DOCUMENTS

Security Begins With Awareness ™

POLICY FOR THE PROCESSING AND PROTECTION OF PERSONAL DATA OF KARMASIS INFORMATION SOLUTIONS JOINT STOCK COMPANY

INTRODUCTION

According to the Law on the Protection of Personal Data numbered 6698 (hereinafter referred to as the "Law"), this Personal Data Processing and Protection Policy (hereinafter referred to as the "Policy") prepared by Karmasis Bilişim Çözümleri Ticaret Anonim Şirketi (hereinafter referred to as the "COMPANY") regulates the procedures and principles to be followed in the protection and processing of personal data. As per Article 20 of the Constitution of the Republic of Turkey, everyone has the right to demand the protection of their personal data. In this regard, the COMPANY takes the necessary care for the protection of personal data and makes it a company policy through this Policy, which is a constitutional right. In order to protect personal data processed in accordance with relevant legislation, the COMPANY takes necessary administrative and technical measures. This Policy sets out the basic principles adopted by the COMPANY in the processing of personal data, including:

- Processing personal data in accordance with the law and honesty principles,
- Keeping personal data accurate and up-to-date when necessary,
- Processing personal data for specific, clear, and legitimate purposes,
- Processing personal data in a relevant, limited, and measured manner in connection with the purpose for which they were processed,
- Preserving personal data for the period specified in relevant legislation or as long as necessary for the purpose for which they were processed,
- Informing and enlightening data subjects,
- Establishing the necessary system for data subjects to exercise their rights,
- Taking necessary measures for the protection of personal data,
- Complying with relevant legislation and the regulations of the Personal Data Protection Board when transferring personal data to third parties,
- Showing necessary sensitivity for the processing and protection of sensitive personal data.

1. PURPOSE and SCOPE

- In line with the principle of conducting the sustainability of the activities of the "COMPANY" in transparency, the fundamental principles adopted by the "COMPANY" regarding compliance with the regulations in the "Law" for its data processing activities are determined, and the practices carried out by the "COMPANY" are disclosed.
- The "Policy" determines the processing conditions of personal data and sets forth the main principles adopted by the "COMPANY" in the processing of personal data. In

this context, the "Policy" is directed towards the real persons whose personal data are processed in all personal data processing activities within the scope of the "Law," whether they are carried out automatically or not, and whether they are a part of any data recording system.

- Within this scope, personal data of real persons are processed, including employees, job candidates, interns, bank officials, cyberpark personnel, relatives of employees, shareholders/partners, business partners, business partner representatives, employers, employer/representatives, references, insurance company/agency officials, witnesses, suppliers, supplier employees, supplier officials, persons who receive products or services, employees of the persons who receive products or services, and authorized representatives of the persons who receive products or services, and other third parties.
- The "COMPANY" reserves the right to make changes to the "Policy" in line with legal regulations.

1.1. Definitions

Personal Data - Any kind of information related to an identified or identifiable natural person. Therefore, processing of information related to legal persons is not within the scope of the Law. For example, Name, Surname, ID Number, E-mail, Address, Date of Birth, Credit Card Number, etc.

Sensitive Personal Data - Data relating to race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance, membership in associations, foundations or trade-unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

Processing of Personal Data - Refers to any operation performed on personal data, whether fully or partially automated, or non-automated means that form part of any data recording system, such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, sharing, classifying, or preventing their use, to make the data accessible. In other words, any activity performed on personal data, starting from the initial acquisition of data, is considered data processing.

Data Subject/Related Person - The real person whose personal data is processed. For example, employees, suppliers.

Data Recording System - Refers to an automated or non-automated recording system that processes personal data structured according to certain criteria, or is part of any data recording system.

Data Controller - The natural or legal person who determines the purposes and methods of processing personal data, and is responsible for establishing and managing the data recording system.

Data Processor - The natural or legal person who processes personal data on behalf of the data controller, based on the authority granted by the data controller.

Explicit Consent - Informed and freely given consent regarding a specific matter.

Anonymization - Refers to rendering data so that it can no longer be associated with an identified or identifiable individual by any means, including by matching it with other data. Techniques such as masking, aggregation, data derivation, data perturbation, etc. can be used to make personal data unidentifiable with any real person.

