BOSS YÖNETİŞİM HİZMETLERİ A.Ş. POLICY ON STORAGE AND DESTRUCTION OF PERSONAL DATA

January 23, 2017

1. INTRODUCTION

1.1. INTRODUCTION

Storage and destruction of personal data is among the top priorities of our Company. The most important part of this issue consists of the protection, storage and destruction of the personal data of our customers, prospective customers, employees, employee candidates, visitors, employees, shareholders and officials of the organizations that we cooperate with and third parties, which is governed by virtue of this Policy. The activities of our Company related to the storage and destruction of the personal data of our employees are governed in line with the principles of this Policy.

As per the constitution of the Republic of Turkey, everyone has the right to ask for the protection and destruction of their personal data. In terms of the protection and destruction of personal data, which is a constitutional right, the Company pays due care to the protection and destruction of personal data, which is governed by this policy, and adapts this as a Company policy.

Within this scope, the Company takes the necessary administrative and technical measures for the protection of personal data processed in accordance with the applicable legislation. This Policy shall provide detailed explanations regarding the fundamental principles adopted by our Company in processing the personal data, which are listed below:

- Rendering the personal data in compliance with law and principles of honesty,
- Ensuring that the personal data is accurate and, if necessary, up-to-date,
- Processing the personal data for specific, clear and legitimate purposes,
- Processing the personal data to the extent it is relevant, limited and proportionate to the purposes for which data are processed,
- Maintaining the personal data for a period stipulated in the applicable legislation or required for the purpose of processing thereof and destroying them when the necessary conditions are met,
- Elucidating and informing the data subjects,

  a Establishing the necessary system to enable the data subjects to exercise their rights,

  b Taking necessary measures for the storage of personal data, c Acting in compliance with the applicable legislation and the regulations of the Personal Data Protection Board (PDP Board) while transferring the personal data to third parties in line with the requirements of the purpose of processing thereof,

d Displaying the required sensitivity to the processing and protection of private personal data.

1.2. POLICY OBJECTIVE AND DEFINITIONS

The main objective of this Policy is to provide explanations regarding the personal data processing activities carried out by the Company pursuant to the law and the systems adopted for the protection of personal data and, in this context, to provide transparency by informing the people whose personal data is being processed by our company.

Definition	**Remarks**
Express Consent	Consent in relation to a specific matter, which is based on being informed and which is given with free will.
Anonymization	The personal data is changed in such a way that it loses its personal data quality without possibility of restoring the same. e.g.: Rendering the personal data incapable of being associated with a real person by means of techniques such as data masking, data aggregation or data distortion, etc.
Employee Candidate	Real persons who have made a job application to our company in any manner or allowed our company to review their resumes and related information.
Employees, Shareholders and Officials of the Organizations which we cooperate with.	Real persons that work at the organizations which we have any type of business relations with (including but not limited to business partners, suppliers, etc.), including the shareholders and officials of these organizations.
Processing of Personal Data	Any transaction carried out on the data, such as obtaining, recording, storage, preservation, alteration, reorganization, disclosure, transfer, takeover, making available, classifying the personal data or preventing its usage, by fully or partly automatic means, or by non-automatic means provided that they are part of a data recording system.
Data Subject	The real person whose data are processed. For example; Customers and employees.
Personal Data	Any kind of information about an identified or identifiable real person. Thus, processing of the information in relation to legal persons is outside the scope of the Law. For example; name and surname, Republic of Turkey ID No, e-mail, address, date of birth, credit card number etc.
Customer	Real persons who use or used the services provided by our Company regardless of whether they have any contractual relationship with our Company.
Private Personal Data	Data in relation to race, ethnic origin, political opinion,

	philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures and biometric and genetic data are private personal data.
Prospective Customer	Real persons who have requested to use or are interested in our services or deemed to potentially have such interest as per the commercial practices and principle of honesty
Company Shareholder	Real persons who are shareholders of our company
Company Official	Members of the board of directors of our company and other authorized real persons
Third Party	Third party real persons who have relations with the aforementioned persons to ensure transaction security between our company and these persons, or protect their rights and procure advantage (e.g.: Surety, Accompanying Person, Family Members and Kith and Kin)
Data Processor	Real and legal persons who process personal data on behalf of the data controller based on the authorization given by the data controller. For example, the cloud computing company which keeps our Company's data, their interviewers who obtain the signatures of the customers on the forms, the call center company which makes calls within the frame of scripts etc.
Data Controller	Data controller is the person who determines the purposes and means of processing of personal data, and who manages the medium (data recording system) where data are systematically recorded.
Visitor	Real persons who have entered the physical premises owned by our Company for various reasons or visited our internet sites.

1.3. SCOPE

This Policy covers all the personal data which are either processed by automatic means, or by non-automatic means provided that they are part of a data recording system.

1.4. APPLICATION OF THE POLICY AND THE RELEVANT LEGISLATION

The legislation which is in force in respect of the processing, storage and destruction of personal data shall be applicable as a matter of priority. In case of any conflicts between the legislation in force and the Policy, our Company accepts that the legislation in force shall prevail.

Our Company collects and processes verbal, written and electronic personal data due to both the regulations of the Social Security Institution, Turkish Employment Agency (İşkur), Regional Labor Organization, Directorate General of Migration Management, Revenue Administration and other relevant institutions, and our service contracts.

Our Company will be able to share the personal data in question only upon the explicit consent of our customers or in the other cases stipulated in Article 5/f of the Law on the

Protection of Personal Data and, in particular, in the legislation we are subjected to, with the purpose of providing our customers with value added services, opportunities and possibilities and increasing the service quality, only with the following: CottGroup Companies, "hereinafter to be referred to as CottGroup", which our Company is a subsidiary of (please see the list of the Group companies in Annex 3 hereto) and our affiliates both at home and abroad which will join the CottGroup Companies in the future, our direct and indirect subsidiaries and joint ventures, or public organizations and institutions which are authorized to request such data due to a legal requirement and, provided that sufficient measures are taken, domestic and foreign organizations, suppliers, authorized vendors/ dealers/ business partners with which we have contractual relations arising from our activities. Please visit *http://www.cottgroup.com* to obtain information on the partners of our company, companies within the group and our affiliates.

Among the CottGroup Companies, Boss Yönetişim Hizmetleri A.Ş. which holds all the necessary certifications, hosts and stores all the records belonging to the group companies at its own data center and follows up the destruction processes thereof.

The Policy has been created by materializing the rules laid down by the relevant legislation within the scope of the implementations of the Company. Our Company carries out the necessary system preparations to act in compliance with the time periods stipulated in the Law No 6698 on the Protection of Personal Data (the "Law") and the Regulation On The Deletion, Destruction And Anonymization Of Personal Data (the "Regulation").

1.5. DATE OF EFFECTIVENESS OF THE POLICY

This Policy issued by our Company takes effect on January 23, 2018. In case of renewal of the entire Policy or its specific articles, the date of effectiveness of the Policy shall be updated.

The Policy is published on the internet site of our Company and made available to the relevant people upon the request of data subjects.

2. PRINCIPLES IN RELATION TO STORAGE OF PERSONAL DATA

In accordance with Article 12 of the Law, our Company takes the necessary technical and administrative precautions in order to prevent unlawful processing of personal data to be processed by itself and unlawful access to data as well as to ensure proper security level for retaining the data and, within this scope it conducts or procure the conducting of the necessary inspections. Furthermore, all the processes are carried out within the scope of ISO 27001 Information Security Management System of Boss Yönetişim Hizmetleri A.Ş., which manages CottGroup data center.

2.1. ENSURING SECURITY OF PERSONAL DATA

2.1.1. Technical and administrative measures taken for Lawful Processing of Personal Data

Our Company takes any technical and administrative measures according to the technological capabilities and the cost of application, in order to ensure lawful processing of the personal data.

a) Technical measures taken for Lawful Processing of Personal Data

Main technical measures taken by our Company for lawful processing of the personal data are listed below:

- The operations of processing of personal data performed in our Company are controlled by technical systems that are created.

- By virtue of internal inspection mechanism, any technical measures taken are reported to the relevant person.

- Personnel with knowledge about technical issues is hired.

Within the scope of ISO 27001 Information Security Management System, risk management and risk processing plans, duties and responsibilities, business continuity plans, emergency incident management procedures are used and their records are maintained. Our Company publishes an information security policy including all these activities and makes arrangements regarding the awareness of the employees with respect to information security and relevant threats. As a dynamic procedure in which selected inspection targets are measured and the inspections are continuously followed up in terms of their performance and fitness for the purpose, information security management takes place among our most important assets through active support from the management and participation of the employees.

b) Administrative measures taken for Lawful Processing of Personal Data

Main administrative measures taken by our company for lawful processing of the personal data are listed below:

- The personnel is informed and trained about the law on protection of personal data as well as processing of personal data in accordance with law.

- The personnel is made aware of the information portfolio of our company and the related parties, and their values.

- Regarding the personal data processing operations performed by the business units of our company, the requirements to be fulfilled for ensuring conformity of such operations with the requirements of personal data processing as required by the Law are determined specific to each business unit and the detailed operation performed by it.

- In order to fulfill certain legal compliance requirements determined by our business units, awareness is raised specific to the relevant business units and application rules are determined. Any administrative measures required for inspection of these issues and ensuring continuity of the application are implemented via policies and trainings.

- Management takes any measures required for performance of any required software/ hardware/ version/ update modifications related with processing of data in a manner that would not disrupt security and system continuity.

- Department Managers inform their personnel about the Security Policies and Procedures, and Risk Management.

- The data processing manager reviews the effects of technological modifications on the systems of the company once a month.

- The Company Management enables the personnel to be informed about the quickly changing informatics security and security threats.

2.1.2. Technical and administrative measures taken for Prevention of Unlawful Access to the Personal Data

In order to prevent imprudent or unauthorized disclosure of, access to, transfer of or any other unlawful access to the personal data, our company takes technical and administrative measures depending on the nature of the data to be protected, the technological capabilities and the cost of application.

a) Technical Measures Taken for Prevention of Unlawful Access to Personal Data

Main technical measures taken by our company for prevention of unlawful access to the personal data are listed below:

- The company management inspects continuously the physical and system access authorizations of the personnel through the relevant systems in order to optimize data security and sustainability of the services provided and minimize potential data loss.

- Technical measures conforming to the technological developments are taken and the measures taken are updated and renewed periodically.

- Technical solutions for access and authorization are put into practice in compliance with the legal compliance requirements determined as per business function.

- Any technical measures taken are reported to the relevant person by virtue of the internal inspection mechanism and any issues that create risk are reassessed and the required technological solutions are produced.

- Any software and hardware including virus protection systems and firewalls are installed.

- All the entries into and exists from the Company are recorded. The records are followed up daily by the Human Resources Deputy Specialist. Records are converted into a filterable list in an order in the common media.

- Any measures are taken for ensuring proper protection and control of the information produced, kept and transferred internally in the company.

- In case of loss or theft of the computers, hard disks of all the personnel are encrypted with Bitlocker to prevent reading of important data by undesirable persons.

- All the personnel shall have access to and use the information within scope of the authorization granted to them.

- A Data Subject is defined for each data, and without the consent of the Data Subject, the Data Processing Specialist may not take any action or perform any transaction related with any electronic data of which s/he is not the data subject.

- Each department is responsible for the documents kept in their room. The personnel shall have access to the documents kept in the relevant department as specified in the access authorization table and any document may be taken outside the department upon approval of the department manager. Access Authorization table sets out definitions related with access to documents of the departments.

- Security awareness trainings shall be provided continuously.

- Access control has been optimized with additional regulations such as visitor admission and portable media policies.

- Personnel with knowledge about technical issues is hired.

b) Administrative Measures Taken for Prevention of Unlawful Access to Personal Data

Main administrative measures taken by our company for prevention of unlawful access to the personal data are listed below:

- Training is provided to the personnel about the technical measures to be taken for prevention of unlawful access to the personal data.

- Processes are designed and applied internally in the company per each business unit for access to the personal data and relevant authorization in accordance with the legal compliance requirements.

- Personnel is informed that they may not disclose any personal data learned to third persons in contradiction with the legislation, use them for any purpose other than the purpose of processing and that such obligation will survive their departure from the relevant position, and the necessary undertakings are obtained from them accordingly.

- Information portfolio and any type of personal data have been classified.

