Personal Data Protection and Privacy Statement

Table of Contents

As SICPA TURKEY, we attach importance to the privacy and security of your personal data. In this context, we would like to inform you about how we process, use and protect the personal data we collect from our customers, suppliers, business partners, their employees and officials and all other third parties while conducting our business relationships.

All terms and expressions used in this statement shall refer to the meaning ascribed to them in the Personal Data Protection Law No.6698 ("Personal Data Protection Law ") and other legislation. The term "You" in this statement refers to you personally. The term personal data is used to include sensitive personal data. The meanings of the terms and abbreviations in the Policy are given in Appendix - Abbreviations.

Please note that if you do not accept the Policy, you should not communicate your personal data to us. If you choose not to provide us with your personal data, in some cases we cannot provide you with our services, respond to your requests or provide full functionality of our services.

We would like to remind you that it is your responsibility to ensure that the personal data you submit to our company is accurate, complete and up to date. Furthermore, if you share data of other people with us, it is your responsibility to collect such data in accordance with local legal requirements. In this case, it means that you have obtained all the necessary permissions from us to collect, process, use and disclose their information of the third party and our Company cannot be held responsible in this context.

ABOUT SICPA TURKEY

Established in 2007, our company SICPA TURKEY offers high-tech solutions on Trademark Security and Product Tracking Systems.

SICPA TURKEY offers technological services and solution packages that enable the prevention of unregistered, counterfeit and illegal products by developing tailor-made solutions for the monitoring of products in the supply chain and the separation of counterfeit-real products in terms of trademark and product security which are of great importance in our age.

In the statement, the term "we" or "Company" or "SICPA TURKEY" is used to refer to SICPA TURKEY Urun Guvenligi Sanayi Ve Ticaret A.S acting in Yayla Mah, D-100 Karayolu, Ruya Sok, No: 2, Tuzla/Istanbul registered under registration No.619621/0 in the Istanbul Trade Register.

OUR PRINCIPLES ON PERSONAL DATA PROCESSING

All personal data is processed by our Company in accordance with the Personal Data Protection Law and related legislation. Pursuant to Article 4 of K the Personal Data Protection Law, the basic principles that we take into consideration while processing your personal data are as follows:

- Data Processing in Accordance with Law and Good Faith rules: Our Company acts in accordance with the principles of legal regulations and general trust and good faith rules in the processing of personal data. In this context, our Company considers the proportionality requirements in the processing of personal data and does not use the personal data except for the purpose.
- **Ensuring that Personal Data is Accurate and Update:** it ensures that the personal data it processes are accurate and update by taking the basic rights of the personal data subjects and their legal interests into account.
- **Data Processing for Specific, Open and Legitimate Purposes:** Our Company clearly and accurately determines the purpose of processing any legitimate and lawful personal data. Our

company is in connection with the products and services provided by it, and processes the personal data as necessary.

- **Processing the Personal Data In Connection With Purpose of Processing In A Limited and Reasonable Way:** Our Company processes personal data in a manner that is suitable for the realization of the specified purposes and avoids the processing of personal data which is not related to the achievement of the purpose or which is not needed.
- **Maintenance of Personal Data for the time required for the purpose foreseen in the relevant legislation or for the purpose for which it was processed:** Our Company maintains personal data only for the period specified in the relevant legislation or for the purpose for which it was processed. In this context, our Company first determines whether or not a period is stipulated for the storage of personal data in the relevant legislation, if a period is determined, it acts in accordance with this period and if it is not determined, it stores the personal data for the period required for the purpose for which they are processed. In the event that the reasons requiring expiration or elimination of the time expire, personal data is deleted, destroyed or made anonymous by our Company.

DATA SUBJECT CATEGORIES

The categories of data subjects other than employees (including interns and subcontractor employees) whose personal data are processed by our company are listed in the table below. A separate policy regarding the processing of personal data of our employees has been established and implemented within the company. Persons who fall outside the following categories may also submit requests to our Company within the scope of the Personal Data Protection Law, and their requests will also be considered under the Policy.

RELATED PERSON AND HIS/HER CATEGORY	DESCRIPTION
Customer	Judicial entities, whose receive any services from SICPA TURKEY.
Potential Customer	Real or legal persons who have requested or are interested in using our services or have been evaluated in accordance with the practices and good faith rules that they may have interest.
Visitor	Real persons who have entered the physical facilities owned or organized by our Company for various purposes or who have visited our websites.
Third Person	Third party real persons (e.g., guarantors, companions, family members and relatives) having relationship with such persons in order to ensure the security of business transactions between our Company and the above-mentioned parties or to protect the rights and benefits of the persons mentioned above, or all real persons, whose personal data have to be processed by our Company for a particular purpose, even if it is not stated clearly under the Policy.
Employer Candidate	Real persons, who have applied for a job in any way or have submitted their resumes and relevant information to our Company for review.
Employee of the Group Company	Employees and representatives of the SICPA group companies located abroad.

Employees, Shareholders and Officers of the Organizations That We Cooperate	Real persons, including the shareholders and officers of those institutions, who work in the organizations having all kinds of business relationships (including, but not limited to, business partners, suppliers, etc.)

WHEN DO WE COLLECT PERSONAL DATA ABOUT YOU?

We collect your personal data mainly:

- When you buy or use our services (Museum Card, Museum Pass, e-ticket, etc.);
- When you sell goods or provide us with services;
- When you subscribe to our newsletters and choose to receive our marketing messages;
- When you contact us via our website, e-mail, social media platforms, other online media or telephone;
- When you apply for a job;
- When you join our company events and organizations;
- Indirectly, for example, by using a "cookie" and personalizing the software used to make the website tailored to your specific preferences, or by monitoring certain pages of the site (e.g. your IP address) or other technical means that allow us to monitor your use of the site; and
- When you contact us for any purpose as a potential customer/supplier/business partner/subcontractor.

We will only process personal data that we obtain in the above cases in accordance with this Policy.

WHAT PERSONAL DATA DO YOU PROCESS ABOUT YOU?

The personal data that we process about you depends on the type of business relationship between us (e.g. customer, supplier, business partner, etc.) and the way that you contact us (e.g. via phone, e-mail, website, printed documents, etc.).

Basically, our methods of processing personal data enable any circumstances, where you join our business activities, competitions, promotions and surveys or to contact us in any way, when you apply for Museum Card, Museum Pass or e-ticket via our website, or by phone or email, or via the specific electronic application for our customers. In this context, the personal data processed by us about you is described under the following categories:

Data categories	**Examples**
Identity information:	Information in identity documents such as title, gender, date of birth, etc.
Contact information:	Email, phone number and address.
Login information of the account:	Login ID, password and other security codes.
Photos and/or videos, which will indicate your ID:	Photo and video images and audio data processed when you visit our company for security reasons or when you participate in events organized by our Company, and visual data processed by CCTV records when you visit our company facilities.
Financial data:	Credit card data, bank account data and billing information.