VERBIS - Data Controllers Registry Information System.

1.2. Entry into Force

The Policy has been published by the COMPANY on www.karmasis.com website and entered into force. Relevant legal regulations regarding the processing and protection of personal data will be primarily applied. In case of any conflict between the provisions of the "Law" and the regulations included in this "Policy", the provisions of the legislation shall apply. The COMPANY reserves the right to make changes to the Policy in parallel with legal regulations.

2. DATA SUBJECTS, PROCESSED DATA, PROCESSING PURPOSES AND DATA CATEGORIES

2.1. Categories of Data Subjects

The data subjects within the scope of the Policy are all natural persons whose personal data is being processed by the COMPANY. In this context, the general categories of data subjects are as follows:

DATA SUBJECT CATEGORIES	DESCRIPTION
Employee	Real persons who are employed based on an employment contract and whose personal data is obtained through employment relationship, in accordance with the Labor Law No. 4857, at "COMPANY".

DATA SUBJECT CATEGORIES	DESCRIPTION
Job Applicant	Real persons who apply for a job by submitting their CV, filling out a job application form or using other methods, and who communicate through career websites or referral channels.

DATA SUBJECT CATEGORIES	DESCRIPTION

Intern/Apprentice - Real persons who are undergoing an internship within the scope of Vocational Training Law No. 3308 at “COMPANY”.

DATA SUBJECT CATEGORIES DESCRIPTION

Shareholder/Partner/Employer or Representative/Chairman of the Board-Vice Chairman-Member - Real persons who are shareholders, have management authority, and similar powers in the company.

DATA SUBJECT CATEGORIES DESCRIPTION

Supplier/Authorized Person/Employee - Real persons who are suppliers, authorized persons, and employees of the company with whom the company has business relationships for obtaining goods/services.

DATA SUBJECT CATEGORIES DESCRIPTION

Potential Supplier/Authorized Person/Employee - Real persons who have the potential to establish a business relationship with the COMPANY, and who are potential suppliers, authorized persons or employees that the COMPANY may obtain goods/services from.

DATA SUBJECT CATEGORIES DESCRIPTION

Customer/Client or Authorized Person/Employee - Real persons who benefit from the products and services offered by the COMPANY.

DATA SUBJECT CATEGORIES DESCRIPTION

Potential Product or Service Recipient/Authorized Person/Employee Real persons who have the potential to use the products and services offered by the “COMPANY”, and have the potential to become customers.

DATA SUBJECT CATEGORIES DESCRIPTION

Visitor - Real persons who visit the premises and website of the “COMPANY”.

DATA SUBJECT CATEGORIES DESCRIPTION

Third Parties: The categories listed above refer to natural persons, excluding employees of the COMPANY. For example; Employee/Employee Candidate/Intern Relatives, Parent, Guardian, Witness, etc.

The categories of data subjects are indicated for the general purpose of information sharing. The fact that the data subject does not fall within any of these categories does not negate their status as a data subject as defined by the Law.

2.2. Personal Data That Can Be Processed

Personal data refers to information that identifies or can identify a person. The categories of personal data that can be processed by "COMPANY" and listed in VERBIS are specified below.