- Unless approved or labeled otherwise, all information is deemed confidential.

- If any information has various levels of confidentiality, the storage media is labeled according to the information with the highest level of confidentiality.

- Notwithstanding the level of confidentiality of information, the managers must always have access to such information.

- General Manager shall determine the trade secrets.

- A disposal date shall be determined for the documents and instruments and such date shall be managed according to the Procedure on Control of Records.

- The level of confidentiality determined for any information shall be reviewed at least annually.

- A file naming system should be established to ensure separation of various file types used from each other.

- Data classification labels should be in conformity with the labeling system of the company. The Procedure on Control of Documents shall apply in this regard.

- The users should upload the backup of their own computers on the files determined on the servers.

- Any attempts for exceeding authorization by the users that are logged-in the systems should be monitored and any violation of authorization should be controlled.

- In order to monitor the user's rights, any information about the transmission of confidential information to it should be sent to each user in controlled media, via cargo firms which have signed a confidentiality agreement, or by registered mail with return receipt requested.

- Each asset connected to the company network shall be named in a manner not understandable by the persons outside BOSS.

- All information of the company shall be put into one of the five classification categories given below: "Highly confidential", "Confidential", "General", "Public" and "Unimportant information".

- All the company know how is sub-labelled as per with access matrix. The sub-labels are operating with the DLP. Thus, the labels and sub-labels are based on the local retention periods in accordance with the applicable laws.

- In case a document that is to be labelled as "confidential" / "highly-confidential" the DLP generates an automated labeling mechanism by analyzing the document. (i.e. in case the document has ID information for an EU citizen or a Turkish citizen, credit card numbers, IBAN number, etc. DLP generates a label)

- All the information obtained from external sources shall be labeled properly by taking into consideration the classification system used throughout the entire corporation, including the computer storage media.

- If any information is determined as confidential, labels should be attached on a visible spot depending on the level of confidentiality of the information.

- The person who changes the content of any document containing confidential information shall use suitable classification label.

- Confidential information can be copied only by the authorized data subject.

- The user performing such copying process shall be responsible for the documents submitted to the photocopy personnel/left in the photocopy machine.

- Any official document issued by the persons should be written by non-erasable ink and bear a suitable mark. Any change made should be underlined, dated and re-approved.

- The phrase "CONFIDENTIAL" shall be written on all pages of confidential documents.

2.1.3. Storage of Personal Data in Secure Media

Our company takes technical and administrative measures depending on the technological capabilities and cost of application in order to ensure storage of personal data in secure media and prevent destruction, loss or modification of them for unlawful purposes.

a) Technical measures taken for Storage of Personal Data in Secure Media

Main technical measures taken by our company for storage of personal data in secure media are listed below:

- Systems in conformity with the technological developments are used in order to store personal data in secure media.

- Personnel specialized on technical issues is hired.

- Technical security systems are established for storage media and any technical measures taken are reported to the relevant person by virtue of the internal inspection mechanism and any issues that create risk are re-assessed and any required technological solutions are produced.

- In order to ensure secure storage of personal data, back-up programs are used in accordance with the law.

- All the system level passwords (for example, root, administrator) are required to be changed quarterly by the system.

- The system administrator uses different passwords for each system.

- The user is trained about not to share his/her password with others, not to write it on paper or insecure electronic media.

- A user ID and password may not be used in several computers simultaneously.

- Passwords are used for various purposes. Some of these are: User passwords, Web access passwords, e-mail access passwords, screen protection passwords, router access passwords etc. All users must pay attention to select a strong password.

- Servers are stored in physically secure environments. No unauthorized access to the system rooms is allowed. Entry into and exit from the system rooms are performed under control.

- It is forbidden to install operating system and the other software on the servers for usage purposes. Consent of the General Manager is required for the applications to be installed on the servers.

- The operating systems, system software and security software on the servers are updated continuously.

- Change Management Policy is also applicable to the servers.

- Any services not used on the server are deactivated.

- Backups with the same features are stored for the critical and important servers and in case of emergency, such backup server can be activated immediately.

- As determined by the Information Network and System Manager, logs are subject to regular inspection and follow-up by our company.

- If remote control of the servers is required, the communication between the management console and server is ensured via SSL over VPN.

b) Administrative Measures taken for Storage of the Personal Data in Secure Media

The main administrative measures taken by our company for storage of the personal data in secure media are listed below:

- The information security applications relate to all of our business processes performed by acting in accordance with law and legislation and conforming to the obligations arising from the agreements and labor obligations as well as our personnel, customers, solution partners, suppliers and all the relevant parties that may be affected from the result of our works.

- All the assets of our company are shown in the Assets Inventory. Assets Inventory is subject to change in due course in connection with any modification and developments. The data obtained as a result of risk evaluation in the assets inventory constitutes basis for continuous improvement and training of personnel in our company. Information security applications are an essential part of all the operations performed and are reviewed at least annually.

- Ensuring security of information sources is closely related to awareness and sensitivity of the personnel on this issue and their understanding and implementation of the powers and liabilities granted to them well. Therefore, our Company determines how to deal with the security aspect of the issues such as selection of the relevant personnel, assignment of any liabilities and powers, their dismissal, training etc., under policies and procedures.

- Continuity of three fundamental components of the information security management system is ensured in all the operations performed; Confidentiality: Prevention of unauthorized access to the important information, Integrity: Demonstration of accuracy and integrity of the information, Accessibility: Demonstration of accessibility to the information by the authorized persons, when necessary. The relevant system standards are related with the security of all data in written, printed, verbal and similar media, and not only the data stored in electronic media.

- Training is provided to the personnel about secure storage of personal data.

- It is forbidden to give password to any person on the phone.

- It is not allowed to share passwords with third persons.

- Passwords are subject to change at least once every 90 days, but it is allowed not to use password during file exchange with the customers and partners upon request of the customer/partner, or the passwords may be changed upon request of the customers/partners. If the request for change sent to the customer/partner is rejected upon expiry of the period of 90 days, the expired password will still be used in the communication with the customer/partner.

- The passwords for access to the database servers, modems, exchange, anti-virus program, collective e-mail sending software shall be kept in a document that can only be accessed by IT officer and General Manager.

- System automatically checks whether the passwords have been changed or not.

- Personnel competence and roles have been determined for granting right of access to the information of various level.

- Users are provided with written notifications showing their rights of access and the relevant confirmation is taken.

- Discipline procedure is applied in the cases when the unauthorized personnel sees or obtains any confidential and sensitive information in the company.

- A background search is conducted for the person to which liabilities will be assigned in information systems, any declared academic and professional information are confirmed and reference search is made in the work environment and externally to obtain satisfactory information about the character of the person.

- The users with access to critical data signs confidentiality agreements.

- Corporate information security awareness trainings are provided. They are scheduled in the annual training plans and included in the training catalog.

- Access rights of the users whose job definition has changed or who has left the company are deleted immediately.

2.1.4 Inspection of the Measures Taken for Protection of Personal Data

Our Company performs or ensure performance of any necessary inspections internally pursuant to article 12 of the Law. The results of such inspection are reported to the relevant department within the scope of the internal operation of the Company and operations are performed for improvement of the measures taken.

2.1.4. Measures to be Taken In case of Unauthorized Disclosure of Personal Data

If the personal data processed in compliance with article 12 of the Law is obtained by third persons through unlawful means, our company runs a system that ensures notification of such issue to the data subject and PDP Board as soon as possible.

If it is deemed necessary by the PDP Board, this issue may be announced on the web site of the PDP Board or via any other means.

2.2. RESPECTING THE RIGHTS OF DATA SUBJECT, DEVELOPMENT OF CHANNELS FOR TRANSFER OF SUCH RIGHTS TO OUR COMPANY AND EVALUATION OF THE REQUESTS OF THE DATA SUBJECTS

Our Company enforces any required channels, internal operation, administrative and technical arrangements in accordance with article 13 of the Law in order to assess the rights of data subjects and inform the data subjects as required.

If the data subjects submit their claims for the rights listed below to our Company in writing, our Company concludes the claim free of charge as soon as possible and at the latest within thirty days, depending on the nature of claim. However, if the transaction requires any additional cost or effort, our Company shall charge a fee at the rate to be determined by the PDP Board or if not determined a reasonable fee. Data subjects are entitled to;

- Learn whether or not personal data have been processed,

- Request information on the procedure, if personal data have been processed,

- Obtain information on the purpose of processing personal data and find out whether personal data has been used as fit for the purpose,

- Obtain information about the third persons to whom personal data were communicated domestically or abroad,

- If personal data have been processed in an incomplete and wrongful manner, to request correction of the same, and to request that the third parties to whom personal data are transferred are also informed about the transaction executed in this regard,

- In the case where, although they have been processed pursuant to the legislative provisions, the reasons requiring them to be processed cease to exist, to request that the personal data are deleted or destroyed, and the third parties to whom personal data are transferred are also informed about the transaction executed in this regard,

- Object to the occurrence of a result which is detrimental to the person concerned as a result of analyzing the processed data exclusively through automatic systems,

- Request compensation for damages in the case where damages are sustained as a result of the illegal processing of personal data,

- Request disposal of personal data if the requirements are fulfilled.

More detailed information about the rights of the data subjects is available in Section 10 of this Policy.

2.3. PROTECTION OF PRIVATE PERSONAL DATA

The Law gives special importance to certain personal data for the reason that they have a risk to cause victimization of the persons or discrimination when processed unlawfully.

Such data consists of the data in relation to race, ethnic origin, political opinion, philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Our company acts responsibly towards protection of the private personal data that is defined as data of "private nature" by the Law and that is processed in accordance with law. Within this scope, our Company applies any technical and administrative measures taken for protection of personal data with regard to private personal data with due care and any required inspections are made internally.

More detailed information about the processing of private personal data is available in Section 3 of this Policy.

2.4. RAISING AWARENESS AND INSPECTION OF THE BUSINESS UNITS FOR THE PROTECTION AND PROCESSING OF PERSONAL DATA

Our Company ensures that the necessary trainings are given to the business unit in order to raise awareness on the prevention of illegal processing of and access to the personal data and retention of the data.

The systems required for raising awareness on the protection of personal data among the existing and newly recruited employees of the business units in our company and in this regard, cooperation with professional people are established if required.

2.5. RAISING AWARENESS AND INSPECTION OF THE BUSINESS PARTNERS AND SUPPLIERS FOR THE PROTECTION AND PROCESSING OF PERSONAL DATA

Our Company ensures that the necessary trainings and seminars are given to the business partners in order to prevent illegal processing of and access to the personal data and raise awareness on the retention of the data.

3. PRINCIPLES IN RELATION TO PROCESSING OF PERSONAL DATA

Our Company performs processing of personal data in accordance with article 20 of the Constitution and article 4 of the Law, in conformity with the law and good faith principles, by pursuing accurate and when necessary up-to-date, and specific, explicit and legitimate goals, and in a manner that is connected and limited with the relevant goal, and by acting proportionately. Our Company stores personal data for a time period as stipulated by the legislation or as required by the purpose of processing of personal data.

Our Company processes the personal data on the basis of one or more of the conditions set out in Article 5 of the Law on processing of personal data, pursuant to Article 20 of the Constitution and Article 5 of the Law.

Our Company informs the data subjects and provides the necessary information upon the information request of the data subjects, pursuant to Article 20 of the Constitution and Article 10 of the Law.

Our Company acts in compliance with the stipulations on the processing of private personal data pursuant to Article 6 of the Law.

Our company acts in line with the regulations stipulated in the law with respect to the transfer of personal data and established by the PDP Board, pursuant to articles 8 and 9 of the Law .

3.1. PROCESSING PERSONAL DATA IN COMPLIANCE WITH THE PRINCIPLES STIPULATED IN THE LEGISLATION

3.1.1. Processing in Compliance with Law and Principles of Good Faith

In the processing of personal data; our Company acts in compliance with the principles which are enshrined in legal regulations and those which are related to general confidence and good faith. Within this scope, it takes into consideration the requirements of proportionality and use the personal data only to the extent required to achieve the relevant purpose.

3.1.2. Ensuring that the Personal Data is Accurate and Up-To-Date when Necessary

Our Company ensures that the personal data processed by it are accurate and up-to-date by taking into account the fundamental rights of the data subjects and its own legitimate benefits. It takes the necessary measures in this regard. For instance, the Company has established a system which enables the data subjects to correct their personal data and confirm their accuracy. Detailed information about this issue is available in Section 10 of this Policy.

