HERA CHARGE ELECTRONICS INC.
PERSONAL DATA PROCESSING AND PROTECTION POLICY

INTRODUCTION
In accordance with the Law on the Protection of Personal Data No. 6698 (“Law”); this Personal Data Processing and Protection Policy (“Policy”) of HERA CHARGE ELECTRONICS INC. (Mersis: 0461 1117 5740 0001) (hereinafter referred to as “HERA CHARGE” or “COMPANY”) regulates the procedures and principles that must be adhered to in fulfilling the obligations regarding the protection and processing of personal data by HERA CHARGE.

1.PURPOSE AND SCOPE
The aim is to ensure the sustainability of the principle of conducting “HERA CHARGE” activities with transparency. In this context, the basic principles adopted for compliance with the regulations contained in the Law on the Protection of Personal Data No. 6698 (“KVK Law”) regarding the COMPANY's data processing activities are determined, and the practices carried out by “HERA CHARGE” are explained.
The Policy specifies the conditions for processing personal data and outlines the main principles adopted by HERA CHARGE in processing personal data. Within this framework, the Policy targets all personal data processing activities under the Law, conducted either automatically or through non-automatic means as part of a data recording system, relating to individuals whose personal data are processed.
“HERA CHARGE” reserves the right to amend the “Policy” in line with legal regulations.

1.1. Definitions

COMPANY: HERA CHARGE ELECTRONICS INC.
Personal Data/Data: Any information related to an identified or identifiable natural person.
Sensitive Personal Data: Data regarding race, ethnic origin, political opinion, philosophical belief, religion, sect, or other beliefs, clothing, membership in associations, foundations, or unions, health, sexual life, criminal convictions, security measures, as well as biometric and genetic data.
Processing of Personal Data: Any operation performed on personal data, such as collection, recording, storage, preservation, alteration, reorganization, disclosure, transfer, acquisition, making available, classification, or prevention of the use of data, whether fully or partially automated or non-automated as part of a data recording system.
Third Parties and individuals whose personal data are processed by the “COMPANY”: These are individuals related to third parties with whom “HERA CHARGE” interacts to ensure the security of commercial transactions or to protect the rights and interests of those mentioned above. Examples include joint debtors (Guarantors, Note Debtors), companions, family members, and relatives.
Personal Data Owner / Relevant Person: Refers to stakeholders and employees of the “COMPANY”, business partners, authorized representatives, job applicants, visitors, group customers, potential customers, third parties, and individuals whose personal data are processed by the COMPANY.
Data Recording System: A system that processes personal data structured according to certain criteria.
Data Controller: The natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system.
Data Processor: A 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: Consent based on being informed about a specific subject and expressed freely.
Anonymization: The process of making data that was previously associated with a person impossible to relate to an identified or identifiable natural person, even when matched with other

data.
Law: Refers to the Law on the Protection of Personal Data No. 6698.
KVK Board: The Personal Data Protection Board.

1.2. Effectiveness and Amendments
The Policy has been made public by being published on the “COMPANY”’s website. In case of any conflict between the applicable legislation, primarily the Law on the Protection of Personal Data No. 6698, and the provisions included in this Policy, the provisions of the legislation shall apply. The “COMPANY” reserves the right to amend the Policy in line with legal regulations. The current version of the Policy can be accessed from the “COMPANY”’s website [www.heracharge.com].

