security are listed as follows:

1. Security Cameras

Controlling the entry and exit of environments containing personal data and monitoring these environments with 24-hour security cameras is one of the methods to ensure physical environment security. This monitoring can be performed at the entrance of the organization or in the form of monitoring in areas where data requiring double protection are available.

In case of monitoring with a security camera, attention should be paid to the aspects such as placing warning (information) visuals in areas with security cameras, having detailed information and disclosure texts ready and informing people by means of these texts, not using the recorded images for purposes other than ensuring the security of physical environment and destruction of images within a reasonable time.

2. Registering Visitors

One of the methods of controlling the entry and exit of environments containing personal data is to keep records of persons other than employees at the workplace. Persons visiting the workplace can be registered with a data recording system created digitally or physically. Thus, in the event of a data breach regarding the data stored in physical environment (for example, in case of theft of a device), it can be easily found who is at the workplace on the relevant dates. While taking this measure, the most important thing that people who are engaged in data processing activities should pay attention to is to ensure that this data is processed proportionate. For example, in case of visitor card application, the identity card of visitors should not be held hostage; for the purpose of verifying the declared name, it must be returned to the data subject after identity check. In addition, visitor register books or other recording environments should be destructed after a reasonable period of time has passed.

3. Providing Additional Security Measures Inside or Outside the Organization

Additional security measures can be taken while protecting sensitive personal data or strictly confidential data within the organization. For example, if sensitive personal data is stored in a paper environment, it should be stored in lockers and access to these lockers should only be with certain people. In addition, methods such as defining passwords for persons who have access to entry and exit of environments such as server room, human resources department, R&D department that are important for the organization or containing sensitive personal data, setting up a card reader system or installing fingerprint reader systems can be followed. The measure to be taken here should be compared with the nature of the data to be protected and the principle of proportionality should be respected. In addition, if the method of data protection is to process sensitive personal data, that is, to process the biometric data of the data subjects, it is necessary to obtain the explicit consent of the persons and to operate the policies and procedures accordingly.

4. Providing Environments Resistant to Disasters Such as Fire/Flood

Protection of the physical environments containing personal data against external risks (fire, flood, etc.) with appropriate methods is also one of the measures to be taken. That is, it is recommended to use fire or crash resistant cabinets for data stored in paper environment. In addition, the fact that the system room is fire resistant in every aspect is one of the important information security elements.

In addition, depending on the measure of backing up personal data, which is one of the technical measures, keeping the backups in a different location than the workplace or even in a different city will be one of the top level measures to be taken in order to protect them against natural disasters. Physical environment security should also be provided for the areas in the locations where the backups are kept. To sum up, the measures to be taken to ensure the protection of data against natural disasters are not limited and taking measures at the highest level is important according to the nature of the data.

5. Other Aspects to Consider When Working Remotely During Pandemic

There will be various measures to be taken during the pandemic when many organizations have adopted the practice of working remotely; because, in this period, the most difficult situation to protect personal data is that it has become indispensable to take the data out of the organization. Taking corporate devices out of the workplace, employees' need to use their personal devices, or sending physical documents to the home addresses of employees/those entitled for many reasons create these risks.

Shortly, the points to be considered by employees in such situations are keeping corporate devices and paper data in protected areas against dangers such as theft and accidents, prevent other people living in the house from using corporate devices or, if personal devices are used, log out of all corporate accounts when someone else needs to use the device, a good track of the cargo coming to the employee's home on behalf of the organization and preventing loss of information on this issue. These measures are not limited in number, and it is basically important that people provide the highest level of protection measures when working remotely, as well as at workplace.

On the other hand, technical measures also need to be taken while working remotely, and all administrative and technical measures should be considered in a holistic manner. You can check out our article titled Technical Aspects to be Considered During Working Remotely through our

KVKK&GDPR March Newsletter to have further information on the subject.

Şeyma Kaplan | Legal Consultant | Attorney

Technical Measures - Transferring Sensitive Personal Data Transferred to Removable Memory, CD, DVD with Encryption

According to the Article 12/1 of KVKK, data controllers have to take all necessary technical and administrative measures in order to prevent unlawful processing of personal data, to prevent unlawful access to personal data and to ensure that personal data are stored in accordance with the law.

These measures are elaborated in the Personal Data Security Guide published by the Authority and specified at the notification stage to VERBIS.

One of these measures is to transfer of sensitive personal data transferred to portable memory, CD, DVD media with encryption.

Organizations are most likely to use removable memories and store their backups on DVDs in terms of tracking their daily operations and ease of access. In addition to being protected against attacks that may come from outside, organizations should also be prepared against any data breach that may occur internally.The most important step in preventing data breaches that may occur internally is to prevent the data of the organization from leaking out.