3.1.3. Processing for Specific, Clear and Legitimate Purposes

Our Company has set its objective as lawful and legitimate processing of personal data explicitly and strictly. Our Company processes personal data in connection with the services provided by it and to the extent required in this regard. Our Company reveals the purpose for which the personal data will be processed even before the commencement of personal data processing activity.

3.1.4. Being relevant, limited and proportionate to the purposes for which data are processed

Our Company processes the personal data in a way to achieve the purposes determined and avoids processing of personal data which are not relevant or required for achieving the purpose. For instance, no processing of personal data with the purpose of meeting any possible future needs is carried out.

3.1.5. Retaining for the Period Stipulated in the Relevant Legislation or the Period Required for the Purpose of Processing Thereof

Our Company retains personal data only for the period set out in the relevant legislation or the period required for the purpose of processing thereof. In this context, first of all our Company identifies whether a period is stipulated in the relevant legislation for the storage of personal data, and if a period is prescribed, it acts in accordance with it, whereas if no period is prescribed, it retains the personal data for the period required for the purpose of processing thereof. Upon expiry of the specified period or if the reasons that require the processing of personal data cease to exist, the personal data is deleted, destroyed or anonymized by our

Company. Our Company does not store personal data in consideration of any possibilities to use them in the future. Detailed information about this issue is available in Section 9 of this Policy.

3.2. PROCESSING OF THE PERSONAL DATA BASED ON AND LIMITED TO ONE OR MORE OF THE CONDITIONS OF PROCESSING OF PERSONAL DATA LISTED IN ARTICLE 5 OF THE LAW

Protection of Personal Data is a constitutional right. Fundamental rights and freedoms can be restricted only in connection with the reasons stated in the relevant articles of the Constitution without changing their essence and exclusively by the law. By virtue of the third paragraph of article 20 of the Constitution, personal data may only be processed in the cases required by law or upon explicit consent of the person. Our Company processes the personal data accordingly and in accordance with the Constitution only when required by law or upon explicit consent of the person. Detailed information about this issue is available in Section 7 of this Policy.

3.3. ELUCIDATING AND INFORMING THE DATA SUBJECT

Our Company informs data subjects whilst obtaining the personal data in accordance with Article 10 of the Law. In this context, it gives information about the identity of the Company and its representative, if any, the purpose for which personal data will be processed, to whom and for which purposes the processed data may be transferred, method and the legal reason of collecting personal data, and the rights possessed by the data subject. Detailed information about this issue is available in Section 10 of this Policy.

It has been stipulated in Article 20 of the Constitution that everyone is entitled to be informed about their own personal data. Accordingly, “requesting information” is also listed among the rights of the data subject as per Article 11 of the Law. Within this scope, our Company provides the necessary information upon the information request of the data subject, pursuant to Article 20 of the Constitution and Article 11 of the Law. Detailed information about this issue is available in Section 10 of this Policy.

3.4. PROCESSING OF PRIVATE PERSONAL DATA

Our Company acts diligently in compliance with the stipulations of the Law in processing of the personal data which are specified as data of “private nature” under the Law.

Article 6 of the Law stipulates that certain personal data which bears the risk of victimization and discrimination of the persons if processed illegally, are designated as “private” personal data. Such data consists of the data in relation to race, ethnic origin, political opinion, philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

In line with the Law, private personal data may be processed by our Company in the following cases, provided that the adequate measures to be determined by the PDP Board are taken:

- Upon explicit consent of the data subject or
- In the absence of explicit consent of the data subject;

– Private personal data other than the health condition and sexual life of the data subject, in cases where stipulated by laws,

– Private personal data in respect of the health of the data subject and sexual life are only processed by the persons who are bound by a duty of confidentiality or the authorized bodies and institutions for the purpose of public health protection, preventive medicine, medical diagnosis, treatment and healthcare services, planning and management of health services and financing thereof.

3.5. TRANSFER OF PERSONAL DATA

In line with its lawful data processing purposes, our Company may transfer the personal data and private personal data of the data subject to third parties by taking necessary security measures. In this context, our Company acts in compliance with the stipulations set forth in Article 8 of the Law. Detailed information about this issue is available in Section 6 of this Policy.

3.5.1. Transfer of Personal Data

In line with the legitimate and lawful purposes for the processing of personal data, our Company may transfer the personal data to third parties on the basis of and to the extent limited with one or more of the conditions for processing of personal data stipulated in Article 5 of the Law and listed herein below:

- Upon explicit consent of the data subject;
- If the transfer of personal data is expressly permitted by the laws,
- If it is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent;
- If it is necessary to transfer the personal data of parties of a contract, provided that such transfer is directly related to the establishment or performance of that contract,
- If the transfer of personal data is mandatory to fulfill the legal obligations of our Company.
- If the data subject has made the personal data public,
- If the transfer of personal data is mandatory for the creation, usage, or protection of a right,
- If the transfer of personal data is mandatory for the legitimate interests of our Company, provided that the fundamental rights and freedoms of the data subject are not harmed.

3.5.2. Transfer of Private Personal Data

In line with its legitimate and lawful data processing purposes and by paying the due care and attention, taking necessary security measures and establishing sufficient precautions stipulated by PDP Board, our Company may transfer the private personal data to third parties under the following circumstances:

- Upon explicit consent of the data subject or
- In the absence of explicit consent of the data subject;

– Private personal data of the data subject apart from health condition and sexual life (data in relation to race, ethnic origin, political opinion, philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, criminal convictions and security measures and biometric and genetic data), in cases where stipulated by the laws,

– Private personal data in respect of the health of the data subject and sexual life are only processed by the persons who are bound by a duty of confidentiality or the authorized bodies and institutions for the purpose of public health protection, preventive medicine, medical diagnosis, treatment and healthcare services, planning and management of health services and financing thereof.

4. CATEGORIZATION, PURPOSES OF PROCESSING AND STORAGE PERIODS OF THE PERSONAL DATA PROCESSED BY OUR COMPANY

Our Company informs the data subject about which data subject group processes their personal data, the purposes of processing of personal data of the data subject and their storage times within the scope of the obligation to inform in accordance with article 10 of the Law.

4.1. CATEGORIZATION OF PERSONAL DATA

Our Company processes the below mentioned categories of personal data by informing the relevant persons pursuant to Article 10 of the Law, in line with our Company's legitimate and lawful purposes for the processing of personal data, based on and to the extent limited with one or more of the conditions of personal data processing set forth in Article 5 of the Law, in compliance with the general principles of Law and in particular the principles stipulated in Article 4 of the Law relating to processing of personal data, and all the obligations regulated under the Law, and limited to the periods set forth within the scope of this Policy. The data subjects within the scope of this Policy, whose personal data are processed under these categories, are identified in Section 5 of this Policy.

CATEGORIZATION OF PERSONAL DATA	DESCRIPTION
Credentials	All the information on the documents such as Driver's License, Identity Card, Residence Document, Passport, Bar Association Identity Card and Marriage Certificate, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically, or non-automatically as part of a data recording system

Contact Details	Information such as telephone number, address or e-mail, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically, or non-automatically as part of a data recording system
Information on Customers	Information obtained or generated about a person as a result of our commercial activities and the operations carried out by our business units in this regard, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically, or non-automatically as part of a data recording system
Information on Family Members and Kith and Kin	Information on the family members and kith and kin of the data subject in relation to the services we provide or in order to protect the legal interests of the Company and data subject, which explicitly belong to a real person who is identified or identifiable, and which are found in the data recording system
Information on Customer Transactions	Information on the records regarding the use of our services and the customer's instructions and requests required for their use of services; which explicitly belong to a real person who is identified or identifiable, and which are found in the data recording system
Physical Space Security Information	Personal data in relation to the entries and documents received on entry to physical space or during the stay in the physical space, which explicitly belong to a real person who is identified or identifiable, and which are found in the data recording system
Transaction Security Information	Personal data processed to ensure our technical, administrative, legal and commercial security whilst carrying out our business, which explicitly belong to a real person who is identified or identifiable, and which are found in the data recording system
Risk Management Information	Personal data processed by means of methods used in accordance with the generally accepted legal and business practices and good faith principles to enable us to manage our commercial, technical and administrative risks, which explicitly belong to a real person who is identified or identifiable, and which are found in the data recording system
Financial Information	Personal data processed in relation to the information, documents and entries which show any financial outcome which has been reached according to the type of legal relationship that our company has established with the data subject, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically, or non-automatically as part of a data recording system
Personnel Information	Any kind of personal data processed to obtain information that will constitute basis for the creation of personnel rights of our employees or real persons who are employed by our Company, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically

	or non-automatically as part of a data recording system
Employee Candidate Information	Personal data processed in relation to those individuals who have made an application to become employed by our Company or who have been evaluated as a employee candidate in accordance with our Company's human resources requirements pursuant to business practices and good faith principles or those who are employed by our Company, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of a data recording system
Information on Transactions of Employee	Personal data in relation to any business transaction which has been executed by our employees or the real persons who have employment relations with our Company, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system
Information on the Employee's Performance and Career Development	Personal data processed for the purpose of measuring the performance of our employees or the real persons who are employed by our Company, and planning and administer their career development within the scope of our Company's human resources policy which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system
Information on Fringe Benefits and Interests	Your personal data which are processed for planning of the fringe benefits and interests that we offer and will offer to our employees or the real persons who are employed by our Company, for determination of the objective criteria in relation to the entitlement thereto, and follow-up of the entitlement thereto, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system
Legal Transactions and Compliance Information	Your personal data processed within the scope of determination and pursuit of our legal receivables and rights, discharge of our debts and our legal obligations and compliance with the policies of our Company, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system
Audit and Inspection Information	Your personal data processed within the scope of our Company's legal obligations of and compliance with its policies, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system

Private Personal Data	Information that is stipulated in Article 6 of the Law, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system
Information on Request/Complaint Management	Personal data relating to the receipt and evaluation of any request or complaint addressed to our Company, which explicitly belong to a real person who is identified or identifiable, and which are processed in part or in full automatically or non-automatically as a part of data recording system

4.2. PURPOSE OF PROCESSING OF PERSONAL DATA

Our Company process the personal data to the extent limited with the purposes and conditions in terms of the personal data processing set forth in Article 5, Item 2 and Article 6, Item 3 of the Law. These purposes and conditions can be listed as below;

- Engagement of our Company with the relevant activity in relation to the processing of your personal data is explicitly stipulated by laws,
- The processing of your personal data by our Company is directly related to and necessary for the conclusion or performance of a contract,
- The processing of personal data is mandatory for the fulfillment of our Company's legal obligation,
- Provided that you have revealed the personal data to the public; our company processes the personal data to the extent limited with your purpose of publicity,
- Processing of personal data by our Company is obligatory for the establishment, exercise or protection of rights of our company or yourselves or third persons,
- Provided that your fundamental rights and freedoms are not infringed, the processing of personal data is obligatory for the legitimate interests of our Company,
- The processing of personal data by our company is obligatory for the preservation of the life and physical integrity of the data subject or another person, and in such a case, the data subject being in a position where he /she cannot give his/her consent due to an actual impossibility or legal invalidity,
- The processing of private personal data other than the health condition and sexual life of the data subject is stipulated by laws,

– Private personal data in respect of the health of the data subject and sexual life are only processed by the persons who are bound by a duty of confidentiality or the authorized bodies and institutions for the purpose of public health protection, preventive medicine, medical diagnosis, treatment and healthcare services, planning and management of health services and financing thereof.

In the case that the above conditions do not exist; the Company seeks to obtain the express consent of the data subjects in order to process personal data.

Under the aforementioned conditions; our Company may process the personal data for the purposes including but not limited to:

- Within the scope of conducting the necessary works by our business units to perform the business activities carried out by our Company and carrying out the related business processes; our customers who take services from our Company concerning such activities are obliged to obtain the necessary permissions from their employees and the relevant persons /data subjects) in their capacity as data controller and act in accordance with their obligation to inform.