2.PERSONAL DATA, DATA OWNERS, DATA PROCESSING PURPOSES, AND DATA CATEGORIES
2.1. What are Your Personal Data?
Personal data means information that identifies or can identify you. The categories of personal data that may be processed by the “COMPANY” are listed below.
Identity Data: This data category includes types of data such as T.R. Identity Number, name, surname, place and date of birth, marital status, gender, and a sample of the identity document.
Family Members and Relatives Information: Information about the personal data owner's family members and relatives.
Contact Data: A group of data that can be used to reach the person (phone number, postal address, email, fax number, IP address, etc.).
Sensitive Personal Data: This data category includes types of data such as health data obtained for personnel's employment and occupational safety, biometric data collected during employment entrance and exit, and criminal convictions and security measures.
Visual Data: Refers to images of individuals captured in security camera recordings for security purposes in the physical environments of the “COMPANY” or photos taken during personnel's employment entrance.
Personnel Files: Types of data that must be legally created as part of the personnel's employment contract, including identity and contact information, as well as profession, education, financial data, etc.
Biometric Data (Facial Recognition System): Types of data obtained, subject to the personnel's written request for alternative methods, regarding the personnel's employment entrance and exit systems.
Visual Records: Types of data that include catalogs, photographs, videos, and all other visual records taken in work areas or areas that can be considered as workplaces for the purposes of conducting and promoting institutional and business activities.
Contract Data: All data, such as signatures, signature circulars, and personal information of real persons, processed in the database as a result of contractual ties established by the “COMPANY” with its customers, business partners, suppliers, and external resources.
Location Data: Refers to all location data of employees processed by the “COMPANY” for internal audit purposes.
Performance Data: All data processed within the “COMPANY” for personnel for internal audit and increasing operational efficiency, and outside the “COMPANY” for the performance evaluation of business partners.
Employee and Job Applicant Information: Personal data processed regarding individuals who have applied to be an employee of the “COMPANY”, or whose applications have been evaluated by the “COMPANY” based on commercial custom and rules of honesty, or who are in a working relationship with the “COMPANY”.
Physical Space Security Information: Personal data related to records and documents obtained during physical entry to premises and during stays inside the premises, such as camera recordings.

Visual Data: Visual records that clearly belong to an identified or identifiable natural person and are associated with the personal data owner within the data recording system.
Operational Security Information: Personal data processed to ensure our technical, administrative, legal, and commercial security while conducting our business activities.
Risk Management Information: Personal data that is clearly related to an identified or identifiable natural person and is processed to manage the "COMPANY"'s commercial, technical, and administrative risks.
Financial Information: Personal data related to any financial outcomes generated according to the type of legal relationship established between the "COMPANY" and the personal data owner, including information, documents, and records.
Location Data: (Position Data)
Request and Complaint Data: Personal data related to the receipt and evaluation of any requests or complaints directed to the "COMPANY".

2.2. Categories of Data Owners
The data owners within the scope of the Policy are all natural persons whose personal data are processed by the "COMPANY." In this context, the general categories of data owners are as follows:

DATA OWNER CATEGORIES	DESCRIPTION
1. Employee	Refers to natural persons who perform services under an employment contract with the "COMPANY."
2. Intern	Refers to natural persons working as interns at the "COMPANY."
3. Job Applicant	Refers to natural persons who apply for a job by sending a CV or through other means to the "COMPANY."
4. Third Parties	Refers to natural persons excluding "COMPANY" employees in the categories mentioned above.
5. Business Partners / Shareholders / Suppliers and their Employees	Refers to parties and their employees who supply goods or services to the "COMPANY" based on instructions and contractual agreements for the purpose of carrying out the "COMPANY"'s commercial activities.
6. Visitor	Refers to natural persons visiting the "COMPANY"'s premises and website.
7. Customer	Refers to natural persons benefiting from the products and services offered by the "COMPANY."
8. Potential Customer	Refers to natural persons showing interest in using the products and services offered by the "COMPANY," having the potential to become a customer.

The data owner categories are specified for general information sharing purposes. The fact that a data owner does not fall under any of these categories does not eliminate their status as a data owner as defined in the Law.

2.3. Purposes of Personal Data Processing

For Employees:

- Managing Employee Satisfaction and Engagement Processes
- Fulfilling Obligations Arising from Employment Contracts and Legislation
- Conducting Audits / Ethical Activities

- Conducting Training Activities
- Managing Access Permissions
- Conducting Activities in Compliance with Legislation
- Managing Financial and Accounting Operations
- Planning Human Resources Processes
- Conducting/Monitoring Business Activities
- Conducting Occupational Health and Safety Activities
- Providing Information to Authorized Persons and Institutions
- Managing Administrative Activities
- Ensuring Business Continuity and Physical Security of the Premises
- Managing Information Security Processes
- Managing Employee Benefits and Rights Processes
- Managing Financial and Accounting Operations
- Planning Human Resources Processes
- Conducting/Promoting Business Activities
- Providing Information to Authorized Persons, Companies, and Institutions
- Making necessary legal notifications to official institutions, benefiting from incentives, and reporting to relevant authorities within the scope of official audits
- Conducting human resources operations and specifically personnel activities
- Ensuring employee monitoring and conducting necessary data processing activities within the employer's management rights