Any other information you voluntarily decide to share with SICPA TURKEY:	Any personal data that you share at your own discretion, and any feedbacks, opinions, requests and complaints, evaluations, comments and related evaluations, uploaded files, interests, and detailed information that you submit to us at your own discretion via personal data, social media, online platforms or other media, and any information provided our detailed review process before we establish a business relationship with you.
Electronic data collected automatically	When you visit or use our website or applications, subscribe to our newsletters, and contact us by other electronic means,, we may collect electronic data sent to us by your computer, mobile phone or other access device (e.g. device hardware model, IP address, operating system version and settings, your time and duration of using our digital channel or product, your actual location, links you clicked, motion sensor data, etc. that can be collected when you activate location-based products or features).
Legal proceedings and compliance information:	Your personal data, audit and inspection data processed within the scope of determination of legal receivables and rights, follow-up and execution of our debts and compliance with our legal obligations and policies of our Company
Data of corporate customer/supplier:	As a result of the operations carried out by our business units within the scope of our services, the information obtained and produced about the data subjects such as employees/signatories, employees or signatories within the body of the customer/supplier.
Event management and security information:	Information and evaluations about the events that have the potential to affect our company's employees, managers or shareholders, vehicle license plate and vehicle information, and organization of airport transportation and transfer.
Personal data collected from other resources:	To the extent permitted by applicable laws and regulations, we may also collect your personal data through public databases, social media platforms, and methods and platforms through which our business partners collect personal data on our behalf. For example, before establishing business relationships with you, we may conduct research on publicly available sources to ensure the technical, administrative and legal security of our business activities and transactions. It may also be possible for you to transmit some personal data from third parties to you (e.g. personal data of guarantor, companion, family members, etc.). In order to manage our technical and administrative risks, we may process your personal data through methods that are generally accepted in these areas in accordance with generally accepted legal, commercial, and good faith.

PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDING

The security cameras are used to secure the security of our company and facilities and personal data are processed in this way. Within the scope of monitoring with security camera; to improve the quality

of the service provided, to ensure the safety of life and property of the company's physical campuses and people in the company, to prevent abuses, to protect the legitimate interests of data subjects.

Personal data processing activities carried out by our company with security cameras are carried out in accordance with the Constitution, Personal Data Protection Law and the relevant legislation.

Pursuant to article 4 of the Personal Protection Law, our company processes the personal data in a limited and reasonable way in connection with the purpose for which they are processed. It is not subject to monitoring the privacy of the person in a way that may result in interference that exceeds the security objectives. In this context, the warning signs are placed in the common areas, where CCTV recording is made and the data subjects are informed. However, due to the legal interests of our Company in keeping CCTV records, their express consent is not obtained. Furthermore, any technical and administrative measures are taken in accordance with article 12 of the Personal Protection Law to ensure the security of personal data obtained as a result of CCTV monitoring.

Moreover, a procedure has been prepared for areas with CCTV cameras, monitoring areas of cameras, and record retention periods and has been put into practice in our Company.

This procedure is taken into consideration before the CCTV camera is placed and the camera is then placed. It is not permitted to install cameras that exceed the safety purpose and exceed the privacy of persons. Only a certain number of employees of the Company have access to CCTV camera images and these authorizations are reviewed regularly. Personnel with access to these records sign a commitment to protect personal data in accordance with the law.

FOR WHICH PURPOSES DO YOU USE YOUR PERSONAL DATA?

The purpose of using your personal data varies depending on the type of business relationship between us (eg customer, supplier, business partner, etc.). The following are basically our purposes for processing your personal data. Personal data processing activities related to the Candidates are explained in the above section "Processing of Personal Data of Employee Candidates."

Our Purpose of Processing Any Personal Data	**Examples**
Assessment of the potential suppliers/ business partners	Conducting our review and conflict of interest process in accordance with our risk rules.
Establishment and management of customer relations	Realization of the sales transactions of the services and products offered by our company, and submission of our offers for services.
Management and conclusion of the contract process between us and our suppliers/business partners	Procurement of goods and services, invoicing, management of the processes executed through our website applications, preparation and execution of the contracts, ensuring any legal transaction security after the contract, management of the logistics processes, compensation, improvement, development and diversification of our products and services, submission of alternatives to the judicial/real entities, which whom our Company is in commercial relations, development products and services, evaluating new technologies and applications,

	determination and implementation of the commercial and business strategies of our Company, management of the operations (demand, proposal, evaluation, order, budgeting, contract), and management of product/project/manufacturing/investment quality processes and operations, in-house system and application management operations, financial operations and financial affairs.
Management of the direct marketing processes	Making marketing notifications regarding our services by email and telephone, conducting any satisfaction surveys or providing any suitable services for your likes in the following process by taking your opinions and comments on social media, online platforms or other media into consideration, informing our customers about our innovations, campaigns and promotions, conducting campaign activities, designing any special promotional activities for customer profiles and conducting advertising, promotion and marketing activities to be created through customer "classification" and personal information to prevent unwanted email messages, and proposing to you our services according to your liking, usage habits and needs, and determining and implementing any commercial and business strategies.
Communication and support (upon your request)	Responding to any requests for information about our services, providing any support for requests received through our communication channels, and updating our records and database.
Performance of legal obligations	Execution of tax and insurance processes, performance of our legal obligations under the relevant legislation and especially Law No.5651 and other legislation, Law No.6563 on the Regulation of Electronic Commerce and other legislation, the Turkish Penal Law No.5237 and the Personal Data Protection Law No.6698, performance of the legal obligations under the relevant legislation, management of the processes in the official institutions, compliance and audit of the obligation of keeping record and information, audit and inspection of the official authorities, follow-up and conclusion of our legal rights and lawsuits, and performance of the necessary processes in accordance with the laws and regulations that we are subject to such as data disclosure upon request of the official authorities.
Protection of benefits of the company and provision of security	Performance of any necessary inspection activities within the scope of the determined requirements and obligations in order to ensure performance of the legal obligations specified in the Personal Data Protection Law as required or rendered compulsory by the legal regulations, conducting the conflict of interest controls, ensuring the legal and commercial security of the persons who are in business relationship with our company, keeping the CCTV records for the protection of the company devices and assets, taking the technical and administrative security measures, conducting the satisfaction surveys after our services, to carry out the necessary works for the development of the services we provide, implementation and supervision of workplace rules, management of quality processes, planning and execution of social responsibility activities, protection

	of the commercial reputation of the SICPA Group, the occurrence of all incidents, accidents, complaints, lost and stolen events. reporting the conditions, taking necessary precautions and taking precautions, transferring the rules to be followed for the dangerous situations that may occur during the maintenance and repair and measuring the professional competencies of the subcontractors, ensuring the order of the entry and exit of the company employees and obtaining the necessary information in terms of security and quality, performance of reporting and other obligations determined by laws and regulations.
Design and implementation of the commercial activities of the Company	Communication, market research and social responsibility activities carried out by our company for purposes of budgeting, and determining, planning and implementing the commercial policies of the Company in the short, medium and long term, and of determining and implementing commercial and business strategies of the Company.
Reporting and audit	Establishing communication with the SICPA group companies located abroad, and carrying out necessary activities, internal audit and reporting processes.
Protection of the rights and benefits	Defense against legal claims such as lawsuits filed against our company, investigations, etc.

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING?

Because the marketing activities are not assessed in the scope of the exemptions arranged in article 5/2 of the Personal Data Protection Law, as a rule, we always obtain your consent to process your personal data within the scope of marketing activities. Our company may send you any promotional communications about products, services, events and promotions at regular intervals. Such promotional communications can be sent to you by different means such as email, phone, SMS text messages, mail and social networks of third parties.

To provide you with the best personalized experience, sometimes these communications can be adapted to your preferences (for example, as you talk us about them based on results from your website visits or links that you click on in our emails).

Upon you approval, we may carry out any marketing activities for purposes of processing any personal data such as internet advertising, Targeting, Re-targeting, cross-selling, campaign, opportunity and product/service advertisements for specific products and service for you, using the Cookies for this purpose, making your commercial offers by considering your preferences and recent purchases, and furthermore, monitoring your usage habits according to your previous records during your visit to web applications and providing any specific products for you, submitting any specific advertising, campaigns, advantages and other benefits for you especially for sales and marketing activities, performing other marketing and CRM activities, creating new products and services, forwarding any electronic commercial messages (campaign, newsletter, customer satisfaction surveys, product and service ads), sending gifts and promotions, and organizing and keeping informed about corporate communication and other activities and invitations within this scope.