- Ensuring business activities and business continuity, planning and execution of activities,

- Following up of finance and/ or accounting transactions,

- Event management,

- Submitting information to the authorities pursuant to the legislation,

- Planning and performance of corporate communication activities,

- Planning and performance of operation processes

- Planning and execution of access authorizations of business partners and/ or suppliers to the information

- Management of anything related to human resources, consultancy, payroll calculation, wages

- Provision of any software services

- Legal requirements of work permit, registered e-mail address, e-signature and similar services.

- Within the scope of conducting the necessary works and carrying out the relevant business processes to enable the relevant persons utilize the services of our company;

- Planning and execution of customer relations management processes,

- Following-up of the customer requests and/ or complaints,

- Planning and execution of marketing processes of services,

- Following-up of contract processes and/ or legal requests,

- Within the scope of ensuring compliance with human resources policies of our Company;

- Fulfilling the obligations within the frame of occupational health and safety and taking necessary measures,

- Evaluating the job applications in conformity with the human resources policies of our company,

- Fulfilling the obligations for the company employees arising from the employment contract and/ or legislation,

- Carrying out recruitment and dismissal transactions

- Evaluating wage- performance process,

- Managing wages and payrolls,

- Planning and implementation of internal training activities and

- Performing other human resources operations,

- Within the scope of establishing the legal and commercial security of our company and the people who have business relations with our company;

- Following-up of the legal affairs of the Company,
- Planning and implementation of the operational activities required for ensuring the performance of Company's activities in compliance with the Company procedures and/ or the applicable legislation,
- Creating and following-up of visitor records,
- Ensuring security of the Company's fixtures and resources,
- Ensuring security of company's operations,
- Planning and execution of emergency management processes,
- Planning and/ or execution of company's financial risk processes,

• Within the scope of determining and implementing our company's commercial and business strategies;

- Financial operations, communication, market research and social responsibility activities, purchasing operations, product/ project/ production/ investment quality processes and operations carried out by our Company,
- Internal system and implementation management operations,
- Planning and implementation of external training activities,
- Management of relations with the business partners and/ or suppliers

.

If the data subject does not give explicit consent, this shouldn't be interpreted as non-performance of all personal data processing activities of our relevant business units within the scope of the above purpose; but non-performance of personal data processing activities, which don't require the explicit consent of the data subject for the processing of personal data as per the first paragraph that fall outside the scope of the personal data processing activities within the same scope of purpose and those of our business units who are oriented towards this purpose.

4.3. STORAGE PERIOD OF PERSONAL DATA

Provided that it is stipulated by the applicable laws and legislations, our Company retains the personal data for the periods mentioned therein.

Unless the legislation prescribes how long personal data should be stored, our company processes personal data for the period required pursuant to the implementations and the business practices, in connection with the services provided by our company while processing that data and then deletes, destroys or anonymizes the personal data. Detailed information about this issue is available in Section 9 of this Policy.

If the purpose for processing the personal data ceases to exist and the period prescribed by the relevant legislation and company expires; personal data may only be stored to constitute evidence in the legal disputes or to claim the right associated with the person data or establish defense. In determination of these periods, storage periods are determined based on the periods of limitation for asserting the aforementioned right, and although the periods of limitation have expired, the examples in the previous requests made to our Company on the same issues. In this case, the personal data stored are not accessed for other purposes, however, when it is necessary to use them in the relevant legal dispute, the relevant personal data are accessed. After the period mentioned here has expired, personal data are deleted, destroyed or anonymized.

5. CATEGORIZATION OF PERSONAL DATA PROCESSED BY OUR COMPANY IN RESPECT OF THE DATA SUBJECTS

5.1. CATEGORIZATION OF PERSONAL DATA

Despite the fact that our company processes the personal data of the below listed categories of data subjects, the scope of this policy is limited to our customers, potential customers, employee candidates, company shareholders, company officials, our visitors, employees, shareholders and officials of the organizations with which we cooperate.

Although the categories of the persons whose personal data are processed by our Company are within the above mentioned scope, the persons who are outside this scope may submit their requests under the Law and their requests shall be taken into consideration within the scope of this Policy.

The concept of third parties within the scope of this policy is clarified below.

Data Subject Category	Description
Customer	Real persons who use or used the services provided by our Company regardless of whether they have any contractual relationship with our Company.
Prospective Customer	Real persons who have requested to use or are interested in our services or deemed to potentially have such interest as per the commercial practices and principle of honesty
Visitor	Real persons who have entered to our Company physically for various reasons or visited our internet sites
Third Party	Third party real persons who have relations with the aforementioned persons to ensure transaction security between our company and these persons or protect their rights and procure advantage
Employee Candidate	Real persons who have made a job application to our company in any manner or allowed our company to review their resumes and related information.
Company Shareholder	Real person(s) who are shareholders of our Company
Company Official	Members of the boards of our company and other authorized real

	person(s)
Employees, Shareholders and Officials of the Organizations whom we cooperate with.	Real persons that work at the organizations whom we have any type of business relations with (including but not limited to business partners, suppliers, etc.), including the shareholders and officials of these organizations.

6. THIRD PARTIES TO WHOM OUR COMPANY TRANSFERS PERSONAL DATA AND THE PURPOSES OF TRANSFERRING

6.1. TRANSFER TOOLS

Our Company notifies data subjects about the data groups to whom the personal data are transferred in accordance with Article 10 of the Law.

Our company may transfer the persona data of the customers to the below listed person groups in accordance with Article 8 and Article 9 of the Law:

(i) business partners
(ii) suppliers
(iii) affiliates
(iv) shareholders
(v) legally competent public institutions and organizations
(vi) legally competent private jurists

Our Company acts in compliance with the provisions stipulated in Section 2 and Section 3 of this Policy whilst transferring personal data.

7. PROCESSING PERSONAL DATA ON THE BASIS OF AND TO THE EXTENT LIMITED TO THE PROCESSING CONDITIONS SET OUT IN THE LAW

Our Company informs data subjects about the data personal data processed in accordance with Article 10 of the Law.

7.1. PROCESSING OF PERSONAL DATA AND PRIVATE PERSONAL DATA

7.1.1. Processing of Personal Data

Express consent of the data subject constitutes only one of the legal basis which enables lawful processing of personal data. Apart from express consent, personal data may also be processed in case of the existence of one of the below-specified conditions. The basis on which personal data processing activity is carried out may be one or more than one of the below-specified conditions. If the processed data are private personal data, then the conditions set forth under this section shall apply.

Although the legal basis regarding to the processing of personal data by our Company differs, the general principles of Article 4 of the Law is complied with for all kinds of data processing activities.

(i) Availability of the Express Consent of the Data Subject

One of the conditions for the processing of personal data is the explicit consent of the data subject. The explicit consent of the data subject should be given specific to a matter, based on informing and by free will.

Apart from the purpose of processing arising from the reasons why personal data has been obtained (primary processing), in case of any processing of personal data (secondary processing), presence of at least one condition listed in items (ii), (iii), (iv) (v), (vi), (vii) and (viii) of this section is required and if any one of such conditions is not present, then our company processes the personal data upon the explicit consent of the data subject given for these processing activities.

In order to process the personal data on the basis of the explicit consent of the data subject, the explicit consents of the customers, potential customers and visitors are taken by the relevant methods.

(ii) Being Explicitly Stipulated by the Laws

The personal data of the data subject shall be processed lawfully if it is explicitly stipulated by the Laws.

(iii) Inability to Obtain Express Consent of the Relevant Person Due to Actual Impossibility

Data may be processed without the explicit consent of a person if it is compulsory to process personal data in order to protect the life or body integrity of that person or any other person where a person cannot give his/her consent or whose consent is deemed invalid due to actual impossibility.

(iv) Direct Relationship with Conclusion or Performance of a Contract

In case it is necessary, it is possible to process personal data belonging to the parties of a contract, provided that it is directly related to the conclusion or performance of said contract.

(v) Fulfillment of Legal Obligation by the Company

Personal data of the data subject may be processed, if processing is compulsory to fulfill the legal obligations of our Company as a data controller.

(vi) Revealing the personal data to the public by the data subject

The personal data may be processed if such personal data is revealed to the public by the data subject himself/ herself.

(vii) Mandatory processing of Data for Establishment or Protection of a Right

In case data processing is mandatory for establishing, exercising or protecting a right, personal data of the data subject may be processed.

(viii) Mandatory Processing of Data for the Legitimate Interest of Our Company

If processing of data is mandatory for the legitimate interests of our Company, personal data of the data subject may be processed, provided that the fundamental rights and freedoms of the data subject are not infringed.

7.1.2. Processing of Private Personal Data

In case of lack of explicit consent of the data subject; the private personal data are processed by our company only in the following circumstances provided that sufficient measures determined by the PDP Board have been taken:

(i) Private personal data other than the health condition and sexual life of the data subject, in cases where stipulated by laws,

(ii) Private personal data in respect of the health of the data subject and sexual life are only processed by the persons who are bound by the duty of confidentiality or authorized bodies and institutions for the purpose of public health protection, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

(iii) Circumstances which are obligatory to be monitored in terms of personnel affairs such as medical visits, health report, sick leave, maternity leave and as per the provisions of labor law, social security and occupational health in order to provide the services related to the human resources and payroll processes.

8. DATA PROCESSINGACTIVITIES WITHIN THE PREMISES

In this section explanations shall be given regarding to the camera surveillance system of our Company and information shall be provided on how the protection of personal data, confidentiality thereof and fundamental rights of a person are ensured.

Within the scope of camera surveillance activities, our Company aims to increase the quality of the services provided, ensure its reliability, establish safety of the customers and other people and protect the interests of the customers in respect of the service they take.

Measures against Theft - Sabotage - Vandalism

The security of the premises against theft and terrorism is provided by the building management. Entrances to our company are controlled by camera recording.

* Closed circuit camera systems, audio recording devices,

Closed Circuit TV do not provide images externally. It is monitored on LCD TV.

It is monitored by the Company Executives over Internet.

Movement Detectors, burglar alarms,

8.1 . MONITORING ACTIVITIES

8.1.1. Legal Basis for Camera Surveillance Activities

The camera surveillance activities of our company are carried out in compliance with the Law on Private Security Services and the applicable legislation.

8.1.2. Conducting Camera Surveillance Activities In terms Of the Personal Data Protection Law

Our Company acts in accordance with the statutory regulations provided in the Law whilst conducting camera surveillance activities for security purposes.

Our Company conducts camera surveillance activities in order to ensure security in terms of the purposes stipulated in the laws and in compliance with the conditions listed in the Law for the processing of personal data.

8.1.3. Notification of Camera Surveillance Activities

Our company informs the data subject pursuant to Article 10 of the Law.

In addition to the provision of information regarding the general issues (See Section 3/ Paragraph 3.3), our Company gives notification by means of more than one methods regarding the camera surveillance activities in compliance with the reference regulations in the EU.

The objective is, therefore, to prevent infringement of the fundamental rights and freedoms of the data subject and ensure transparency and elucidation of the data subject.

8.1.4. Purpose of Conducting Camera Surveillance Activities and Being Restricted with the Purpose

Our company processes the personal data in a manner relevant, limited and proportionate to the purposes for which data are processed, pursuant to Article 4 of the Law.

The purpose for the camera surveillance activities conducted by our company is limited to the purposes listed in this Policy. Accordingly, the surveillance areas and number of the security cameras and the time when surveillance will be conducted are put into practice in a manner adequate and limited to achieve this purpose. Surveillance is not carried out at areas which may be deemed as intervention in the way to infringe the personal privacy and beyond the security purposes (for instance, toilets).

8.1.5. Ensuring Security of the Data Obtained

Our Company takes the necessary technical and organizational measures for ensuring security of the personal data obtained as a result of the camera surveillance activities, pursuant to Article 12 of the Law. (See: Section 2/Paragraph 2.1)

8.1.6. Storage Period of the Personal Data Obtained As a Result of Camera Surveillance Activities

Detailed information regarding to the storage period of the personal data obtained as a result of camera surveillance activities of our company is provided under Article 4.3 entitled Storage Period of Personal Data of this Policy.

8.1.7. The Persons Who Have Access to the Information Obtained As a Result of Monitoring and the Persons to Whom Such Information is Transferred

Only a limited number of employees have access to the records recorded and retained in the digital media.

8.2. MONITORING THE ENTRANCES AND EXITS OF THE VISITORS WITHIN THE BUILDING

In order to establish security and for the purposes mentioned in this Policy, our Company conducts processing of personal data regarding to the monitoring of entrances and exits of the visitors.