For Job Applicants:

- Conducting Selection and Placement Processes for Applicants Submitting Job Application Forms
- Managing Job Application Processes
- Conducting human resources operations, particularly recruitment processes
- Ensuring Business Continuity and Physical Security
- Managing Recruitment Policies and Employment and Contract Processes within the scope of human resources operations
- Tracking Requests/Complaints
- Managing Information Security Processes

- Conducting Internal Audits/Investigations/Intelligence Activities
- Conducting Activities in Compliance with Legislation
- Providing Information to Authorized Persons, Institutions, and Organizations
- Managing Emergency Response Processes
- Conducting Communication Activities
- Conducting activities with legal, technical, and administrative consequences

For Interns/Students:

- Tracking Requests/Complaints
- Managing Information Security Processes
- Conducting Internal Audits/Investigations/Intelligence Activities
- Conducting Activities in Compliance with Legislation
- Providing Information to Authorized Persons, Institutions, and Organizations
- Managing Emergency Response Processes
- Conducting Communication Activities
- Ensuring Business Continuity
- Conducting activities with legal, technical, and administrative consequences
- Regulating and Monitoring Employment Relationships
- Ensuring Physical Security of the Premises
- Ensuring Business Continuity Activities
- Receiving and Evaluating Suggestions for Improving Business Processes
- Ensuring the Security of Movable Assets and Resources

Security of Data Controller Operations:
Conducting Occupational Health and Safety Activities,
Executing Payroll Payments.

For Shareholders/Business Partners/Supplier Companies:
Personal data belonging to your company's authorized personnel and employees may be processed within the scope of the commercial relationship between you and the “COMPANY,” in accordance with the provisions of Article 5 of the Law, for the following purposes, in compliance with the fundamental principles set forth in the Law, including the conditions for personal data processing:

- Executing supply chain management processes.
- Performing functions such as corporate resource planning, reporting, and marketing.

- Executing investment and marketing processes for products/services.
- Determining risk limits and conducting collateralization studies.
- Carrying out necessary quality, confidentiality, and standard audits.
- Fulfilling requirements set by laws and regulations (tax legislation, consumer protection legislation, obligations under the law of obligations, commercial law, customs law, legislation on electronic communication, etc.).
- Meeting obligations related to e-invoicing, e-delivery notes, and e-archiving.
- Complying with requests from public institutions and organizations as required or mandated by legal regulations.
- Fulfilling legal obligations specified in the Personal Data Protection Law (KVKK).
- Ensuring the security of Data Controller Operations.
- Securing movable property and resources.
- Tracking requests/complaints.
- Conducting storage and archiving activities.
- Managing advertising/campaign/promotion processes.
- Executing performance evaluation processes.
- Conducting marketing analysis activities.
- Managing organization and event activities.
- Implementing customer satisfaction activities.
- Managing customer relationship management processes.
- Executing production and operational processes for goods/services.
- Executing sales processes for goods/services.
- Authentication and record creation.
- Signing contracts and conducting negotiations with the “COMPANY.”
- Executing contract processes and providing information related to the “COMPANY.”
- Conducting strategic planning activities and risk management processes.
- Executing communication activities.
- Conducting internal audits/investigations/intelligence activities.
- Managing loyalty processes related to companies/products/services.
- Ensuring the physical security of the premises.
- Providing post-sale support services for goods/services.

- Managing information security processes.