When the applicable legislation requires, we will ask for your consent before we start the above activities. You will also be given the opportunity to revoke (stop) your consent at any time. In

particular, you can always stop sending marketing notifications to you by following the unsubscribe instruction in each email and SMS message.

If you log in a SICPA TURKEY account, you may be given the option to change your communication preferences under the relevant section of our website or application. You can always contact us to stop sending marketing communications to you (you can find the contact details below in the above section "What Are Your Rights to Your Personal Data?").

FOR WHICH LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data for the following legal reasons under article 5 of the Personal Data Protection Law and especially the Turkish Commercial Law No.6102, Turkish Law of Obligations No. 6098, Tax Procedure Law No. 213, and the electronic commerce legislation:

Legal Reasons	**Examples**
We process your personal data by obtaining your express consent pursuant to the Personal Data Protection Law and other legislations in any circumstances that require your express consent (in this case, we would like to remind that you may withdraw your consent at your desired time).	We obtain your consent to carry out our marketing activities.
In any circumstances allowed under the current legislation	Name of the relevant person must be written on the invoice under article 230 of the Tax Procedural Law.
Where it is compulsory to protect the vital benefits of any person	Provision of the medical information of the member of the Board of Directors, who feel faint, to a physician.
Where we enter into and perform the contract with you and perform our obligation under a contract	The identity information of the customer is obtained under a contract with the customer.
Where we perform our legal obligations	We perform our legal obligations and submit any information required by the decree to the court.
If your personal data is made public by you	You must send us an email message, enter the contact information of the employee candidate to the website containing the job applications and use your personal information made public by means such as social media, etc. to contact you.
When we must process any data to create or protect any right, exercise our legal rights and defend against any legal claims made against us.	Protection and when necessary, use of the documents having a nature of proof/evidence.

Where our legitimate benefits require, provided that they never harm any basic rights and remedies	Provision of security of our company networks and information, performance of our company activities, determination of any suspicious procedures and checking if the procedures comply with our risk rules, and utilizing any storage, accommodation, maintenance and support services for purpose of providing the IT services in technical and security aspects.

We would like to emphasize that, if your Personal Data is processed upon your express consent, and you withdraw your consent, you will be removed from the commercial membership program, where such data processing based on an express consent is required, and you will not be able to benefit from the advantages that you receive through such transactions as of the respective date.

WHEN DO WE SHARE YOUR PERSONAL DATA?

Domestic Data Transfer

Our Company is responsible for acting in accordance with the decisions and related regulations as prescribed in the Personal Data Protection Law and made by the Committee on transfer of personal data. As a rule, our Company cannot transfer any personal data and special data of the data subjects to other real persons or legal entities without the express consent of the related person. However, in any circumstances, where it is required by the Personal Data Protection Law and other Laws, the data may be transferred to the authorized administrative or judicial authority or organization without the express consent of the related person as prescribed by the legislation and within limits specified in the legislation.

Furthermore, in any circumstances stipulated in Articles 5 and 6 of the Personal Data Protection Law, it is possible to transfer the personal without the consent of the related person. Our company may transfer the personal data to any third persons in accordance with the conditions set forth in the Personal Data Protection Law and other relevant legislation and by taking all safety precautions specified in the legislation, it is specified otherwise in such agreement if there is an agreement entered into between us and data subject, or in the said contract and in the law or other relevant legislation.

International Transfer of Personal Data

Our company may transfer any personal data to any third parties in Turkey and process and store it in Turkey or outside Turkey and transfer it to abroad including outsourcing in accordance with the conditions set forth in the Personal Data Protection Law and other relevant legislation and by taking all safety precautions specified in the legislation, it is specified otherwise in such agreement if there is an agreement entered into between us and data subject, or in the said contract and in the law or other relevant legislation.

As a result, we seek the express consent of the data subjects pursuant to article 9 of the Personal Data Protection Law to transfer any personal data to abroad. However, it is prescribed that any personal data may be transferred to abroad without seeking the express consent of the data subject, provided that one of the provisions specified in article 9 and article 5/2 or article 6/3 of the Personal Data Protection Law is available and

a) Adequate protection is available in a foreign country, to which the personal data will be transferred; or

b) In absence of adequate protection, the data controllers in Turkey and in the relevant foreign country undertake the adequate protection in written and the consent of the Committee is available.

Accordingly, in the exceptional cases where the express consent is not sought for the transfer of the personal data mentioned above, in addition to the conditions of unauthorized processing and transfer, the Company is required to have adequate protection in accordance with the Personal Data Protection Law. The Personal Data Protection Committee will determine whether adequate protection is provided. In the case of the absence of adequate protection, the data controllers in Turkey and in the relevant foreign country undertake the adequate protection in written and the consent of the Committee is available.

We will share your personal data only for the following purposes. Except in these cases, we pay a special attention not to share your personal data. The parties, with whom we share the personal data, are as follows:

- **Service providers and business partners:** They include the parties, with whom our Company establishes business partnerships for the purposes of sales, promotion and marketing of our Company's services, after-sales support, while we carry out any commercial activities of our Company. Just like many businesses, we can also work with the reliable third parties such as information and communication technology providers, consultancy service providers, cargo companies and travel agencies to conduct any functions and services in the most efficient manner and in accordance with current technologies within the scope of some data processing activities. In this context, we may share any data to carry out our business activities. This sharing is limited in order to ensure the fulfillment of the objectives of establishing and performing the business partnership. The marketing service support company, with whom we share the data, may be established abroad. In this context, we share the data internationally in accordance with the provisions of articles 8 and 9 of the Personal Data Protection Law on international data sharing.

- **Official Authorities:** We share your personal data with the relevant governmental, judicial and administrative authorities, as required by law or when we need to protect our rights (e.g. tax authorities, law enforcement agencies, courts and enforcement offices).

- **Private judicial entities:** Pursuant to the provisions of the relevant legislation, any personal data may be shared under the legal powers of any private judicial entities, which are authorized to obtain any information and documents from our Company, for limited purposes (e.g. an Occupational Health and Safety Company).

- **Professional consultants:** We may share your personal data with any professional consultants such as banks, insurance companies, auditors, lawyers, financial advisers and other consultants.

- **Other persons in connection with corporate transactions:** We may share your personal data from time to time for purposes of carrying out any corporate procedures such as the sale, restructuring, merger, joint venture or other use of our business, assets or shares (including those related to any bankruptcy or similar process). We may share.

HOW LONG DO WE STORE YOUR PERSONAL DATA?

We store your personal data only for necessary period to fulfill the purpose for which it was collected. We set these periods separately for each business process and if we do not have any other reason to store your personal data at the end of the relevant period, we will destroy your personal data in accordance with the Personal Data Protection Law.

We consider the following criteria when we determine the destruction times of your personal data:

- Within the scope of the purpose of processing the relevant data category, the period of time accepted as a general practice in the industry where the data controller operates;
- The time required for the processing of personal data in the relevant data category and when the legal relationship established with the relevant person shall continue;
- The period in which the legitimate benefit obtained by the data controller shall be valid in accordance with the law and the good faith rules, depending on the purpose of the relevant data category being processed;
- The period in which the risks, costs and responsibilities that may arise from the storage of the relevant data category for the purpose of processing them shall continue legally;
- Whether the maximum period to be determined is appropriate to keep the relevant data category accurate and up-to-date when necessary;
- The period in which the data controller is obliged to keep personal data in the relevant data category due to his legal obligation; and
- The timeout set by the data controller to assert a right depending on a personal data in the relevant data category.