PERSONAL DATA CATEGORIES DESCRIPTION

1- Identity: Data containing information about a person's identity such as name, surname, national ID number, nationality, mother's and father's names, place of birth, date of birth, gender, and signature, as well as documents such as driver's license, ID card, and passport, and other information such as social security number, vehicle license plate, etc.
2- Communication: Information such as telephone number, address, e-mail address, fax number, IP address.
3- Location: Information that determines the location of the person using location tools; such as GPS location, travel data, etc.
4- Personnel records: Other information that needs to be taken within the scope of the personnel file that needs to be legally created within the framework of the employment contract with the personnel, as well as other personnel information related to other activities.
5- Legal Transaction: Information related to legal transactions such as lawsuits, executions, power of attorney, etc.
6- Customer Transaction: Information contained in documents related to individuals who have received products or services.
7- Physical Space Security: Personal data related to records and documents taken during entry into physical space and during stay in the physical space; camera records and records taken at security checkpoints.
8- "Transaction Security: Personal data processed to ensure technical, administrative, legal, and commercial security while conducting commercial activities.
9- Risk Management: Personal data processed to manage commercial, technical, and administrative risks.
10- Finance: Personal data processed for documents, records, and information showing any financial results created depending on the type of legal relationship, including bank account numbers, IBAN numbers, credit card information, financial profile, wealth data, income information, and other financial information
11- Professional Experience: Information related to professional experience and expertise, such as education, duties, titles, etc.
12- Marketing: Information related to marketing activities, such as advertising and promotion.
13- Visual and Audio Records: Personal data processed for records and documents other than those in the Physical Space Security category, such as camera records, security point records, pictures, videos, call center recordings, etc. taken during entry into or presence within the physical space.
14- Race and Ethnic Origin: These are special categories of personal data, and they include data related to individuals' race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance, association with a union or similar organization, health, sex life, criminal convictions, and security measures, as well as biometric and genetic data. The expansion of special categories of personal data by analogy is not possible."
15- Political Views
16- Philosophical Beliefs, Religion, Denomination, and Other Beliefs

17- Appearance and Dress
18- Membership in Associations
19- Membership in Foundations
20- Membership in Trade Unions
21- Health Information
22- Sexual Life
23- Convictions and Security Measures
24- Biometric Data
25- Genetic Data
26- Other Information

Other categories of personal data that need to be processed but do not fit into the categories mentioned above.

2.3. Categories of Personal Data Owners and Processing Purposes

The personal data processed by the "COMPANY" is based on and limited to the processing conditions in the Law. The purposes of processing the personal data that can be processed by the "COMPANY" and listed in VERBIS are given below.

PURPOSES OF DATA PROCESSING

Execution of Emergency Management Processes

Execution of Information Security Processes

Execution of Employee Candidate / Intern / Student Selection and Placement Processes

Execution of Employee Application Processes

Execution of Employee Satisfaction and Loyalty Processes

Fulfillment of Employee Contractual and Legal Obligations

Execution of Employee Rights and Benefits Processes

Execution of Audit / Ethical Activities

Execution of Training Activities

Execution of Access Authorization Processes

Compliance with Legal Regulations in Activities

Execution of Finance and Accounting Affairs

Execution of Loyalty Processes for Company / Product / Services

Provision of Physical Space Security

PURPOSES OF DATA PROCESSING

Execution of Assignment Processes

Tracking and Execution of Legal Affairs

Execution of Internal Audit / Investigation / Intelligence Activities

Execution of Communication Activities

Planning of Human Resources Processes

Execution / Supervision of Business Activities

Execution of Occupational Health / Safety Activities

Receipt and Evaluation of Suggestions for Improvement of Business Processes

Execution of Business Continuity Activities

Execution of Logistics Activities

Execution of Procurement Processes for Goods / Services

Execution of Post-Sales Support Services for Goods / Services

Execution of Sales Processes for Goods / Services

Execution of Product / Service Production and Operation Processes

Execution of Customer Relationship Management Processes

Execution of Activities for Customer Satisfaction

Organization and Event Management

Execution of Marketing Analysis Studies

Execution of Performance Evaluation Processes

Execution of Advertising / Campaign / Promotion Processes

Execution of Risk Management Processes

Execution of Storage and Archive Activities

Execution of Social Responsibility and Civil Society Activities

Execution of Contract Processes

Execution of Sponsorship Activities

Execution of Strategic Planning Activities

Tracking of Requests / Complaints

Provision of Security of Movable Assets and Resources

Execution of Supply Chain Management Processes

Execution of Wage Policy

Execution of Product / Service Marketing Processes

Ensuring the Security of Data Controller Operations

Foreign Personnel Work and Residence Permit Procedures

Execution of Investment Processes

Execution of Talent / Career Development Activities

Provision of Information to Authorized Persons, Institutions, and Organizations

Execution of Management Activities

Creation and Tracking of Visitor Records

Other

3. PRINCIPLES AND PROCEDURES TO BE FOLLOWED IN DATA PROCESSING

3.1. General Principles for Processing Personal Data

Your personal data is processed by the 'COMPANY' in accordance with the personal data processing principles set forth in Article 4 of the Law. In this context:

- Pursuant to the principle of Processing in Compliance with the Law and Honesty, 'COMPANY' acts in compliance with the principles introduced by legal regulations and the general principles of trust and honesty while processing personal data. In accordance with the principle of honesty, 'COMPANY' takes into account the interests

and reasonable expectations of the relevant individuals while striving to achieve its data processing objectives.