When the name and surnames of the persons who come to the premises as a visitor are obtained or by means of notices put up in the Company or otherwise availed to the access of the visitors, such data subjects are informed accordingly. The data obtained in order to monitor the entrances and exits of the visitors are processed only for this purpose and the related personal data are recorded to the data recording system in physical medium.

8.3. STORAGE OF THE RECORDS REGARDING TO THE INTERNET ACCESS PROVIDED TO THE VISITORS OF OUR PREMISES

In order to ensure the security by our Company and for the purposes mentioned in this Policy, our Company may provide internet access to our visitors as per their requests. In this context, the log records regarding to your internet access are recorded pursuant to the mandatory provisions of Law no 5651 and the legislation regulated in accordance with this law; such records are processed only if requested by the authorized public organizations and institutes or to fulfill our legal obligations during the internal auditing processes.

The log records obtained within this frame are accessible only by a limited number of employees. The Company employees, who have access to the subjected records, access to such records only to use them upon the request and during the inspection processes of authorized public organizations and institutions and share them with legally authorized persons. The limited number of persons who have access to the records represent by virtue of a confidentiality agreement that they shall protect the confidentiality of the data accessed.

8.4. FIRE

Smoke has an impact on the disk heads, optic disks and tape drivers. The most dangerous cause of smoke is cigarettes. Smoking is not allowed in the system room.

The fire and smoke detectors in the system room should be controlled to ensure that they are in working condition. In case of an alert, it should be ensured that such alerts are communicated to the relevant people by e-mail, SMS, telephone, etc. Automatic fire alarm system should be checked to ensure that it could be deactivated in case of false alarms and emergencies.

It is ensured that the portable fire extinguishers are located to the door as close as possible and the personnel who have access to the system room has adequate experience to use this extinguisher and the fire extinguishers are controlled on a monthly basis to ensure that they are full.

Automatic gas fire extinguishing systems should be preferred for the system rooms. If the fire extinguishing system is a gas system such as CO^2, FM200, NAF-S–III, Halon, the warning board which demonstrates what to be done to ensure that the personnel who will enter to the system room upon the fire alert is not effected by the gas should be placed on the outside of the door of the system room or at a suitable place.

Mobile phones, walkie-talkies, any kind of radio receivers and transmitters damage the computer systems. In particular, strong transmitters damage the computer systems permanently. Some gas fire extinguishing systems may tend to explode when close to the aforementioned receivers - transmitters. In no way receivers - transmitters should be used in environments where this kind of fire extinguishers are located. Any receivers and transmitters should be kept at a minimum distance of 2.5 m away from computer systems, cables and peripheral units.

8.5. TEMPERATURE

Likewise humans, computer hardware can maintain their functionality between certain temperature values. For many hardware, maintaining the room temperature between 10-25 °C would be suitable. If the temperature of the environment where the hardware are located is too high, the fans of the systems would not be sufficient and the components of the hardware could be damaged or the systems would switch to protect mode. If the temperature decreases too much, when the hardware are switched on, they would enter into thermal shock and may become inoperative due to cracking of the circuits.

The appropriate temperature range (generally 20-25 °C) should be determined by making use of the user manuals of the hardware and the room temperature should be balanced by means of air conditioning and climatization systems.

Thermal heat detectors should be placed in the system room to enable alarms in too hot and too cold temperatures. In case of an alert, it should be ensured that such alerts are communicated to the relevant people by e-mail, SMS, telephone, etc.

The hardware placed too close to the walls may hinder the ventilation and cause an increase of the inner temperatures of the systems. Thus, attention should be paid to placing the hardware not too close to the walls.

8.6. EARTHQUAKE AND EXPLOSION

Although the vibration is too low to disturb the people, it may harm computer systems in the long term. Even the lightest vibration may over time lead to distortion in the head adjustments of the hard disks. If you are in a region with high vibrations, it may be considered to cover the ground in the system room with rubber or plastic-derivative materials.

Although every earthquake wouldn't damage the systems directly, it may have effects which would result in indirect damages to the hardware. In order to ensure business continuity in the event of a possible severe earthquake;

- It is avoided to place the hardware too high above the ground.
- The racks are fixed to the ground, ceiling and among each other by means of rack mount kits.
- All the hardware in the racks are fixed by means of screws and cable ties.
- The hardware are kept away from the windows, especially on the higher floors above the ground floor.

Although computer systems are not likely to explode, there is the possibility that the buildings where these systems are located, specially the buildings where gas and combustible components are stored may explode. Storing the hardware in special steel cases or constructions may be considered against the explosion possibility.

The location of the system room is selected in the way that it is away from the stations which may be center of explosion. The backups are stored in cases resistant to explosion and earthquake or other safe places outside the organization. Business continuity is ensured by keeping the system backups at different locations and establishing alternative mirroring methods at different servers or disaster recovery centers.

9. CONDITIONS FOR DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Despite the fact that our Company processes personal data in compliance with the provisions set forth in Article 138 of Turkish Penal Code and Article 7 of the Law, if the causes which require the processing of the personal data cease to exist, such personal data shall be deleted, destroyed or anonymized upon the decision of our Company or the request of the data subject.

9.1. OBLIGATION TO DELETE, DESTROY AND ANONYMIZE PERSONAL DATA

Despite the fact that our Company processes personal data in compliance with the provisions set forth in Article 138 of Turkish Penal Code and Article 7 of the Law, if the causes which require the processing of the personal data cease to exist, such personal data shall be deleted, destroyed or anonymized upon the decision of our Company or the request of the data subject. Within this scope, our Company fulfills its relevant obligations through the methods explained in this section.

9.2. METHODS FOR DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Recording Media: The personal data of the Data controllers and Data subjects to whom we provide services are stored in the media listed in the below table, in compliance with the applicable legislation, in particular the provisions of the Law on Protection of Personal Data, and the international data security principles.

Electronic Media

- Firewalls
- DHCP
- DC
- File Server
- SQL Server1
- SQL Server2
- Application Server1
- Application Server2
- Application Server3
- Application Server4
- Application Server5
- Storage Server
- TFS Server
- Terminal Server
- Web Application Server1
- Web Application Server2
- Web Application Server3 (SOLLinux)
- WSUS
- MAIN Server
- Replicate Server1
- Replicate Server2

Physical Media

- Unit Cabinet
- System Room

- Archive Rooms
- Archive Provider Companies

Softwares

- Informasoft
- Bordromat
- Logo
- Delta
- Systems of Global Partners
- X2
- Luca
- Microsoft Office Environments

9.2.1. Deletion of Personal Data

If the causes which require the processing of the personal data cease to exist, such personal data may be deleted, destroyed or anonymized upon the decision of our Company or the request of the data subject. The deletion and destruction techniques commonly used by our Company are listed below:

Retention of data by our Company's employees in the portable media belonging to the Company is prohibited and this issue is followed by the policies and procedures.

Various advanced crypto and blocking (software) techniques are used against the stealing of portable media.

(i) Physical Deletion

Personal data may be processed by non-automatic means provided that it is a part of data recording system. In this context, various methods can be determined depending on the type of the data. Generally, methods such as cutting out the relevant data physically from the document, removing it from the file and making it invisible in an illegible way by using indelible ink can be used.

(ii) Secure Deletion Software

When the data processed fully or partially by automatic and non-automatic means and retained in the digital media are deleted/ destructed; methods that ensure unrecoverable deletion of the data from the software are used.

Deleting personal data on cloud systems; removing, restricting access authorizations of the relevant users to the file in the central server or the directory where the file is located; deleting the relevant lines in the databases together with the database inquiries; or deleting the data on portable media by means of suitable software are regarded within this scope.

However, if the deletion of the personal data may cause inaccessibility of the data in the system and unavailability of these data, provided that below conditions are provided, the personal data shall be deemed to be deleted if they are archived after they become unconnected with the related person.

− Being inaccessible by or unavailable to any other organization, institution or person

− Taking any and all technical and administrative measures to ensure that personal data are accessed only by our company and associated authorized people.

(iii) Sending to a Specialist for Secure Deletion

In some cases, our Company may cooperate with a specialist to delete the personal data on behalf of the Company. In such case, the personal data are deleted/ destroyed in a secure way, making the recovery impossible.

9.2.2. Destruction of Personal data

One or more of the below techniques can be used if destruction of personal data is required.

Degaussing: It is a method where magnetic media is passed through special devices where it is exposed to high magnetic fields to distort the data in them in an undecipherable way. The process which is generally referred to as Degaussing is distorting the unwanted data in the data recording media. If the destruction by this method fails, then the destruction will be completed by destroying the media physically.

Physical Destruction:

Some data may be printed on papers (Such as Personnel Affairs files) When these data are deleted/ destroyed, the personal data are destroyed physically, so that it cannot be used thereafter. In this context, various methods can be determined depending on the type of the data. Generally, methods such as cutting out the relevant data physically from the document, removing it from the file and shredding it in an unrecoverable and illegible manner can be used.

When magnetic data media are destroyed by means of chemical transactions and hard-disk breakers and cutters, the directives in the equipment and media policies shall be utilized.

Overwriting: Overwriting is a data destruction method which makes legibility and recovery of the former data impossible by writing random data constituting of at least seven 0’s and 1’s on the magnetic media and rewritable optic media by means of special software.

9.2.3. Techniques for Anonymization of the Personal Data

Anonymization of personal data is to render it impossible for personal data to be associated in any manner with a real person who is identified or identifiable, even if they are matched with other data. Our Company may anonymize the personal data when the causes which require the processing of the lawfully processed personal data cease to exist.

In accordance with Article 28 of the Law and the Regulation; the anonymized personal data may be processed for purposes such as research, planning, statistics. This type of processing is outside the scope of the Law and the Regulation and the explicit consent of the data subject shall not be sought. In consideration with the fact that the as the processing of anonymized data will be outside the scope of the Law and the Regulation, the rights set forth in Section 10 of this Policy shall not be valid for these data.

Anonymization is to prevent identification of the relevant person by removing or changing all the direct and/ or identifiers in a dataset or to make it impossible for such data to be recognizable in a group or crowd in a way that it cannot be associated with any real person.

Any data which do not indicate to a specific person as a result of preventing or losing such characteristics

are deemed as anonymized data. In other words, while such data were identifying

a real person before anonymization, after this transaction it becomes impossible for such data to be associated with the real person and its connection with that person is broken.

The purpose of anonymization is to break the connection between the data and the person identified by such data. All the transactions for breaking the connection by means of either automatic or non-automatic techniques such as

grouping, masking, derivation, generalization, randomization, etc., applied to the record system where personal

data is retained are called anonymization. The data obtained as a result of applying these methods

should not identify a specific person.

Sample anonymization methods are demonstrated in the table below:

Method	Implementation
Anonymization Methods That Do not Create Value Irregularity	• Removing Variables • Removing Records • Local Suppression • Generalization • Top and Bottom Limit coding • Global Coding • Sampling
Anonymization Methods That Create Value Irregularity	• Micro-aggregation • Data Swapping • Adding Noise • Re-sampling
Statistical Methods That Strengthen Anonymization	• K-Anonymity • L-Diversity • T-Closeness

9.2.3.1. Anonymization Methods That Do not Create Value Irregularity

In anonymization methods that do not create irregular values, no amendments or addition, removals are made to the values of the data in the dataset, instead the rows and columns of the data scheme are changed completely. That way, the data are changed in general, but the values in the relevant fields maintain their original form. Some of the anonymization methods that do not create irregular values are illustrated below.

a) Removing Variables

It is an anonymization method by removing one or more variables from the table by deleting them completely. In such case, the entire column in the table shall be removed. This method can be used when the variable is highly identifying, there is no better solution, the variable is too sensitive to be disclosed to public or irrelevant for the analytical purpose.

Age	Gender	Postal Code	Income	Religion
20	F	SO17	20.000	Budist
38	M	SO18	22.000	Muslim
29	M	SO16	32.000	Christian
31	F	SO17	31.000	Muslim
44	F	SO15	68.000	Jewish
78	M	SO14	28.000	Jewish

Example of removing variables

b) Removing Records

In this method, the anonymization is strengthened by removing a line which contains singularity and the possibility to generate assumptions regarding to the dataset is decreased. Generally the removed records are those which do not have a common value with other records and could be easily identifiable by people who are familiar with the dataset.