HOW DO WE DISPOSE YOUR PERSONAL DATA?

Although any personal data have been processed in accordance with the provisions of the relevant law, Article 138 of the Turkish Penal Code and Article 7 of the Personal Data Protection Law, if any reasons that require processing the personal are eliminated, it is deleted, destroyed or made anonymous at our Company's own discretion or if the personal data subject requires so.

In this context, the Personal Data Storage and Destruction Policy has been prepared. Our company reserves the right not to fulfill the request of the data subject, in cases where it has the right and/or obligation to maintain personal data in accordance with the relevant legislation. When the personal data is also processed in non-automated ways, provided that it is part of any data recording system, the system that destruct of the personal data physically in a way that cannot be subsequently used when data is deleted/destroyed is implemented. When our company agrees with a person or organization to process personal data on its behalf, the personal data is deleted securely by such person or organization so that it cannot be recovered. Our company is able to make personal data anonym when the reasons that require the processing of personal data processed in accordance with the law are eliminated.

TECHNIQUES OF DESTRUCTING THE PERSONAL DATA

Deletion of Personal Data

Although our company has been processed in accordance with the provisions of the relevant law, it may delete personal data at its own discretion or upon the request of the personal data subject in case the reasons requiring processing are eliminated. Deletion of personal data is the process of making personal data inaccessible and non-reusable by the relevant users. Our company takes all technical and administrative measures to ensure that the deleted personal data cannot be accessed and reused for the relevant users.

<u>Process of Deleting the Personal Data</u>

The process of deleting the personal data is as follows:

- Determination of the personal data that will be subject to deletion;
- Identification of the relevant users for each personal data by using the access authorization and control matrix or similar system;
- Determination of the authorizations of the relevant users and methods such access, retrieval and reuse; and
- Closing and eliminating the authorizations and methods of access, retrieval and reuse of the relevant users within the scope of personal data.

Method of Deleting the Personal Data

Data Recording Media	**Description**
Personal Data Available In the Servers	Among the personal data available in the servers, for ones, which require storage and which period expires, the access authorization of the relevant users is cancelled by the system administer and the deletion operation is conducted.
Personal Data Available In the Electronic Media	Among the personal data available in the electronic media, ones, which require storage and which period expires, may never be accessed and reused by other employees (relevant users) except the database administrator.
Personal Data Available In the Physical Media	Among the personal data stored in the physical media, ones, which require storage and which period expires, may never be accessed and reused by other employees except the department manager responsible for document archive. Furthermore, it is stroke out/dyed/deleted and the blackening operation is applied so that is cannot be read.
Personal Data Available In the Portable Media	Among the personal data stored in the Flash-basd storage media, ones, which require storage and which period expires, are encrypted by the system administrator and stored by the encoding keys in safe media by giving only the system administrator an access authorization.
Personal Data Available In the Physical Media	Among the personal data stored in the physical media, ones, which require storage and which period expires, may never be accessed and reused by other employees except the department manager responsible for document archive. Furthermore, it is stroke out/dyed/deleted and the blackening operation is applied so that is cannot be read.
Personal Data Available In the Optic/ Media	Among the personal data stored in the Flash-based storage media, ones, which require storage and which period expires, are encrypted by the system administrator and stored by the encoding keys in safe media by giving only the system administrator an access authorization.

Since personal data can be stored on a variety of media, they must be erased in a manner appropriate to the media. Examples include:

As a Service, Application Type Cloud Solutions (such as Office 365 Salesforce, Dropbox, etc.): Data must be deleted in the cloud system by the delete command. Note that the relevant user is not authorized to retrieve deleted data on the cloud system, while performing the aforementioned operation.

Personal Data in Hardcopy: Any personal data in hardcopy should be deleted by using the blackening method. The blackening operation is performed by cutting the personal data on the relevant documents where possible and making them invisible to the relevant users by using fixed ink which is irreversible and not readable by technological solutions.

Office Files on the Central Server: The file must be deleted by the delete command in the operating system or the access rights of the relevant user on the directory where the file or file is located must be removed. It should be noted that the relevant user is not a system administrator at the same time.

Personal Data in Portable Media: Personal data in Flash-based storage media must be stored in encrypted form and deleted by using appropriate software.

Databases: The relevant rows containing personal data must be deleted by database commands (DELETE, etc.). It should be noted that the relevant user is not a database administrator at the same time.

Destruction of Personal Data

Although our company has been processed the personal data in accordance with the provisions of the relevant law, it may destroy it at its own discretion or upon the request of the personal data subject, where the reasons requiring processing the personal data are eliminated. Destruction of the personal data is the process, in which personal data cannot be accessed, retrieved or reused by anyone in any way. The data controller is obliged to take all necessary technical and administrative measures for the destruction of personal data.

Data Recording Media	**Description**
Personal Data Available In the Physical Media	Among the personal data stored in the physical media, ones, which require storage and which period expires, are destroyed in a shredder so that it cannot be recycled.
Personal Data Available In the Optic/ Media	Among the personal data stored in the optic media and magnetic media, ones, which require storage and which period expires, are melted, incinerated or pulverized and thus destroyed physically. Furthermore, the magnetic media is passed through a special device and exposed to a high magnetic field, making the data on it unreadable.

Physical Destruction: The personal data can be processed in non-automated ways, provided that it is part of any data recording system. While such data is deleted/destroyed, a system, which destroys the personal data physically so that it cannot be reused afterwards, is implemented.

Secure Deletion from the Software: While any data processed in fully or partially automated ways and stored in digital media is deleted/destroyed, the methods, which deleting the data from the related software so that it cannot be recovered, are used.

Secure Deletion by A Specialist: In some cases, you can agree with a specialist to delete the personal data on your behalf. In this case, the personal data is deleted/destroyed securely by the person skilled in the art so that it cannot be recovered.

Blackening: It is a process, which makes any personal data physically unreadable.

Methods of Destruction of Personal Data

To destroy the personal data, all copies of the data must be identified and disposed of individually by using one or more of the following methods, depending on the type of systems where the data is found:

Local Systems: One or more of the following methods can be used to destroy data on these systems: i) De-magnetization: It is a process, in which the magnetic media is passed through a special device and exposed to a high magnetic field and the data on this device is destroyed so that it cannot be read. ii) Physical Destruction: It is a process, in which the optic media and magnetic media are melted, incinerated or pulverized and thus destroyed physically

physical destruction of optical and magnetic media such as melting, burning or dusting. Data is rendered inaccessible by processes such as melting, incinerating, pulverizing or passing the optical or magnetic media through a metal grinder. If rewriting or de-magnetization is not successful on the solid state disks, such media must also be destroyed physically. iii) Rewriting: It is a process, in which the recovery of old data is prevented by writing random data of 0 and 1 at least seven times on the magnetic media and rewritable optical media. This process is done by using a special software.