- Pursuant to the principle of Ensuring that Personal Data are Accurate and Up-to-Date When Necessary, it is necessary to keep personal data accurate and up-to-date in order to protect the fundamental rights and freedoms of the relevant individual from the perspective of 'COMPANY'. 'COMPANY' has an active duty of care in ensuring that the information of the relevant individual is kept accurate and up-to-date. Therefore, all communication channels are open to ensure that the information of the relevant individual is kept accurate and up-to-date.
- Pursuant to the principle of Processing for Specified, Explicit, and Legitimate Purposes, 'COMPANY' clearly and specifically determines the legitimate and legal purpose of personal data processing. 'COMPANY' processes personal data that are necessary for and related to its commercial activities.
- Pursuant to the principle of Being Relevant, Limited and Proportionate to the Purposes for Which They are Processed, 'COMPANY' processes personal data only for the purposes that are related to its business activities and necessary for the performance of its duties. Therefore, 'COMPANY' processes personal data in a way that is appropriate for the realization of the determined purposes, and does not process personal data that are irrelevant or not necessary for the purposes.
- Pursuant to the principle of Retaining Personal Data Only for the Period Stipulated by Relevant Legislation or Required for the Purposes for Which They were Processed, 'COMPANY' keeps personal data for only the period stipulated by the relevant legislation or required for the purposes for which they were processed. In this context, 'COMPANY' first determines whether a period has been stipulated for the storage of personal data in the relevant legislation, and if a period has been determined, it acts in accordance with that period, and if no period has been determined, 'COMPANY' keeps personal data for the period necessary for the purposes for which they were processed. 'COMPANY' relies on the storage periods in its personal data inventory, and at the end of these periods, personal data are deleted, destroyed or anonymized within the framework of the obligations within the scope of the Law, depending on the nature of the data and the purpose of their use.

3.2. Processing Conditions for Personal Data

The COMPANY" processes personal data only within the purposes and conditions of personal data processing requirements specified in the second paragraph of Article 5 of the Law. As a general rule, personal data cannot be processed without the explicit consent of the relevant person. However, in the presence of one of the following conditions, personal data can be processed without the explicit consent of the relevant person: These purposes and conditions are as follows:

- The processing of your personal data is explicitly stipulated in the legislation and laws to which "The COMPANY" is subject in the relevant activity,
- The processing of your personal data by "The COMPANY" is directly related and necessary for the establishment or performance of a contract, and processing of personal data of the parties to the contract is necessary to provide the requested products and services or to fulfill the requirements of the concluded contracts,

- The processing of your personal data is mandatory for "The COMPANY" to fulfill its legal obligations,
- Processing of personal data by "The COMPANY" limited to the purpose of public disclosure, provided that personal data has been publicly disclosed by the data owner,
- The processing of personal data by "The COMPANY" is mandatory to establish, use, or protect the rights of the data owner or third parties, in accordance with "The COMPANY's" legislation or internal practices,
- Processing of personal data is mandatory for "The COMPANY's" legitimate interests, provided that it does not harm the fundamental rights and freedoms of the data owner,
- Processing of personal data by "The COMPANY" is mandatory for the protection of the life or physical integrity of the data owner or someone else, and if the data owner is unable to explain his/her consent due to actual or legal invalidity.