For instance, in a data set which contains organization – Department– division results, only one person is included from any sector to the survey. In such a case, it may be preferred to remove the records of this person instead of "sector" variable from the whole survey results.

Age	Gender	Place of Birth	Department	Department
31	F	Istanbul	Accounting	General
31	M	Istanbul	Accounting	General
31	M	Ankara	Sales	Retail
43	F	Ankara	Sales	Wholesale
51	M	Eskişehir	Finance	Collection

Example of removing records

c) Local Suppression

The purpose of local suppression method is to render the dataset more secure and reduce the identifiability risk. The combination formed by the values of a specific record creates a rare status and if such status would most probably make that person identifiable in the relevant group, the value that causes the exceptional status is changed as "unknown".

For instance, the below table shows the disability status in terms of age, gender and profession classification. In this table, age=54 forms an exceptional status and increases the risk of identifiability and making assumptions.

Age	Gender	Profession	Disability

			Status
27	F	Teacher	**N/A**
28	M	Architect	**N/A**
16	M	Teacher	**N/A**
30	F	Public Accountant	**N/A**
54	F	Engineer	**1st Degree**
52	F	Engineer	**Positive**

Local Suppression original dataset

Therefore, if the age and profession segment of the said record is changed to "unknown" by local suppression and a new status is obtained, then the identifiability risk of the dataset shall bee reduced.

Age	Gender	Profession	Disability Status
27	F	Teacher	**N/A**
28	M	Architect	**N/A**
16	M	Teacher	**N/A**
30	F	Public Accountant	**N/A**
Unknown	F	Unknown	**1st Degree**
52	F	Engineer	**Positive**

Distribution after local suppression

d) Generalization

It refers to the transaction of transforming the relevant personal data from a private value to a more general value. This is the most common method while generating cumulative reports and for the operations based on total numbers. The new values obtained as a result show the total values and statistics of a group which makes it impossible to reach to a real person.

For example, a person with Turkish ID No. 12345678901 lives in the European side and works at the work place in the Asian side of Istanbul. By using generalization method in the anonymization transaction, a result revealing that "In the Human resources Platform, xx% of the employees who live in the European side work at the work place in the Asian side" can be reached.

e) Top and Bottom Limit coding

Top and Bottom Limit coding method is obtained by defining a category for a certain variable and combining the values that remain in the grouping created by this category. Generally the lowest and highest values of a variable are brought together and proceeded by making a new definition for these values.

In the following example Table 1 shows the original data set, whereas Table 2 shows the re-designed and anonymized forms of the variables upon top and bottom limit coding.

Age	Gender	Profession	Annual Gross Salary	Province	Expenses (Monthly)
3*	F	Engineer	92,000	Istanbul	**8,000**
4*	M	Architect	110,000	Istanbul	**9,600**
4*	M	Doctor	149,000	Istanbul	**10,000**
5*	F	Doctor	123,000	Ankara	**10,800**
5*	M	Doctor	125,000	Ankara	**11,100**
2*	M	Pharmacist	85,000	Ankara	**16,300**

Table 1 top and bottom limit coding original dataset

The values of Income and Expense (Monthly) variables in the Table are changed as below by applying top and bottom limit coding method;

Income (Annual): Low = values lower than or equal to 100,000; Medium = values between 100,000 and 120,000; High = values higher than or equal to 120,000,

Expenses (Monthly): Low = values lower than or equal to 10,000;

Medium = Values between 10,000 and 11,000; High = values higher than or equal to 11,000,

The table anonymized according to these coding shall become as below:

Age	Gender	Profession	Annual Gross Salary	Province	Expenses (Monthly)
3*	F	Engineer	Low	Istanbul	**Low**
4*	M	Architect	Middle	Istanbul	**Low**
4*	M	Doctor	High	Istanbul	**Middle**
5*	F	Doctor	High	Ankara	**Middle**
5*	M	Doctor	High	Ankara	**High**
2*	M	Pharmacist	Low	Ankara	**High**

Table 2 dataset anonymized after top and bottom limit coding

f) Global Coding

Global coding is a grouping method used for datasets to which bottom and top coding can not be applied or which don’t include numeric values or has values which cannot be listed numerically. Generally it is used where certain values are grouped to facilitate making predictions and assumptions. A common and new group is formed for the selected values and all the records in the data set are replaced with this new definition.

In the below example, Table 1 show the original dataset, whereas Table 2 shows the anonymized dataset after applying global coding.

Gender	Profession	District	Civil Status
F	Architect	Çankaya	**Married**

F	Engineer	Çankaya	**Single**
F	Architect	Çankaya	**Divorced**
F	Architect	Çankaya	**Single**
F	Engineer	Çankaya	**Single**
F	Engineer	Çankaya	**Divorced**
F	Engineer	Çankaya	**Married**

Table 1 Global coding original dataset

In this dataset, as a conglomeration is seen in two categories of the profession variable of the data regarding to the women population in a single district, a single category can be obtained by merging the subjected two categories and in this way the data can be made more secure.

Gender	Profession	District	Civil Status
F	Architect or Engineer	Çankaya	**Married**
F	Architect or Engineer	Çankaya	**Single**
F	Architect or Engineer	Çankaya	**Divorced**
F	Architect or Engineer	Çankaya	**Single**
F	Architect or Engineer	Çankaya	**Single**
F	Architect or Engineer	Çankaya	**Divorced**
F	Architect or Engineer	Çankaya	**Married**

Table 2 Dataset where the profession field is anonymized after global coding

g) Sampling

In sampling method, instead of the whole dataset, a subset taken from the dataset is disclosed and shared. In this way, as it is not known whether a person, who is known to be within the whole dataset, takes place in the disclosed or shared sample subset, the risk of making accurate predictions on the persons is decreased. Simple statistics methods are used in the determination of the subset to be used for sampling.

For example, if a dataset regarding to the demographics, professions and health conditions of women living in Istanbul is disclosed or shared after anonymization, it may be meaningful to scan and make predictions from the subjected dataset concerning a woman who is known to be living in Istanbul.

However, if the data is disclosed or shared after anonymization by leaving only the records of the women whose registered province is Istanbul and removing of those who are registered in other provinces, as an intruder who has accessed the data may not predict whether a woman, who is known to live in Istanbul, is registered in Istanbul or not, he/she will not be able to make accurate predictions about whether the information of the woman he/she knows takes place within such data.

9.2.3.2. Anonymization Methods That Create Value Irregularity

In discordance with the aforementioned methods, in methods that create value irregularity; the current values are altered and the values of the data set are distorted. In such case as the values of the records are changing, the benefit that is planned to be obtained from the dataset should be calculated accurately. Although the values in the data set is changing, it may still be possible to benefit from such data by protecting the overall statistics from being distorted.

Some of the anonymization methods that create irregular values are illustrated below.

a) Micro-aggregation

In this method, first all the records in the dataset are arranged in a meaningful order and then the whole set is divided into a certain number of subsets. Next, the average of the value concerning the determined variable in each subset is calculated and the value in the subset for that variable is replaced with the average value. In this way, the average value of that variable valid for the whole dataset will not change.

In Table 1 below, the records are divided into groups of three according to their proximities as per their values in the "Income" column and the groups are marked with color codes. The arithmetic average of the values in each group are calculated and all the records in the group are replaced with new values to prevent identification of the original value.

Age	Gender	Zip Code	Income
23	F	1556	**25,000**
37	F	1559	**28,000**
41	M	1559	**37,000**
25	F	1557	**49,000**
34	M	1558	**56,000**
48	M	1556	**60,000**

Table 1 Micro-aggregation original dataset

New value for Group 1 as a result of micro-aggregation: (25,000 + 28,000 + 37,000) / 3 = 30,000

New value for Group 2 as a result of micro-aggregation: (49,000 + 56,000 + 60,000) / 3 = 55,000

Age	Gender	Zip Code	Income
23	F	1556	**30,000**
37	F	1559	**30,000**
41	M	1559	**30,000**
25	F	1557	**55,000**
34	M	1558	**55,000**
48	M	1556	**55,000**

Table 2 Dataset obtained as a result of micro-aggregation

b) Data Swapping

Data swapping is altered records obtained by swapping values of a subset of variables between selected pairs of records. This method is used fundamentally for variables that can be categorized and the main idea is to transform the data base by swapping the values of the variables between the records of the individuals.

Age	Gender	Province	Income
21	F	Istanbul	20,000
24	F	Ankara	30,000
35	M	Izmir	30,000
36	F	Istanbul	25,000
45	M	Izmir	55,000
50	M	Izmir	15,000

Table 1 Data Swapping original dataset

Table 1 has the records that contain original values Table 2 contains the new dataset obtained as a result of data swapping. As it can be seen from the subjected table, the income information of the record which includes Age="24", Gender="F", Province="Ankara" and the income information of the record which includes Age="45", Gender="M", Province="İzmir" are swapped. In the same way, the income information of the record which includes Age="35", Gender="M", Province="İzmir" and the income information of the record which includes Age="50", Gender="M", Province="İzmir" are swapped and a new dataset is formed.

Age	Gender	Province	Income
21	F	Istanbul	25,000
24	F	Ankara	55,000
35	M	Izmir	15,000
36	F	Istanbul	20,000
45	M	Izmir	30,000
50	M	Izmir	30,000

Table 2 Dataset obtained as a result of data swapping

c) Adding Noise

In this method, additions and removals are applied to ensure a determined level of distortion of a selected variable. This method is used mostly for datasets which contain numerical values. Distortion is applied to each value to the same extent.

Age	Gender	Province	Income
21	F	Izmir	45,000
24	F	Ankara	20,000
35	M	Ankara	123,000
36	F	Ankara	18,000
45	M	Istanbul	75,000

50	M	Istanbul	**7,000**

Table 1 Adding Noise original dataset

In Table 1, -5.000 is applied to the values of each record for the income variable and the new variables in Table

2 are formed.

Age	Gender	Province	Income
21	F	Izmir	**40,000**
24	F	Ankara	**15,000**
35	M	Ankara	**118,000**
36	F	Ankara	**13,000**
45	M	Istanbul	**70,000**
50	M	Istanbul	**2,000**

Table 2 Dataset obtained as a result of adding noise

9.3. Statistical Methods That Strengthen Anonymization

As a result of bringing some values of anonymized datasets together in individual scenarios, the possibility to determine the identities of the people in the records or making assumptions concerning their personal data may emerge.

Because of this reason, the anonymization maybe strengthened by minimizing the individuality of the records within the dataset by applying various statistical methods to the anonymized datasets. The key objective of these methods is to minimize the risk of impairing the anonymization and maintain the benefit to be obtained from the data set at a certain level.

a) K-Anonymity

Identifiability of the persons or convenient prediction of information belonging to a certain person in the records of the anonymized data sets, in case of gathering of the indirect identifiers in accurate combinations has discredited the anonymization processes. Therefore, the datasets anonymized by means of various statistical methods had to be rendered more reliable.

K-anonymity has been developed to allow attribution of more than one person to certain areas in a dataset so as to prevent disclosure of people who demonstrate individual characteristics in certain combinations. If there are more than one records regarding to the combinations formed by gathering some of the variables in a dataset, the probability of identifying the persons that correspond to this combination becomes lower. For example; in Table 1 contains variables such as name-surname, date of birth, gender, school and zip code.

Name Surname	**School**	**Date of Birth Gender**		**Zip Code**
*	1983	M	3440*	**ITU**
*	1982	M	3440*	**METU**
*	1983	M	3440*	**METU**
*	1980	M	3440*	**METU**
*	1982	F	3440*	**Istanbul University**
*	1983	M	3440*	**Bursa Uludağ**
*	1983	M	3440*	**Yıldız University**
*	1980	F	3440*	**Bilgi University**
*	1983	M	3440*	**Bilgi University**

Table 1. K- Anonymity original dataset

Although the data has been anonymized by masking the values of name-surname and zip code variables, if there is only one record containing the same records whilst making such anonymization, it will be possible to identify the right person through that record. However if the records are multiplexed, then a certain level of diversity will be enabled in respect of the variables which may demonstrate singularity. For instance, in Table 1 as six different school diversity has been ensured for the 6 records including date of birth as 1983, gender as male and zip code starting with 3440, it is not possible to make predictions regarding to which one of these 6 schools belongs to a person whose date of birth is 1983, gender is male and zip code is starting with 3440.