Environmental Systems: The destruction methods that can be used depending on the media type are as follows: i) Network devices (switches, routers, etc.): The storage media inside these devices are fixed. Products have often a delete command, but no destruction property. They must be destroyed by using one or more of the suitable methods specified in (a). ii) Flash-based media: the Flash-based media, which have ATA (SATA, PATA, etc.) and SCSI (SCSI Express, etc.) interfaces with the Flash-based hard disk, must be destroyed by using the destruction method recommended by the manufacturer, if they are supported, or by using the <block erase> command or by using one or more of the appropriate methods specified in (a), if they are not supported. iii) Magnetic tape: They are the media that stores data by means of the micro-magnet parts on the flexible tape. It must be destroyed by exposing and de-magnetizing to very strong magnetic media or by physical destruction methods such as incineration or melting. iv) Units like a magnetic disk: These are the media that store data with the help of micro-magnet pieces on flexible (plate) or fixed media. It must be destroyed by exposing and de-magnetizing to very strong magnetic media or by physical destruction methods such as burning or melting. v) Mobile phones (SIM card and fixed memory areas): Portable memory devices have a delete command, but most do not have a destroy command. They must be destroyed by using one or more of the suitable methods specified in (a). vi) Optical discs: Data storage media such as CDs and DVDs. It must be destroyed by physical destruction methods such as incineration, disintegration, melting. vii) Peripherals such as printer, fingerprint door access system with removable data recording media: All data recording media must be destroyed by verifying that they are dismounted by using one or more of the suitable methods specified in (a). viii) Peripherals such as printer, fingerprint door access system with fixed data medium: Most of these systems have the delete command, but no destroy command. The appropriate methods specified in (a) must be destroyed using one or more of the methods.

Hardcopy and Microfiche Media: The media must be destroyed because personal data on these media is permanently and physically written on the media. When this operation is performed, it is necessary

to divide the media into small pieces that are incomprehensible to paper shredders or trimmers, horizontally and vertically if possible, so that they cannot be reassembled. Any personal data transferred from the original hardcopy format to the electronic medium by scanning must be destroyed by using one or more of the suitable methods specified in (a) according to the electronic medium, in which they are located.

Cloud Environment: During storage and use of the personal data in these systems, it must be encrypted by the cryptographic methods, and where possible for personal data, especially for each cloud solution that is serviced, separate encryption keys must be used. When the cloud service relationship ends, all copies of the encryption keys required to make personal data available must be destroyed. In addition to the above media, the destruction of personal data on devices that fail or are serviced is carried out as follows: i) The personal data contained in the related devices must be destroyed by using one or more of the suitable methods specified in (a) before these devices are delivered to the third institutions such as the manufacturer, seller, authorized service center for the maintenance and repair of the related devices. ii) Where such destruction is not possible or not suitable, the data storage media must be removed and stored, and other defective components are delivered to third parties such as manufacturers and sellers. iii) Any necessary measures should be taken to prevent any external personnel from copying and taking the personal data out of the organization.

Making the Personal Data Anonymous

Making the personal data anonym means that the personal data cannot be associated with any other identifiable or identifiable person, even by matching it with other data. Our company is able to make the personal data anonym, when the reasons that require the processing of the personal data processed in accordance with the law are eliminated. In order to make the personal data anonymous, the personal data must be rendered unrelated to a specific or identifiable natural person, even by using the suitable techniques for the recording medium and relevant field of activity, such as the return of data by the data controller or recipient groups and/or matching the data to other data. Our company takes all technical and administrative measures necessary to make the personal data anonym.

Any personal data made anonym in accordance with Article 28 of the Personal Data Protection Law can be processed for research, planning and statistical purposes. Such operations are outside the scope of the Personal Data Protection Law and will not require express consent of the personal data subject.

<u>Methods of Making the Personal Data Anonymous</u>

Making the personal data anonym means that the personal data cannot be associated with any identifiable or identifiable natural person, even if it is matched with other data.

In order to make the personal data anonymous, the personal data must be rendered unrelated to a specific or identifiable natural person, even by using the suitable techniques for the recording medium and relevant field of activity, such as the return of data by the data controller or recipient groups and/or matching the data to other data.

Making the personal data anonym means that all direct and/or indirect identifiers in a data set are removed and replaced and thus prevent the relevant person from being identified or loses their property to distinguish such person in a group or crowd so that such person cannot be associated with a real person. Any data that does not indicate a particular person as a result of blocking or losing these features is considered as data made anonym. Other anonym data is the information that identifies a real person before this process, but after this process, it cannot be associated with the relevant person and has been disconnected from the person. The purpose of making the personal data anonym is to

break the link between the data and the person, whom this data defines. All of the bond breaking operations carried out by automatic or non-automatic methods such as grouping, masking, derivation, generalization, randomization, etc. are applied to the records in the data recording system where the personal data is stored. The data obtained as a result of the application of these methods should not be able to identify a particular person.

The exemplary anonymization methods are described as follows:

Anonymization Methods that do not provide any value irregularity: In methods that do not provide value irregularity, no change or addition, subtraction is applied to the values of the data in the cluster; instead, changes are made to all rows or columns in the cluster. Thus, while the overall data changes, the values in the fields keep their original state.

Removing the Variables

It is a method of anonymization provided by completely deleting one or more of the variables from the table. In this case, the entire column in the table will be removed completely. This method can be used for reasons such as the fact that the variable is a highly descriptive variable, that there is no more appropriate solution, that the variable is too sensitive to be disclosed to the public, or that it does not serve analytical purposes.

Removing the Records

In this method, anonymity is reinforced by subtracting a line containing singularity in the data set and the probability of generating assumptions about the data set is reduced. Often, the records that are extracted are those that do not have a common value with other records and can easily be guessed by those who have an idea of the data set. For example, in a data set that includes survey results, only one person from any sector is included in the survey. In such a case, it may be preferable to remove only the record of this person rather than to subtract the "sector" variable from all survey results.

Regional Masking

The objective of the regional masking method is to make the data set more secure and to reduce the risk of predictability. If the combination of the values of a particular record creates a very visible condition, and it is likely to cause the individual to become distinguishable in the relevant community, the value that creates the exception is changed to "unknown".

d. Generalization

It is the process of converting the relevant personal data from a special value to a more general value. It is the most commonly used method for generating cumulative reports and performing operations based on total figures. The resulting new values show the total values or statistics a group that makes it impossible to access to a real person. For example, assume that a person with Turkish ID No.12345678901 buys diapers from the e-commerce platform, and then also buys wet napkins. In the anonymization process, it can be concluded that xx% of people, who buy diapers from the e-commerce platform, also buy the wet napkin by using the generalization method.

Lower and Upper Limit Coding

The upper and lower limit coding method is defined by defining a category for a given variable and combining the remaining values within the grouping created by this category. Usually, the low or high rates of the values in a given variable are added together and a new definition is made.

Global Coding

The global coding method is a grouping method used in datasets with values that cannot be applied to lower and upper bound codes, do not contain numerical values or cannot be numerically sorted. It is generally used when certain values make it easier to make assumptions and assumptions by clustering. All records in the data set are replaced by this new definition by creating a common and new group for the selected values.

Sampling

In the sampling method, a subset from the cluster is described or shared, rather than the entire data set. This reduces the risk of generating accurate estimates of individuals since it is not known whether a person known to be in the entire data set is included in the disclosed or shared sample subset. Simple statistical methods are used to determine the subset to be sampled. For example, it may be meaningful to make scans and make estimates in the relevant data set of a woman who is known to live in Istanbul if anonymously discloses or shares a dataset of demographic information, occupations and health status of women living in Istanbul. However, Only the records of the women, who are registered in the civil registration office in Istanbul, are left in the relevant data set and the anonymization is removed from the data set and the data is disclosed or shared, and the malicious person who accesses the data has a population record of a woman who knows that she lives in Istanbul, since it is estimated whether the information in the hands of the information belonging to this person cannot make a reliable estimate.

Anonymization Methods That Provide a Value Irregularity: Unlike the above mentioned methods, distorting the values of the data set is created by changing the existing values. In this case, since the values of the records are changing, it is necessary to calculate the benefit planned from the data set correctly. Even if the values in the data set are changing, it is still possible to benefit from the data by ensuring that the total statistics remain intact.