In this context, although organizations do not care much to act based on contracts, confidentiality commitments, policies and procedures with individuals, taking the measures at the highest level required according to the nature of the data will protect the organizations from possible violations and breaches.

The first action to be taken to protect the information assets of the organization is to restrict the USB ports of user computers. The relevant restriction is one of the basic measures to prevent the acquisition or dissemination of data by malicious people.

In addition, organizations must encrypt the data they transfer to portable memory, CD, DVD and similar devices that they use for business processes and ensure the security of the relevant devices.

It is an absolute necessity to encrypt sensitive personal data when stored or transferred via related devices.

Although not limited, the encryption and transfer of data transferred to portable memory, CD, DVD media, which are included in the list of measures to be taken and counted by the Turkish DPA, will be the proof that organizations take the necessary steps to eliminate the risk in case of any data breach.

As a result, ensuring the security of the environments where personal data is located is of particular importance for each environment where personal data is located, and all systems and devices in use must have the necessary data protection elements.

Kübra Özkahraman | Quality Assurance & Training Responsible

LEGISLATION ANALYSIS

Processing Data Based on Legitimate Interest Within the Scope of Article 5 of KVKK and Article 6 of GDPR

Article 5 of KVKK - Conditions for processing personal data

...

(2) Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:

...

f) it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

***

Article 6 of GDPR - Lawfulness of processing

(1)Processing shall be lawful only if and to the extent that at least one of the following applies

...

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

***

The fact that data processing is mandatory for the legitimate interests of data controllers is a legal reason for such data processing activity, provided that it does not harm the fundamental rights and freedoms of the data subject in KVKK and GDPR. On the other hand, both KVKK and GDPR do not include the definition of legitimate interest, this concept has been clarified with the decisions and guidelines of the Data Protection Authorities. Data controllers should evaluate the concrete situation regarding any data processing activity and determine the appropriateness of the legitimate interest as a legal reason.

Legitimate interest generally constitutes an appropriate legal reason for data processing activities that fall within the reasonable expectation of the data subjects and have minimal impact on privacy. The issues regarding the legitimate interest assessment in the light of the decision of the Turkish Personal Data Protection Board dated 25/03/2019 and numbered 2019/78, the opinions of the Working Group 29 and the reasons of the GDPR article are as follows:

- The assessment of legitimate interest consists of 3 parts:
    - Determination of legitimate interest
    - Obligation of data processing for the determined legitimate interest
    - The balance between the rights, freedoms and affected interests of the data subject and the legitimate interest of the data controller

- These three parts are considered as 3-step testing:
    - Purpose test: Is there a legitimate interest?
    - Requirement test: Is the processing essential for that legitimate purpose?
    - Balance test: Do the interests of the data subjects prevail over legitimate interests?

- The following questions need to be answered for the purpose test:
    - Why is the data wanted to be processed, what is wanted to be realized?
    - Who will benefit from data processing How will they benefit from that?
    - Is there a wider public interest in processing?
    - How important are these benefits? What will be the effect if the purpose is not achieved?
    - Is data processing unethical or illegal?

- The following questions should be considered for the requirement test:
    - Does data processing really help to realize that interest?
    - Is there a reasonable way to exercise the interest?
    - Is there a way to achieve the same result that is less intrusive to the interests of the data subjects?

- The following questions should be answered for the balance test:
    - What is the relationship between the data subject and the data controller?
    - Is there any sensitive personal data processed?
    - Would the data subjects expect their data to be used in this way?
    - Would it bother the data controller to explain the data processing in question to them?
    - Would the data subjects want to object or interfere with the activity? What is the possible impact on individuals?
    - How big of an impact will it have on individuals?
    - Will the data of children or disabled persons be processed? Are any of the individuals otherwise vulnerable?
    - Can any action be taken to minimize the impact on privacy?
    - Will people be given the right to object?

- If the legitimate interest in question can be exercised without data processing or with less effect on privacy, data processing based on legitimate interest will no longer be lawful.

- The legitimate interest must be specific and clear. Not only economic interests are the basis for legitimate interests, legitimate interests must be transparent and accountable, such as facilitating business processes or functioning.

- Documentation including the assessment of legitimate interest should be kept in records to strengthen accountability.

Rabia Dağcı | Legal Consultant | Attorney | CIPP/E

Prepared By

Ece Melis Erkoçak

Hazal Özçelik

Kerem Akdağ

Kübra Özkahraman

Onur İzli

Rabia Dağcı

Secvan Livanur Sefer

Şeyma Kaplan

Şule Özcan

Follow Us on Social Media...