3.3. Conditions for Processing Special Categories of Personal Data

4. The "COMPANY" processes personal data of special nature within the purposes and conditions specified in the third paragraph of Article 6 of the "Law" on the processing of personal data of special nature. The "Law" specifies a limited number of personal data of special nature. In other words, it is not possible to increase the number of personal data of special nature. These are data related to the race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, clothing and appearance, membership of associations, foundations or trade unions, health, sexual life, conviction and security measures, as well as biometric and genetic data.
5. The "COMPANY" may process your personal data of special nature with necessary measures in the following cases: ➢ Personal data of special nature are not processed as a principle without the explicit consent of the data subject. The "Law" has introduced prohibitive regulations on this matter. ➢ However, personal data of special nature, except for health and sexual life, are processed without the explicit consent of the data subject in cases prescribed by laws.

4. INFORMATION AND ENLIGHTENMENT OF DATA SUBJECTS

The 'COMPANY' informs personal data owners in accordance with Article 10 of the 'Law' during the acquisition of personal data. In this context, the 'COMPANY' provides information to the data subject about the identity of the data controller, if any, the identity of the representative, the purpose for which personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method of personal data collection and the legal basis, and the rights of the data subject depending on the nature of the data subject and the data processing process. Information texts have been placed in areas where data subjects can see them at the headquarters and on the website of the Company.

5. METHODS OF COLLECTING PERSONAL DATA AND LEGAL BASIS

Personal data is collected through various physical and electronic means, such as website visits, face-to-face communications, establishment and execution of contracts, recruitment processes, visits to our workplaces, telephone calls, emails and any other means, depending on the nature of the personal data and the purpose of processing, in accordance with the legal grounds set forth in Article 5(2) of the Law and subsequent articles, and in cases where no such ground exists, it will be collected with explicit consent. Personal data may be collected through fully automatic, partially automatic, or non-automatic methods, processed and transferred for the purposes listed in this Policy, based on the legal grounds mentioned below:

- Being provided for by the national and international legislation that “COMPANY” is subject to,
- Being necessary for the processing of personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract and is necessary to provide the requested products or services or to perform the obligations under the contract,
- Being mandatory for “COMPANY” to fulfill its legal obligations,
- Being made public by the data subject,
- Being mandatory for the processing of personal data to establish, use or protect a right under the legislation or internal practices of “COMPANY”,
- Being mandatory for “COMPANY”'s legitimate interests, provided that it does not harm fundamental rights and freedoms.

6. TRANSFER OF PERSONAL DATA

In accordance with the additional regulations specified in Articles 8 and 9 of the Law and determined by the Personal Data Protection Board, personal data can be transferred to domestic or foreign countries if there are conditions for the transfer of personal data. The transfer of personal data to third parties within the country can be carried out by the "COMPANY" if at least one of the data processing conditions mentioned in Articles 5 and 6 of the Law and explained under the 3rd title of this "Policy" exists and if the basic principles regarding data processing conditions are followed. The transfer of personal data to third parties abroad can be carried out if at least one of the data processing conditions mentioned in Articles 5 and 6 of the Law and explained under the 3rd title of this "Policy" exists, and if the basic principles regarding data processing conditions are followed, except for cases where the person has given explicit consent. In accordance with the general principles of the Law and the data processing conditions specified in Articles 8 and 9, the "COMPANY" can transfer data to the following Natural and Legal Persons:

➢ Authorized institutions or organizations that are authorized to request personal data of relevant individuals, such as regulatory and supervisory bodies, courts and enforcement offices, and individuals designated by them,

➢ Other business partners and suppliers with whom we cooperate and/or receive services from, limited to obtaining external services for product and service delivery, promotion,

software, resource planning, reporting, marketing, advertising, and similar functions, and benefiting from promotions and campaigns,

➢ Audit firms, independent audit firms, customs firms, accounting/tax consultancy firms, law firms, Joint Health and Safety Unit (JHSU) or Occupational Health and Safety (OHS) firms, who are legally authorized to receive information and documents from "COMPANY" for the purpose and in a limited scope,

➢ Firms that process data on behalf of our company (providing IT support, measuring traffic/customer satisfaction, providing support in profiling, segmentation, and micro-segmentation, supporting personal data processing in sales, advertising, and marketing areas, including SMS, email, archiving),

➢ Service providers, cargo companies, to process and deliver your product/service orders, manage your account, and ensure the continuity of commercial activities,

➢ Banks, payment system providers, and individual pension companies for payment services, risk limit determination, collateral, debt restructuring, and individual pension transactions,

➢ Insurance companies for insurance, coverage, and guarantee transactions,

➢ Audit firms and information security firms for necessary quality, confidentiality, and standard audits,

➢ Authorized public institutions and organizations to fulfill legal obligations and/or requests from official authorities,

➢ Individuals or legal entities to fulfill legal obligations.