For Customers:

- Managing customer relationship management processes.
- Ensuring the physical security of the premises.
- Conducting operations and activities under commercial/contractual relationships and fulfilling financial and legal obligations.
- Promoting and marketing products and services and contacting you regarding them.
- Tracking requests/complaints.
- Fulfilling warranty obligations under the producer's responsibility.
- Ensuring and monitoring the quality, information security, and confidentiality policies and standards of the “COMPANY.”
- Recording and tracking payment-related information.
- Preparing reports and analyses for senior management.
- Conducting customer satisfaction activities.
- Managing customer relationship management processes.
- Executing production and operational processes for goods/services.
- Executing sales processes for goods/services.
- Providing post-sale support services for goods/services.
- Managing purchasing processes for goods/services.
- Executing logistics activities.
- Conducting internal audits/investigations/intelligence activities.
- Managing loyalty processes related to companies/products/services.
- Managing information security processes.
- Fulfilling requirements set by laws and regulations (tax legislation, social security legislation, law of obligations, commercial law, consumer protection law, legislation on electronic communication, etc.).
- Executing sales processes for goods/services.
- Complying with requests from public institutions and organizations as required or mandated by legal regulations.
- Fulfilling legal obligations specified in the law.

For Potential Customers:
Your identity and contact information obtained directly from you through visits to the “COMPANY” premises, requests for orders and price quotes, complaints, and business cards

shared at fairs and events (data on the business card is considered anonymized) are processed in accordance with Article 5/2 of the Law to create offers for requested products, establish contracts, and manage your requests and complaints. Additionally, if you are not a trader or merchant, your information may be processed for marketing purposes to keep you informed about the "COMPANY"'s products and services and offer you special products with your consent.

For Visitors:
During your visits to the "COMPANY," our website, and other business locations, your identity and visual data may be processed for the following purposes to ensure the security of both the "COMPANY" and yourselves, as well as to fulfill our legal obligations and legitimate interests, through security cameras and visitor registration logs:

- Conducting audits/ethical activities.
- Managing information security processes.
- Ensuring physical security of the premises.
- Providing information to authorized persons, companies, and organizations.
- Ensuring the security of Data Controller Operations.
- PRINCIPLES TO BE FOLLOWED IN DATA PROCESSING
  3.1. Principles Regarding the Processing of Personal Data
  Your personal data is processed by the "COMPANY" in accordance with the principles of personal data processing set forth in Article 4 of the Law. The "COMPANY" prioritizes processing your personal data in a manner that is lawful, fair, and limited to the purpose of data processing. Data owners are granted the right to request the correction or deletion of their inaccurate or outdated data to ensure that personal data remains accurate and up-to-date.

"COMPANY" evaluates the processing of personal data for each category of data subject in accordance with specific, clear, and legitimate purposes. The "COMPANY" ensures that personal data is deleted, destroyed, or anonymized after the purpose of data processing ceases to exist or after the duration specified by law has expired.

3.2. Conditions for Processing Personal Data

In accordance with Article 5, paragraph 2, and Article 8, paragraph 2 of the Personal Data Protection Law (KVKK), personal data may be processed without the explicit consent of the data subject under the following conditions:

- When it is directly related to the establishment of a contract and the performance of services,
- In cases explicitly provided for by laws, where processing data is necessary for the establishment, exercise, or protection of a right,
- When it is necessary for the "COMPANY" to fulfill its legal obligations,
- In cases where processing is necessary for the legitimate interests of the "COMPANY," provided that it does not harm the fundamental rights and freedoms of the other party (visitor, employee, job candidate, business partner),

- In cases where a person is unable to provide consent due to actual impossibility, and processing is necessary to protect the life or physical integrity of that person or another person,
- If the personal data requested is made public by the person themselves, this data will be processed and transferred by the “COMPANY” as accurate and up-to-date.

3.3. Conditions for Processing Special Categories of Personal Data

Special categories of personal data, as defined in Article 6 of the Law, are limited to the following: race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, membership in associations, foundations or trade unions, health, sexual life, criminal convictions, security measures, as well as biometric and genetic data.

The “COMPANY” can process your special categories of personal data by taking necessary precautions under the following circumstances:

- Special categories of personal data, excluding health and sexual life, can be processed with the explicit consent of the data subject or when explicitly provided for by laws.
- Health and sexual life-related personal data can be processed without the explicit consent of the data subject by individuals or authorized companies and organizations that are under a confidentiality obligation, solely for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, and planning and managing health services and financing.