Micro Joining

With this method, all records in the data set are first arranged in a meaningful order and then the whole set is subdivided into a certain number of subsets. Then, the value of each subset of that variable is replaced with the average value by taking the average of the value of the specified variable. Thus, the average value of that variable for the entire dataset will not change.

Data Exchange

The data exchange method is the record changes obtained by exchanging values of a variable subset between the pairs selected from the records. This method is mainly used for categorized variables and the main idea is to transform the database by changing the values of the variables between records of individuals.

Adding Noise

With this method, additions and subtractions are performed in order to achieve the determined distortions in a selected variable. This method is often applied to data sets that contain numeric values. Distortion is applied equally to each value.

Statistical Methods to Strengthen Anonymization

In some data sets made anonym, the combination of some values in the records with individual scenarios may lead to the identification of persons in the records or the assumption that their personal data can be derived.

For this reason, anonymity can be strengthened by using various statistical methods in the data sets made anonym by minimizing the singularity of the records in the data set. The main purpose of these methods is to minimize the risk of anonymity deterioration while keeping the benefit of the data set at a certain level.

K-Anonymity

In the data sets made anonym, the fact that the identities of the persons in the records are identifiable or that the information about a particular person becomes easily predictable if the indirect identifiers are combined with the correct combinations has shaken confidence in the anonymization processes. Accordingly, the datasets made anonym by the various statistical methods had to be made more reliable. K-anonymity has been developed to allow the identification of more than one person with specific fields in a data set, to prevent the disclosure of information specific to individuals that exhibit unique characteristics in certain combinations. If there are multiple records of combinations of some of the variables in a data set, the likelihood of identifying the persons corresponding to that combination is reduced

L- Diversity

The L-diversity method, which is developed by the studies conducted on the deficiencies of K-anonymity, takes into account the diversity of the sensitive variables corresponding to the same variable combinations.

T-Proximity

Although the L-diversity method provides diversity in personal data, there are situations in which it cannot provide adequate protection because the method does not deal with the content and sensitivity of personal data. In this form, the process of calculating the degree of closeness of personal data and values among themselves and subdividing the data set according to these degrees of proximity is called as T-proximity method.

Choosing the anonymization method

Our company decides which of the above methods will be applied by looking at the data at their disposal and considering the following features of the data set:

Nature of the data;
Size of the data;
Structure of data in physical media;
Data diversity;
Benefit/processing purpose of the data;
Processing frequency of data;
Reliability of the party to which the data will be transferred;
The meaningful efforts to make the data anonymous;
The magnitude of the damage that may arise in case of anonymity of the data, and and its impact area;
The distribution/centrality ratio of the data;
Control of users' access to relevant data; and

The likelihood that an effort to construct and launch an attack that would disrupt anonymity would make sense.

While it makes a data anonymous, the Company checks the data whether it is a re-identifier by using known or publicly available information from other institutions and organizations to which it transmits personal data by means of contracts and risk analyzes.

Anonymity Assurance

When it decides to make it anonym instead of deleting or destroying a personal data, our company does not disrupt the anonymity by combining the data set made anonym with any other data sets, without creating one or more values in a way that it can make a record unique and anonym. We want consider the fact that the values in the data set cannot be combined and produce an assumption or result. As our company makes anonymous data, any controls are made as the features listed in this article change and anonymity is maintained.

Risks of Corruption of Anonymization by Reverse Processing of Anonymous Data

Since making the personal pers is the process of applying personal data and destroying the distinctive and identifiable characteristics of the data set, there is a risk that these operations can be reversed by various interventions and that the data made anonym becomes re-identifiable and distinctive. This is referred to as disruption of anonymity. The anonymization processes can be accomplished only by manual or automated processes, or by hybrid processes consisting of a combination of both types. It is important, however, that after the data made public is shared or disclosed, any measures are taken to prevent anonymity from being compromised by new users who can access or own the data. The actions carried out consciously about the disruption of anonymity are called "attacks against the disruption of anonymity". In this context, our Company investigates whether there is a risk that the personal data made public may be reversed by various interventions, and that the data made public may become re-identifiable and distinguishable from the real persons, and an operation is established accordingly.

HOW DO WE PROTECT YOUR PERSONAL DATA?

In order to protect your personal data and prevent unlawful access, the Company takes necessary administrative and technical measures in line with the Personal Data Security Guideline published by the Personal Data Protection Committee, prepares the procedures in the company, prepares the clarification and express consent texts, conducts any necessary audits to ensure the implementation of the provisions of the Personal Data Protection Law in accordance with article 12/3 of the Personal Data Protection Law, or procure any external service. The results of these audits are evaluated within the scope of the internal operation of the Company and necessary actions are taken to improve the measures taken.

Your personal data mentioned above will be transferred to physical archives and information systems of our Company and/or our suppliers and kept in both digital and physical media. The technical and administrative measures taken to ensure the security of personal data are described in detail below under two headings:

Technical Measures

We use generally accepted standard technologies and operational security methods, including the standard technology called Secure Socket Layer (SSL), to protect the personal information collected. However, due to the nature of the Internet, information can be accessed by unauthorized persons over

networks without the necessary security measures. We take technical and administrative measures to protect your data from risks such as destruction, loss, tampering, unauthorized disclosure or unauthorized access, depending on the current state of technology, the cost of technological implementation, and the nature of the data to be protected. Within this scope, we conclude data security agreements with the service providers we work with.

1) Ensuring Cyber Security: We use the cyber security products to ensure personal data security, but our technical measures are not limited to this. The first line of defense against attacks from environments such as the Internet is established through measures such as firewall and gateway. However, almost every software and hardware is subjected to a number of installation and configuration operations. Considering that some of the commonly used software, especially older versions, may have documented security vulnerabilities, unused software and services are removed from the devices. Therefore, such unused software and services are primarily preferred because of their ease of deletion rather than keeping them up to date. The patch management and software upgrades ensure that the software and hardware work properly and that the security measures taken for the systems are sufficient to check regularly.

2) Access Restrictions: Access rights to systems containing personal data are restricted and reviewed regularly. Within this scope, employees are granted access rights to the extent necessary for their work and duties and their powers and responsibilities, and access to related systems is provided by using user name and password. When creating these passwords and passwords, combinations of uppercase and lowercase letters, numbers and symbols are preferred instead of numbers or letter sequences related to personal information that can be easily guessed. Accordingly, the access authorization and control matrix is established.

3) Encryption: In addition to using strong passwords and passwords, limiting the number of password entry attempts to protect against common attacks such as the use of brute force algorithm (BFA), ensuring that passwords and passwords are changed periodically, and administrator account and admin privileges are opened only for use when needed. and for employees who have been dismissed from the Data controller, access is restricted without delay, such as deleting an account or closing entries.

4) Antivirus Software: In order to protect against malware, products such as antivirus, antispam, which regularly scans the information system network and detect hazards are used, and the required files are regularly scanned. If personal data will be obtained from different internet sites and/or mobile application channels, it is ensured that the connections are made via SSL or more secure way.

5) Monitoring of Personal Data Security: Checking which software and services are operating in information networks, Determining whether there is any infiltration or non-infiltration in IT networks, Keeping the transaction transactions of all users regularly (such as log records), Security problems as fast as possible reporting. A formal reporting procedure is also set up for employees to report security weaknesses in systems and services or threats using them. Evidence is collected and stored securely in the event of undesired events such as information system crash, malicious software, decommissioning attack, missing or incorrect data entry, violations of privacy and integrity, abuse of information system.

6) Ensuring the Security of Personal Data Environments: If personal data is stored on the devices of the responsible persons or in the media, physical security measures are taken against threats such as theft or loss of these devices and papers. The physical environments containing personal data are protected against external risks (fire, flood, etc.) by appropriate methods and the entrances / exits to these environments are controlled.