7. RIGHTS OF DATA SUBJECTS

As a personal data owner, we would like to inform you that you have the following rights under Article 11 of the Law:

• To learn whether your personal data is being processed or not,

• To request information if your personal data has been processed,

• To learn the purpose of processing your personal data and whether they are being used for their intended purpose,

• To know the third parties to whom your personal data is transferred, whether domestically or internationally

, • To request the correction of your personal data if they are incomplete or inaccurate, and to request that the correction be communicated to third parties to whom your personal data has been transferred in this context,

• To request the deletion or destruction of your personal data if the reasons requiring their processing no longer exist, even if they have been processed in compliance with the KVKK and other related legislation, and to request that the deletion be communicated to third parties to whom your personal data has been transferred in this context

, • To object to the occurrence of a result against you as a result of the analysis of processed data exclusively through automated systems

, • To request compensation if you suffer any damages due to the processing of your personal data in violation of the law.

8. MEASURES REGARDING THE SECURITY, CONFIDENTIALITY, AND PROTECTION OF PERSONAL DATA

The audit and management of personal data security within the departments of "COMPANY" are organized by the Personal Data Protection Committee/Human Resources Department. Awareness is created for the legal requirements determined on a departmental basis, and necessary administrative measures are implemented through company policies, procedures, and training to ensure continuity of implementation and monitoring. Periodic and/or random audits are conducted and commissioned within the organization.

"COMPANY" takes all necessary administrative and technical measures, establishes an audit system within the company, and acts in accordance with the measures provided for in the Law in case of unlawful disclosure, access, transfer, or other security deficiencies that may occur concerning personal data.

In accordance with Article 12 of the Law, "COMPANY" takes necessary technical and administrative measures to ensure an appropriate level of security for preventing the unlawful processing of personal data, unauthorized access to the data, and safeguarding the data. In this context, necessary audits are carried out or commissioned by the company.

"COMPANY" takes technical and administrative measures within the framework of sufficient precautions determined and declared by the Board for special categories of personal data in accordance with the fourth paragraph of Article 6 of the Law for the secure storage, prevention of unlawful processing, and unauthorized access to personal data.

8.1. Technical Measures

The measures taken by the Company regarding the personal data it processes are listed below:

• Network and application security is ensured.

• Security of personal data stored in the cloud is ensured.

• An authorization matrix has been created for employees.

• Access logs are kept regularly.

• Data masking measures are applied when necessary.

• Up-to-date anti-virus systems are used

. • Firewalls are used.

• A user account management and authorization control system is implemented, and their tracking is also performed

. • Log records are kept without user intervention.

• Intrusion detection and prevention systems are used.

• Cybersecurity measures have been taken and their implementation is continuously monitored.

• Encryption is performed

. • Penetration testing is applied.

• Personal data of special nature transferred on portable memory, CD, DVD media are encrypted during transfer.

• Data loss prevention software is used

8.2. Administrative Measures

The measures taken by the Company regarding the personal data it processes are listed below:

• Data security regulations containing data security provisions for employees are available.

• Awareness and training activities on data security are conducted for employees at certain intervals.

• Confidentiality commitments are made.

• The authorities of employees who have changed jobs or left are revoked in this field

. • Signed contracts contain data security provisions.

• Personal data security issues are reported quickly.

• Personal data security is monitored.

• Necessary security measures are taken for the entry and exit of physical environments containing personal data.

• The security of physical environments containing personal data is ensured against external risks (fire, flood, etc.).

• The security of environments containing personal data is ensured.

• Personal data is minimized as much as possible.

• Personal data is backed up and the security of backed up personal data is also ensured

. • Existing risks and threats have been identified.