Therefore, as in Table 2, if the records containing the same values of date of birth, gender and zip code given in the frame are disclosed or shared, it is not possible to make predictions regarding to which one of these 6 schools belongs to a person whose date of birth is 1983, gender is male and zip code is starting with 3440.

Name Surname	**School**	**Date of Birth Gender**		**Zip Code**
*	1980	F	3440*	**METU**
*	1982	M	3440*	**METU**
*	1980	F	3440*	**Bilgi University**
*	1982	M	3440*	**Istanbul University**
*	1983	M	3440*	**ITU**
*	1983	M	3440*	**METU**
*	1983	M	3440*	**Bursa Uludağ**

*	1983	M	3440*	**Yıldız University**
*	1983	M	3440*	**Bilgi University**

Table 2. K- Anonymity applied dataset

b) L-Diversity

L-Diversity method, developed on the basis of the studies carried out on the deficiencies of K-anonymity, takes into account the diversity formed by the sensitive variables corresponding to the sale variable combinations. In Table 1, although K-anonymity has been applied by providing the department of the employees of the company and withholding their name-surname or ID numbers, there is the possibility of making predictions as zip code, age and ethnicity information have been shared.

Zip Code	Age	Nationality	Department
13053	28	Russian	**Production**
13068	29	American	**Production**
13068	21	Chinese	**Accounting**
13053	23	American	**Accounting**
14853	50	British	**Foreign Trade**
14853	55	Russian	**Foreign Trade**
14850	47	American	**Foreign Trade**
14850	49	American	**Foreign Trade**
13053	31	American	**Quality Control**
13053	37	British	**Quality Control**
13068	36	Japanese	**Quality Control**
13068	35	American	**Quality Control**

Table 1. L-Diversity original dataset

Zip Code	Age	Nationality	Department
130**	< 30	*	**Production**
130**	< 30	*	**Production**
130**	< 30	*	**Accounting**
130**	< 30	*	**Accounting**
1485*	≥ 40	*	**Foreign Trade**
1485*	≥ 40	*	**Foreign Trade**
1485*	≥ 40	*	**Foreign Trade**
1485*	≥ 40	*	**Foreign Trade**
130**	3*	*	**Quality Control**
130**	3*	*	**Quality Control**

130**	3*	*	Quality Control
130**	3*	*	Quality Control

Table 2. K=4 Dataset obtained as a result of applying anonymization

As can be seen in Table 2, the information in Table 1 have been grouped in terms of the logic of masking (groups of 4 has been formed by masking zip code and age information) and primarily anonymity has been strengthened by K=4 anonymity method.

However, as can be seen from the table, at the end of the first transaction all "Department" values of the last 4 records have been grouped as "Foreign Trade". In such case it has been shared that everyone with a zip code starting with 130 and at the age of 30s are working at "Foreign Trade" department, regardless of their nationalities.

A user who has information on these two data may easily reach to a conclusion that someone that he/she knows that has these characteristics is working at foreign trade department. Because of this reason, the masking method should be used by paying attention to creating a certain diversity in each group.

In Table 3, groups have been formed in the way that K=4 in a dataset anonymized by grouping the data as below and at the same time diversity has been obtained in each group in the way that L=3 (i.e. By including at least 3 diverse department).

Anonymization has been done by including 4 records and 3 different department in each group. This transaction has strengthened the anonymization transaction and reduced the identifiability of the user with external information.

Zip Code	Age	Nationality	Department
1305*	≤ 40	*	Production
1305*	≤ 40	*	Production
1305*	≤ 40	*	Accounting
1305*	≤ 40	*	Accounting
1485*	> 40	*	Foreign Trade
1485*	> 40	*	Foreign Trade
1485*	> 40	*	Foreign Trade
1485*	> 40	*	Customs
1306*	≤ 40	*	Quality Control
1306*	≤ 40	*	Quality Control
1306*	≤ 40	*	Quality Control
1306*	≤ 40	*	Quality Control

Table 3. K=4 Anonymity and L=3 dataset obtained as a result of applying Diversity

c) T-Closeness

Although L-diversity method provides diversity in the personal data, as the subjected method does not involve content and sensitivity levels of the personal data, there may be circumstances where it cannot provide sufficient protection.

Anonymization process of personal data in such a way by calculating the closeness levels of the values among them and dividing them into sub classes according to these closeness levels is called T-Closeness.

In Table 1, although K-anonymity is ensured as K=3 and L-diversity is ensured as L=3 in terms of date of birth, gender and zip code areas, the department of a person who was born in 1970, residing at 3440* zip code and whose gender is male can be predicted in this group of departments which include Accounting, Finance, Quality, Logistics, Human Resources, Management.

Date of Birth	Gender	Postal Code	Department	Number of Employees
198*	M	3440*	Accounting	**80**
198*	M	3440*	Quality	**20**
198*	M	3440*	Finance	**70**
197*	M	3440*	Logistics	**10**
197*	M	3440*	Human Resources	**10**
197*	M	3440*	Management	**10**

Table 1. K=3 Anonymity and L=3 Diversity applied dataset

In order to reduce such predictability, as can be seen in Table 2, the groups subject to anonymization have been arranged in such a way that each group of 3 records (K=3) include at least 3 different (L=3) department types, whereas it has been ensured that not all 3 of these different departments are operational departments (based on the assumption that other sections are not operational) in order to reduce the predictions regarding to the employees in that group.

Date of Birth	Gender	Postal Code	Department	Number of Employees
≥ 1970	M	3440*	Accounting	**80**
≥ 1970	M	3440*	Quality	**20**
≥ 1970	M	3440*	Finance	**70**
1975 ≤ x ≤1985	M	3440*	Logistics	**10**
1975 ≤ x ≤1985	M	3440*	Human Resources	**10**
1975 ≤ x ≤1985	M	3440*	Management	**10**

Table 2. Dataset obtained as a result of T-Closeness

9.4 TITLES, DEPARTMENTS AND JOB DEFIITIONS OF THOSE WHO PLAY A PART IN THE PROCESSES OF SROTAGE AND DESTRUCTION OF PERSONAL DATA

Pursuant to Article 6, item (f) of the Regulation on the Deletion, Destruction or Anonymization of Personal Data, the authorization matrix which shows titles, units and job descriptions of those involved in the retention and destruction processes is given in ANNEX-1 attached to this Policy.

9.5 PERIODICAL DESTRUCTION TIMES OF PERSONAL DATA

The data controller deletes, destroys or anonymizes the personal data in the first periodical destruction process following the date on which the obligation to delete, destroy or anonymize personal data has become due.

Although this is the general rule, our Company achieves the necessary periodical destruction every six months.

9.6 RIGHTS OF THE DATA SUBJECTS; METHOG-DOLOGY FOR EXERCISING AND EVALUATING THESE RIGHTS

Our Company informs the data subjects about their rights pursuant to Article 10 of the Law and provides guidance to the data subjects on how to exercise such rights and our Company enforces any required channels, internal operation, administrative and technical arrangements in accordance with article 13 of the Law in order to assess the rights of data subjects and make required information to the data subjects.

10. RIGHTS OF THE DATA SUBJECT AND EXCERCISING OF THESE RIGHTS

10.1 Rights of the Data subject

Data subjects are entitled to:

(1) Learn whether or not personal data have been processed,

(2) Request information on the procedure, if personal data have been processed,

(3) Obtain information on the purpose of processing personal data and find out whether personal data has been used as fit for the purpose,

(4) Obtain information about the third persons to whom personal data were transferred domestically or abroad,

(5) If personal data have been processed in an incomplete and wrongful manner, to request remedy of the same, and to request that the third parties to whom personal data are transferred to are also informed about the transaction executed in this regard,

(6) In the case where, although they have been processed pursuant to the Law, Regulation and the relevant provisions, the reasons requiring them to be processed have ceased to exist, to request that the personal data are deleted or destroyed, and the third parties to whom personal data are transferred to are also informed about the transaction executed in this regard,

(7) Object to the occurrence of a result which is detrimental to the person concerned as a result of analyzing the processed data exclusively through automatic systems,

(8) Request compensation for damages in the case where damages are sustained as a result of the illegal processing of personal data.

10.2 Conditions in which Data Subjects cannot Exercise Their Rights

As the following cases are exempted from the scope of the Law pursuant to Article 28 of the Law, data subjects are not entitled to exercise their rights listed in Section 10.01 hereunder:

(1) Processing of personal data for the purposes such as research, planning, and statistics through anonymization by official statistics.

(2) Processing of personal data for the purposes of art, history, literature or science, or within the scope of freedom of expression, provided that national defense, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated or it does not constitute a crime.

(3) Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized for providing national defense, national security, public safety, public order or economic safety.

(4) Processing of personal data by judicial authorities and execution agencies with regard to investigation, prosecution, adjudication or execution procedures.

Pursuant to Article28/2 of the Law, data subjects are not entitled to exercise their rights listed in Section 10.1.1 hereunder, except for the right to request compensation in the following cases:

(1) Processing of personal data is necessary for prevention of crime or investigation of a crime.

(2) Processing of personal data revealed to the public by the data subject herself/himself.

(3) If processing of personal data is necessary for the performance of supervision or regulatory duties, or disciplinary investigation or prosecution by assigned and authorized public institutions and organizations and professional organizations with public institution status.

(4) Processing of personal data is necessary for the protection of economic and financial interests of the state related to budget, tax, and financial matters.

10.3 Exercising of the Rights by the Data Subject

Data subjects may submit their requests regarding to their rights listed under Article 10.01 of this section by sending the document signed originally or with the secure e-signature to the contact details provided at www.cottgroup.com.

Third parties cannot submit any claims on behalf of data subjects.

Submission of a claim by another person other than the data subject can only be possible by virtue of a special power of attorney given by the data subject to the applicant in this regard.

10.4 Data Subject's Complaint Right to the PDP Board

In case the application is rejected, replied insufficiently, or not replied in due time pursuant to Article 14 of the Law; the data subject may file a complaint with the PDP Board within thirty days following the date he/she learns the reply of our Company and in any event, within sixty days following the date of application Pursuant to Accordance with Article of the Law.

10.5 COMPANY'S RESPONDING TO APPLICATIONS

10.5.1. Company's Procedures and Time For Responding to Applications

If the data subjects submit their claims to our Company as per the procedure set forth under paragraph 10.1.3., our Company concludes the claim free of charge as soon as possible, at the latest within thirty days, depending on the nature of claim.

However, in case the process requires any additional cost, our Company shall charge the fee specified by the Personal Data Protection Board.

10.5.2. Information That Can Be Requested by our Company from the Data Subject Who Submitted a Claim

Our Company may request information from the persons who submitted a claim to confirm whether they are the data subject.

Our Company may ask questions to the data subject to clarify the issues included in their application.

10.5.3. Our Company's Right to Reject the Application of the Data Subject

Our Company may reject the application of the data subject in the following cases, by explaining the grounds of rejection:

(1) Processing of personal data for the purposes such as research, planning, and statistics through anonymization by official statistics.

(2) Processing of personal data for the purposes of art, history, literature or science, or within the scope of freedom of expression, provided that national defense, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated or it does not constitute a crime.

(3) Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized for providing national defense, national security, public safety, public order or economic safety.

(4) Processing of personal data by judicial authorities and execution agencies with regard to investigation, prosecution, adjudication or execution procedures.

(5) Processing of personal data is necessary for prevention of crime or investigation of a crime.

(6) Processing of personal data revealed to the public by the data subject herself/himself.

(7) If processing of personal data is necessary for the performance of supervision or regulatory duties, or disciplinary investigation or prosecution by assigned and authorized public institutions and organizations and professional organizations with public institution status.

(8) Processing of personal data is necessary for the protection of economic and financial interests of the state related to budget, tax, and financial matters.

(9) The claim of the data subject may hinder the rights and freedoms of other persons.

(10) The claims require disproportionate efforts.

(11) The requested information is available to public.

10.6 RELATIONSHIP OF COMPANY'S POLICY FOR PROTECTION AND PROCESSING OF PERSONAL DATA WITH OTHER POLICIES AND LEGAL COMPLIANCE

The fundamental policies issued by the company in respect of protection and processing of Personal Data, which are associated with the principals set forth by this Policy are listed below. By establishing the connection of these policies with other fundamental policies applied by the Company in order areas; harmonization is established between the processes carried out by the Company with similar purposes and different policy principles.