If personal data is in electronic form, access between network components can be restricted or separated to prevent personal data security breach. For example, if personal data is being processed in this area by limiting it to a specific portion of the network in use, which is reserved for this purpose, the available resources can be reserved for the security of this limited area, not the entire network.

Measures at the same level are also taken for paper media, electronic media and devices containing personal data of the Company located outside the Company campus. As a matter of fact, although personal data security violations frequently occur due to theft and loss of devices containing personal data (laptop, mobile phone, flash disk, etc.), personal data to be transmitted by e-mail or mail is also sent carefully and with adequate precautions. Sufficient security measures are also taken in case employees provide access to the information system network with their personal electronic devices.

The use of access control authorization and / or encryption methods is applied in case of loss or theft of devices containing personal data. In this context, the password key is stored only in the environment accessible to authorized persons and unauthorized access is prevented.

Paper documents containing personal data are also stored in a locked and accessible environment only, and unauthorized access to these documents is prevented.

If any personal data is obtained by others by unlawful means, the Company shall inform the Personal Data Protection Committee and the data subjects of this fact as soon as possible pursuant to article 12 of the Personal Data Protection Law. if they see necessary, the Personal Data Protection Committee may announce this situation at the website or in by any other means.

7) Storage of Personal Data in the Cloud: In the event that personal data is stored in the cloud, it is necessary for the Company to assess whether the security measures taken by the cloud storage service provider are adequate and appropriate. In this context, two-step authentication control is applied for knowing, backing up, synchronizing the personal data stored in the cloud and providing remote access if necessary. During the storage and usage of the personal data in the said systems, it is provided to be encrypted with cryptographic methods, to be encrypted and sent to the cloud environments, and to the use of individual encryption keys where possible for the personal data, in particular for each cloud solution received. When the cloud service relationship ends, all copies of the encryption keys, which may be used to make personal data available, are destroyed. Access to data storage areas with personal data is logged and improper access or access attempts are instantly communicated to those concerned.

8) Information Technology Systems Procurement, Development and Maintenance: Security requirements are taken into consideration when determining the requirements related to the procurement, development or improvement of new systems by the Company.

9) Backing up of Personal Data: In case of personal data being damaged, destroyed, stolen or lost due to any reason, the Company makes use of the backed up data as soon as possible. The backed up personal data is accessible only by the system administrator, and data set backups are excluded from the network.

Administrative Measures

- All activities carried out by our company have been analyzed in detail in all business units and as a result of this analysis, a process-based personal data processing inventory has been prepared. Risky areas in this inventory are identified and necessary legal and technical measures are taken continuously. (For example, the documents to be prepared within the scope of KVKK have been prepared considering the risks in this inventory)

- Personal data processing activities carried out by our company are audited by information security systems, technical systems and legal methods. Policies and procedures regarding personal data security are determined and regular controls are conducted within this scope.
- From time to time, our company may provide services from external service providers to meet information technology needs. In this case, we ensure that these Data Processing external service providers meet at least the security measures provided by our Company. In this case, a written agreement is signed with the Data Processor and the contract includes at least the following points:
  - The Data Processor acts only in accordance with the instructions of the Data controller, the purpose and scope of the data processing specified in the agreement, the Personal Data Protection and other legislation;
  - The Data Processor acts in accordance with the Personal Data Retention and Destruction Policy;
  - The Data Processor is obliged to keep any data confidential indefinitely in relation to the personal data processed;
  - In the event of any data violation, the Data Processor is obliged to inform the Data controller of it immediately;
  - Our Company will perform or have the necessary audits performed on the Data Processor's systems containing personal data, and may review the reports and service provider on the spot;
  - Our Company will take the necessary technical and administrative measures for the security of personal data; and
  - Furthermore as long as the nature of the relationship between the Data Processor and us is suitable, the categories and types of the personal data transferred to the Data Processor are also specified in a separate article.

- As emphasized in the guidelines and publications of the Authority, personal data is reduced as much as possible within the framework of the data minimization principle, and personal data that is not required, outdated and does not serve a purpose are not collected and if collected in the previous period of the Personal Data Protection Law, a data in accordance with the Personal Data Retention and Disposal Policy is destroyed.
- The employees specialized in technical issues are employed.
- Our Company has set provisions on confidentiality and data security in the Employment Agreements to be signed during the recruitment process of its employees and requests that the employees comply with these provisions. The employees are regularly informed and trained about the personal data protection law and taking necessary measures in accordance with this law. The roles and responsibilities of the employees have been revised and their job descriptions have been revised.
- Technical measures are taken in accordance with technological developments, and the measures taken are periodically checked, updated and renewed.
- The access authorizations are limited and reviewed regularly.
- The technical measures taken are regularly reported to the authorized person, and the issues that constitute risk are reviewed and efforts are made to produce the necessary technological solutions.
- Software and hardware including virus protection systems and firewalls are installed.
- The backup programs are used to ensure the safe storage of personal data.
- Security systems are used for storage areas, technical measures taken are periodically reported to the person concerned as a result of internal controls, risk issues are re-evaluated and necessary technological solutions are produced. The files/printouts stored in the physical environment are stored by the supplier companies and then disposed of in accordance with the established procedures.

- The protection of personal data is also accepted by the top management, a special Committee (the Personal Data Protection Committee) has been established and started to work. A management policy regulating the working rules of the Company's KVK Committee has been put into effect within the Company and the duties of the KVK Committee have been explained in detail.

HOW DO WE PROTECT YOUR SENSITIVE PERSONAL DATA?

A separate policy on the processing and protection of sensitive personal data has been prepared and put into force.

Article 6 of the Personal Data Protection Law is arranged as data of a special quality on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data as they carry the risk of causing the victimization or discrimination of persons when processed in contradiction, and is subject to the processing of this data more sensitive protection.

Pursuant Article 10 of the Personal Data Protection Law, our Company enlightens the Related Persons during the collection of personal data. Special personal data are processed by taking appropriate measures and performing the necessary audits. As a rule, one of the conditions for the processing of sensitive personal data is the express consent of the data subject. Our company offers data subjects the opportunity to disclose their express consent on a specific issue, based on information and freewill.

As a rule, our Company obtains the express consent of the Related Persons in writing for the processing of sensitive personal data. However, pursuant to article 6/3 of the Personal Data Protection Law and In case of the existence of any of the conditions specified in article 5/2 of the Personal Data Protection Law, the express consent of the Related Persons is not required. Besides, in article 6/3 of the Personal Data Protection Law, it stated that the personal data on health and sexual life is processed by the persons or authorities and institutions under the confidentiality obligation for purposes of protecting othe public health, conducting the preventive medicine, medical diagnosis, treatment and care services, and planning and managing healthcare service and financing without the express consent of the relevant person. Regardless of the reason, the general data processing principles are always taken into account in the processing processes and they are complied with.

Our company takes special measures to ensure the security of personal data. Due to the principle of data minimization, sensitive personal data is not collected and processed only when necessary, unless it is necessary for the relevant business process. In case of processing of personal data of special quality, technical and administrative measures are taken to comply with the legal obligations and to comply with the measures determined by the Personal Data Protection Committee.

WHAT ARE YOUR RIGHTS ABOUT YOUR PERSONAL DATA?