• Protocols and procedures for the security of special category personal data have been identified and implemented.

• Periodic and/or random internal audits are conducted and commissioned.

9. DESTRUCTION OF PERSONAL DATA

A PERSONAL DATA STORAGE AND DESTRUCTION POLICY, which determines the procedures for the destruction of personal data, has been prepared and published on the "COMPANY" website (www.karmasis.com). All destruction processes are carried out in accordance with this policy. In accordance with Article 7 of the Law, even if the personal data has been processed in accordance with the law, if the reasons requiring its processing have ceased to exist, "COMPANY" shall destroy the personal data in accordance with the Personal Data Storage and Destruction Policy specially prepared for this purpose, in accordance with the legislation and this "Policy" published by "COMPANY" upon the request of the data subject or ex officio. The personal data inventory, prepared by "COMPANY" and regulating all data processing processes, clearly specifies the storage periods for each data type and process, and these periods are taken as basis in the destruction processes.

10. PROCEDURE FOR DATA SUBJECT APPLICATIONS

You can make your applications regarding your rights listed above by filling out the "RELATED PERSON APPLICATION FORM" which you can obtain from our website with the www.karmasis.com extension or by sending a written document with the same content to the address of our company stated below: Bilkent Cyberpark Plaza C Blok Kat 3 No 20 Çankaya 06800 ANKARA.

In order for the application to be considered a valid application, according to the Regulation on Procedures and Principles for Data Controllers' Application, the relevant person must specify the following information: a) Name, surname, and signature if the application is written, b) For Turkish citizens, T.C. identification number, for foreigners, nationality, passport number or identification number, if any, c) Residence or workplace address for notification, d) If any, the e-mail address, telephone and fax number for notification, e) The subject of the request.

Otherwise, the application will not be considered as a valid application. In applications made without filling out the application form, all of the items listed here must be submitted to the "COMPANY".

For third parties to apply on behalf of data subjects, a special power of attorney issued by a notary must be available on behalf of the person who will apply on behalf of the data subject.

If data subjects communicate their requests regarding their personal data to the "COMPANY" in writing, the "COMPANY" as the data controller carries out the necessary processes in accordance with Article 13 of the "Law" to ensure that the request is concluded as soon as possible and within a maximum of thirty (30) days, depending on the nature of the request.

In order to ensure data security, the "COMPANY" may request information to determine whether the applicant is the owner of the personal data in question. The "COMPANY" may also ask questions related to the application to ensure that the application of the relevant person is concluded in an appropriate manner.

The information and documents specified in the Related Person Application Form submitted to us by the Data Subject will be processed by our company only for the purpose of evaluating, answering and finalizing the application made in accordance with Article 13 of the "Law".

The information obtained within the scope of the application may be collected in written, oral, electronic or physical form. Within the scope of this process, the relevant information may be shared with third parties and companies such as law firms, consulting companies, and subsidiaries of the company to which services are received for the finalization of the relevant application. You can use your rights stated in Article 11 of the "Law" in accordance with the procedures and conditions specified in this form.

The application of the relevant person may be rejected by the "COMPANY" with an explanation if there is a possibility of impeding the rights and freedoms of others, requiring disproportionate effort, or if the information is a public knowledge, among other reasons.

APPLICATION FORMAT - METHOD / PROCEDURE - ADDRESS – EXPLANATION

Written Application

It can be made in person with a wet signature or through a notary.

Bilkent Cyberpark Plaza C Block Floor 3 No 20 Çankaya 06800 ANKARA

The envelope / notification will be labeled as "GDPR Related Person Application".

APPLICATION FORMAT - METHOD / PROCEDURE - ADDRESS – EXPLANATION

The Application via E-mail

The application can be made via e-mail by using the electronic mail address previously notified to and registered in our systems by the Applicant.

The e-mail address to use is info@karmasis.com.

The relevant information and documents specified in the Applicant Data Form will be included in the e-mail content and necessary action will be taken accordingly. The subject line of the e-mail will be "KVKK Applicant Request".

KVKK Data Controller:

Karmasis Information Solutions Trading Inc.

info@karmasis.com