Some of the policies listed in the below table are for internal use only. The principles of the internal policies have been reflected to the Policies available to public in terms of their relevance and, therefore it is aimed to inform the relevant people and ensure transparency and accountability regarding to the processing of personal data carried out by the Company.

In case of any controversies or differences between this Policy and the provisions of the Law on Protection of Personal Data and other relevant legislations, provisions of the Law on Protection of Personal Data and other relevant legislations shall prevail.

This Policy issued by Boss Yönetişim Hizmetleri A.Ş. took effect on 29.12.2017.

In case of any amendments to the Policy, the date of effectiveness and the relevant articles of the Policy shall be updated accordingly. Update table is attached hereto.

RELEVANT POLICIES AND PROCEDURES		
Information Security System Booklet	PL.01 E - MAIL SECURITY POLICY	PL.02 PASSWORD SECURITY POLICY
PL.03 ANTI-VIRUS POLICY	PL.04 INTERNET ACCESS POLICY	PL.05 INFORMATION SYSTEMS BACK-UP POLICY
PL.06 WIRELESS COMMUNICATION POLICY	PL.07 IDENTITY VERIFICATION AND AUTHORIZATION POLICY	PL.08 PERSONNEL SAFETY POLICY
PL.09 REMOTE ACCESS POLICY	PL.10 CLEAN DESK AND CLEAN SCREEN POLICY	PL.11 VISITOR ACCEPTANCE POLICY
PL.12 PORTABLE	PL.13 CHANGE	PL.14 SERVER SECURITY

EQUIPMENT POLICY	MANAGEMENT POLICY	POLICY
PL.15 POLICY ON PROTECTION FROM MALICIOUS CODES AND ATTACKS	PL.16 POLICY ON THE DESTRUCTION OF PORTABLE MEDIUMS	PL.17 POLICY ON THE DISPOSAL OF EQUIPMENT
PL.18 NETWORK ACCESS POLICY	PL.19 INFORMATION AND SOFTWARE EXCHANGE POLICY	PL.20 ACCESS POLICY
PL.21 PHYSICAL SAFETY POLICY	PL.22 INTERNET USAGE POLICY	PL.23 LAPTOP USAGE POLICY
PL.24 POLICY ON THE REMOTE CONNECTION TO THE NETWORK	PL.25 THIRD PARTY SAFETY POLICY	PL.26 ASSET RESPONSIBILITY POLICY
PL.27 SOFTWARE DEVELOPMENT SECURITY POLICY	PL.28 POLICY ON THE PTORECTION AGAINST MALICIOUS SOFTWARES	PL.29 PRINTED MATERIALS AND DISTRIBUTION POLICY
PL.30 INFORMATION PROTECTION POLICY	PL.31 SAFETY AWARENESS POLICY	PL.32 ACCEPTABLE USAGE POLICY
PL.33 PASSWORD PROTECTION POLICY	PL.34 INFORMATION CLASSIFICATION AND LABELLING POLICY	P08 HUMAN RESOURCES PROCEDURE
P09 RISK MANAGEMENT PROCEDURE	P10 PROCEDURE FOR THE DETERMINATION OF MEASUREMENT AND CONTROL METHODS	P11 BUSINESS CONTINUITY AND EMERGENCY MANAGEMENT PROCEDURE
P12 UDER ACCOUNT MANAGEMENT PROCEDURE	P13 DEVICE AND MEDIA CONTROL PROCEDURE.	P14 E - MAIL SECURITY PROCEDURE
P15 CUSTOMER COMPLAINTS MANAGEMENT PROCEDURE	P16 DISCIPLINE PROCEDURE	P17 INCIDENT BREACH PROCEDURE
P18 EQUIPMENT TRACKING PROCEDURE	P19 SYSTEM ROOM USAGE PROCEDURE	P20 COMMUNICATION PROCEDURE
T1001 ANTI-VIRUS INSTRUCTIONS	T1002 VPN SECURITY INSTRUCTIONS	T1003 PATCH SECURITY INSTRUCTIONS
T101 Back-up Instructions	T1101 INFORMATION SECURITY TESTS APPLICATION INSTRUCTIONS	T1201 ACTIVE DIRECTORY SECURITY INSTRUCTIONS
T1301 UPLOADING AND INSTALLATION INSTRUCTIONS	T1901 SERVER MAINTENANCE INSTRUCTIONS	T801 CORPORATE CULTURE INSTRUCTIONS
T802_SALARY AND WORK ADVANCES INSTRUCTIONS	T803 LABOR BACK-UP INSTRUCTIONS	TL 2701_ SECURE DEVELOPMENT ENVIRONMENT INSTRUCTIONS
TL 2702_ SECURE SUSTEM ENGINEERING	DRP_DISASTER MANAGEMENT PLAN	DRP- SCENARIOS

INSTRUCTIONS		
F11.01- BUSINESS CONTINUITY AND EMERGENCY ACTION PLAN	F11.02-EMERGENCY GENERAL PROTECTION PLAN	F11.03 -CALLING LIST
F9.01-ASSET UNDERTAKING STATEMENT and ALLOTMENT OF INFORMATION SECURITY RESPONSIBILITIES	F9.02-RESIDUAL RISK APPROVAL	BUSINESS IMPACT ANALYSIS
AUTHORIZATION MATRICES		

ANNEX - 1

PERSONNEL TITLE, UNIT AND POSITION LIST

PERSONNEL/ CONSULTANT	**POSITION**	**RESPONSIBILITY**
Information Processing Manager	**Information Technologies Department** Implementation of personal data storage and destruction policy Development of deletion, destruction and anonymization techniques. Ensuring the availability of the necessary software and data storage media for the implementation of the policy.	Ensuring compliance with storage times of the processes within the scope of his/her duty and management of the destruction process of the personal data pursuant to periodical destruction time and developing, researching and improving the implementations in this regard.
Information Technologies Support Specialist	**Information Technologies Support** Implementation of personal data storage and destruction policy Performing deletion, destruction and anonymization techniques. Keeping necessary records Maintaining the systems ready and available in line with the policies	Ensuring compliance with storage times of the processes within the scope of his/her duty and carrying out the destruction processes of personal data pursuant to periodical destruction time. Reporting the records to the management regularly
Operation Managers	**Operation Department** Implementation of personal data storage and destruction policy Following-up of destruction times and ensuring destruction of the required records in coordination with Information Technologies	Ensuring compliance with storage times of the processes within the scope of his/her duty and following-up of and carrying out the destruction processes of personal data pursuant to periodical destruction time. Reporting the deficiencies and areas that require improvement to the management
Human Resources Manager	**Human Resources Department** Implementation of personal data storage and destruction policy Following-up of destruction times of the information, documents and certifications regarding to the personnel and ensuring	Ensuring compliance with storage times of the processes within the scope of his/her duty and following-up of and carrying out the destruction processes of personal data pursuant to periodical destruction time. Reporting the deficiencies

	destruction of the required records in coordination with Information Technologies	and areas that require improvement to the management. Maintaining a copy of the log records
Accounting Managers	**Accounting Department** Implementation of personal data storage and destruction policy Following-up of destruction times and ensuring destruction of the required records in coordination with Information Technologies	Ensuring compliance with storage times of the processes within the scope of his/her duty and following-up of and carrying out the destruction processes of personal data pursuant to periodical destruction time. Reporting the deficiencies and areas that require improvement to the management
Finance Managers	**Finance Department** Implementation of personal data storage and destruction policy Evaluation and management of the contracts with suppliers within the scope of the Law on Protection of Personal Data. Following-up of destruction times and ensuring destruction of the required records in coordination with Information Technologies	Ensuring compliance with storage times of the processes within the scope of his/her duty and following-up of and carrying out the destruction processes of personal data pursuant to periodical destruction time. Reporting the deficiencies and areas that require improvement to the management
Business Development and Customer Relations Managers and Consultants	**Customer Relations Department** Implementation of personal data storage and destruction policy Elucidation of the customers about the issue Ensuring that contracts and protocols are prepared within the scope of the Law on Protection of Personal Data Following-up of destruction times and ensuring destruction of the required records in coordination with Information Technologies	Ensuring compliance with storage times of the processes within the scope of his/her duty and following-up of and carrying out the destruction processes of personal data pursuant to periodical destruction time. Reporting the deficiencies and areas that require improvement to the management
Managing Partners	Implementation of personal data storage and destruction	Ensuring compliance with storage times of the

	policy	processes within the scope of his/her duty and management and inspection of the destruction processes of personal data pursuant to periodical destruction time. Following-up of the necessary investments and inventories in this regard Monitoring the logs
Attorney	Ensuring the update of the personal data storage and destruction policy within the scope of the Law on Protection of Personal Data	Information and consultancy on the legislation and practices. Preparation of the contracts

ANNEX - 2

The storage and destruction periods for the data processed by our Company are determined in the Personal Data Processing Inventory on the basis of transaction and process and the inventory is accessible at the link [------------------------------].

Transaction/ Term	Legal Duration of Data Storage	Destruction Period
Company Personnel Payroll Transactions and Payrolling	10 years after the end of business relationship	Within 180 days after the end of the storage period
All the payroll, personnel and service records of the employees of the customers	The subjected personal data shall be stored and processed for the duration of general legal liability period within the frame of Turkish Code of Obligations and other legislations and thereafter when all the conditions of personal data processing cease to exist pursuant to the Law no 6698 on Protection of Personal Data the Regulation On The Deletion, Destruction And Anonymization Of Personal Data and other legislation, the subjected data shall be deleted, destroyed or anonymized ex-officio or	Within 180 days after the end of the storage period
Customers’ records which constitute the basis for the work permit		Within 180 days after the end of the storage period

	upon the request of the data subject. Storage period is10 years.	
General Assembly Transactions	10 years	Within 180 days after the end of the storage period
Tenders/ starting a business/ ministries/ undersecretariats Document preparation process	10 years	Within 180 days after the end of the storage period
Retention of Personnel Records in the Active Directory and other systems	10 years after the end of business relationship	Within 180 days after the end of the storage period
Information regarding to Company's partners and board of directors	10 years	Within 180 days after the end of the storage period
Payments and similar Finance Transactions	10 years after the end of business relationship	Within 180 days after the end of the storage period
Training records	10 years after the end of business relationship	Within 180 days after the end of the storage period
Current account records of the Customers/ Suppliers	10 years after the end of business relationship	Within 180 days after the end of the storage period
Minutes of the Meetings	10 years after the end of business relationship	Within 180 days after the end of the storage period
Active Directory records and necessary Log records	10 years after the end of business relationship	Within 180 days after the end of the storage period
Camera and Surveillance Records	10 years after the end of business relationship	Within 180 days after the end of the storage period

ANNEX - 3

Company	Address	Tax Office	Tax Number	Trade Registry No	Mersis No
Boss Yönetişim Hizmetleri A.Ş. Management Office www.boss.com.tr	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	1800379183	555770	0180037918300011
İstanbul Uluslararası Denetim ve SMMM Ltd. Şti. www.istanbulcpa.com	Astoria Towers Kempinski Residences	Zincirlikuyu	4810544399	673098	0481054439900018

	Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye				
Netkey Bilişim Sistemleri San. Ve Tic. Ltd. Şti. www.netkeysoftware.com	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	6310446636	551045	0631044663600010
Pera Kariyer Çözümleri Danışmanlık Ltd. Şti. www.perakariyer.com	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	7390463365	596859	0739046336500017
UP İnsan Kaynakları Eğitim ve Yönetim Dan.Hiz.Tic.Ltd.Şti. www.upandlearn.com	Demircikara Mahallesi 1419 Sokak B Blok Apt. No:1 B/7 Muratpaşa / Antalya / Türkiye	Antalya Kurumlar	8930275247	745547	0893027524700018

EDI Global Danışmanlık Tercüme ve Çeviri Hiz. Ltd. Şti. www.ediglobal.com.tr	Astoria Towers Kempinski Residences Büyükdere Caddesi No:127 B Kule Kat:8 Esentepe / Şişli / İstanbul / Türkiye	Zincirlikuyu	4640563770	810405	0464056377000013
Ikon Informatics Consultancy Ltd	Sofia 1309, Vazrazhdane District, 70 Tzaribrodska Str, fl. 2, office 3	Bulgaristan	BG201052169	N/A	N/A