Pursuant to article 11 of the Personal Data Protection Law as the data subjects, you have the following rights on your personal data:

- To find out whether your personal data is processed by our Company;
- To request information if your personal data has been processed;
- To learn the purpose of processing your personal data and whether they are used properly;
- To know the third parties to whom your personal data is transferred at home or abroad;

- If your personal data is incomplete or processed incorrectly, to request that it be corrected, and request that the transaction be notified to the third parties to whom your personal data have been transferred;
- Although it has been processed in accordance with the provisions of the KVKK and other relevant laws;
- to request the deletion or destruction of your personal data in the event that the reasons;
- To request the notification to the third parties to whom your personal data are transferred;
- To object to the occurrence of a result against you by analyzing the processed data exclusively through automated systems; and
- To request the loss of your personal data if you have suffered damage due to unlawful processing of your personal data.

You can forward these requests to our Company free of charge in accordance with the Application Notice and by using the following methods:

1) To complete the form available at https://www.muze.gov.tr/kisiselveriler, to sign it with a wet signature and forward it personally to SICPA TURKEY in Yayla Mah, D-100 Karayolu, Ruya Sok, No: 2, Tuzla/Istanbul (please, note that you must submit your identity card);
2) To complete the form available at https://www.muze.gov.tr/kisiselveriler, to sign it with a wet signature, and to forward it to SICPA TURKEY in Yayla Mah, D-100 Karayolu, Ruya Sok, No: 2, Tuzla/Istanbul via a notary public;
3) To complete the application form at https://www.muze.gov.tr/kisiselveriler, to sign it with "your secure electronic signature" under the Electronic Signature Law No. 5070, and send it the form with a secure electronic signature form to sicpaturkey@hs02.kep.tr by e-mail; and
4) Delivering to our Company in writing by using your e-mail address previously notified and registered in our Company's system.

The application must contain first name, last name, if the application is written, signature, Turkish ID Number for the citizens of the Republic of Turkey, on Number, nationality for foreigners, passport number or identification number (if any), residence or business address based on the notice, electronic mail address, telephone and fax number for the notice if any, and subject of the request. Any relevant information and documents are also added to the application.

It is not possible to make any request by third parties on behalf of the personal data subjects. In order for a person other than the personal data subject to make a request, a special power of attorney issued by the personal data subject on behalf of the applicant must have a notarized copy with a wet signature. In the application that contains your explanations about the right that you have as a personal data subject and that you request to exercise your rights mentioned above. If you are acting on behalf of someone else or you are acting on behalf of someone else, you must have a power on this matter and document your power, and the application must contain the identity and address information and the documents confirming your identity must be attached to the application.

Applications to be made by you within this scope will be finalized within the shortest possible time and within 30 days. These applications are free of charge. However, if the process requires additional costs, the fee in the tariff determined by the Personal Data Protection Committee may be charged.

If the personal data subject submits his/her request to our Company in accordance with the prescribed procedure, our Company shall conclude the request free of charge within the shortest time and no later within thirty days according to the nature of the request. However, if the process requires a separate cost, the fee in the tariff determined by the Personal Data Protection Committee will be charged by our Company. Our company may require the relevant person any information to determine whether the applicant is a personal data subject or not. To clarify the matters set forth in the

application of the personal data subject, our company may ask questions about the application of the personal data subject.

If our Company rejects your application, you find our answer inadequate or we do not respond to the application within the period, you can make a complaint to the Personal Data Protection Committee within thirty days from the date, when you learn response of our company and in any case within sixty days from the date of application pursuant to article 14 of the Personal Data Protection Law.

WHAT ARE THE CONDITIONS THAT THE DATA SUBJECTS CANNOT PROVIDE THE RIGHTS OF?

The personal data subjects cannot claim the rights of personal data subjects mentioned above in accordance with Article 28 of the Personal Data Protection Law, since the following cases are excluded from the scope of the Personal Data Protection Law:

- Processing of personal data for purposes such as research, planning and statistics by making it anonym with the official statistics;
- To process any personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, without prejudice to national defense, national security, public security, public order, economic security, privacy or personal rights;
- To process any personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to provide national defense, national security, public security, public order or economic security; and
- The processing of personal data by judicial authorities or enforcement authorities with respect to investigations, prosecutions, proceedings or executions.

Pursuant to Article 28/2 of the Personal Data Protection Law, the personal data subjects cannot claim any other rights listed in article 9 except for the right to claim damages in the following cases:

- If any necessary personal data is processed for crime prevention or crime investigation;
- Any personal data made public by the personal data subject is processed;
- If any personal data must be processed for performance of supervisory or regulatory duties, and for disciplinary investigation or prosecution by the authorized public institutions and organizations and professional organizations in the nature of public institutions based on the authority granted by law; and
- If any personal data must be processed for the protection of the economic and financial interests of the State in relation to budget, tax and financial matters

OTHER PROVISIONS

As explained in detail above, your personal data can be stored, classified according to market research, financial and operational processes and marketing activities, updated in different periods, and to the extent permitted by the legislation, within the framework of the laws and confidentiality principles, and transferred to any third persons and/or suppliers and/or services providers and/or foreign shareholders, to which we are affiliated as the service requires. Any information may be transferred, stored, reported and processed in electronic or hardcopy media in accordance with the policies bound by us with and other reasons foreseen by other authorities.

In case of any inconsistency between the provisions of the Personal Data Protection Law and other relevant legislation and this Policy, the provisions of the Personal Data Protection Law and other relevant legislation shall prevail.

This policy is effective since the date of publication.

We would like to remind you that we may make updates to this statement due to changes in legislation and changes in our company policies. We will publish the most current version of the statement on our website.

Before they enter the website, the User/Users agrees/agree, states/state and undertakes/undertake irrevocably that the User/Users has/have read this Personal Data Protection Policy, will comply with all provisions stated here, and the contents of the website and all the electronic media and computer records of our Company will deemed as definitive evidences pursuant article 193 of the Law of Civil Procedure.

Effective Date: 01.05.2019 Version: 1.0

APPENDIX - ABBREVIATIONS

ABBREVIATIONS	Description
Law No.5651	Law on the Regulation of the Publications Made on the Internet and Combat Against Crimes Committed through these Publications that was published in the copy dated of May 23, 2007 and numbered 26530 of the Official Gazette, and entered into force.
Constitution	Constitution dated of November 7, 1982 and numbered 2709 of Republic of Turkey that was published in the copy dated of November 9, 1982 and numbered 17863 of the Official Gazette, and entered into force.
Application Notice	Notice on the Procedures and Principles of Application to the Data Officer that was published in the copy dated of March 10, 2019 and numbered 30356 of the Official Gazette, and entered into force.
Relevant Person/Relevant Persons or Data subject	A real person, whose personal data is processed, such as any customers of SICPA TURKEY company and/or its group companies under the structure of SICPA TURKEY, and corporate companies, companies, business partners, shareholders, officers, candidate employees, trainees, visitors, third persons and other persons including, but not limited to, ones listed here, with whom the company employs or has a business relation.
Regulation on Deletion, Destruction and Anonymization of Personal Data	Regulation on Deletion, Destruction and Anonymization of Personal Data that entered into force as of January, 2018.
Personal Data Protection Law	Personal Data Protection Law that was published in the copy dated of April 7, 2016 and numbered 29677 of the Official Gazette, and entered into force.
Personal Data Protection Committee	Personal Data Protection Committee
Personal Data Protection Authority	Personal Data Protection Authority
Article	Article
e.g.	Example
Policy	This Personal Data Protection Policy of SICPA TURKEY
Company	Sicpa Turkey Urun Guvenliği Sanayi Ve Ticaret A.S.
Turkish Penal Law	Turkish Penal Law dated of October 12, 2004 and numbered 25611 that was published in the copy dated of September 4, 2004 and numbered 5237 of the Official Gazette and entered into force.
SICPA TURKEY	Sicpa Turkey Urun Guvenliği Sanayi Ve Ticaret A.S.