4. METHODS AND LEGAL REASON FOR COLLECTING YOUR PERSONAL DATA

Your personal data may be collected through various physical, auditory, and electronic means such as website visits, establishment and performance of contracts, recruitment processes, visits to our workplaces, and calls to customer service. Depending on the nature of the personal data and its purpose of processing, it will be collected in accordance with Article 5, paragraph 2 of the Law. If no legal basis exists, your data will be collected with your explicit consent. Your personal data may be collected, processed, and transferred through fully automated, partially automated, or non-automated methods based on the legal reasons outlined below:

- As provided by local or foreign legislation applicable to the “COMPANY,”
- When necessary for the establishment or performance of a contract directly related to the parties involved, processing of personal data is required to provide requested products and services or fulfill the contracts you have entered into,
- When processing data is necessary for the “COMPANY” to fulfill its legal obligations,
- If it has been made public by you,
- When processing is necessary for the establishment, exercise, or protection of a right as required by law or internal practice of the “COMPANY,”
- When processing is necessary for the legitimate interests of the “COMPANY,” provided that it does not harm your fundamental rights and freedoms.

5. TRANSFER OF PERSONAL DATA

In accordance with the conditions set forth in Articles 8 and 9 of the KVKK and additional regulations determined by the Personal Data Protection Board, personal data may be transferred

domestically or internationally if the conditions for the transfer of personal data exist.

The transfer of personal data to third parties within the country is permitted by the "COMPANY" only if at least one of the data processing conditions outlined in Articles 5 and 6 of the Law and explained in Section 3 of this Policy exists, and provided that the basic principles regarding data processing are adhered to.

The transfer of personal data to third parties outside the country can occur if at least one of the data processing conditions outlined in Articles 5 and 6 of the Law exists and if the basic principles regarding data processing are followed, even if the person does not provide explicit consent.

In accordance with the general principles of the Law and the data processing conditions in Articles 8 and 9, the "COMPANY" may transfer data to the following real and legal persons:

- Third-party service providers engaged for services (software, corporate resource planning, reporting, marketing, etc.) strictly related to the provision, promotion, and execution of products and services, as well as for promotions and campaigns in collaboration with and/or through service partners and suppliers.
- Audit firms, independent audit firms, customs companies, financial advisors/accounting firms, and law offices that are legally authorized to receive information and documents from the "COMPANY" within a limited scope.
- Service providers operating domestically and abroad who process data on behalf of the "COMPANY" (providing IT support, customer satisfaction measurement, profiling and segmentation support, and assistance in processing personal data in areas such as SMS, mailing, archiving, etc.).
- Providers necessary for processing your orders, managing your account, conducting commercial activities, and ensuring continuity.
- Banks and payment system companies for payment services, risk limit determination, collateralization, and debt restructuring purposes.
- Audit firms and information security firms necessary for conducting quality, confidentiality, and standard audits.
- Public institutions and organizations for fulfilling legal requirements and/or responding to official requests.

6. NOTIFICATION OF DATA SUBJECTS AND THEIR RIGHTS

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

- To learn whether your personal data has been processed,
- To request information regarding your processed personal data,
- To learn the purpose of processing your personal data and whether it is used in accordance with that purpose,
- To know the third parties to whom your personal data is transferred within the country,
- To request the correction of your personal data in case of incomplete or incorrect

processing, and to request that the action taken in this regard is communicated to third parties to whom your personal data has been transferred.

6. Rights of Data Subjects (continued)

- To request the deletion or destruction of personal data when the reasons for processing cease to exist, even if the data has been processed in accordance with the Law and other relevant legal provisions, and to request that the action taken in this regard be communicated to third parties to whom your personal data has been transferred.
- To object if a result that is against you arises solely from the automated analysis of processed data.
- To request compensation for damages incurred due to unlawful processing of your personal data.

7. Ensuring the Security and Confidentiality of Personal Data

The "COMPANY" takes all necessary measures to prevent unlawful disclosure, access, transfer, or any security deficiencies that may arise concerning personal data, based on the nature of the data to be protected. In this context, the "COMPANY" implements all necessary administrative and technical measures, establishes a monitoring system within the organization, and acts in accordance with the measures prescribed in the KVKK in the event of unauthorized disclosure of personal data.

8. Destruction of Personal Data

The "COMPANY" has prepared a DESTRUCTION POLICY that specifies the methods for destroying personal data. All destruction processes are conducted in accordance with this policy. According to Article 7 of the Law, if the reasons for processing cease to exist, personal data that has been lawfully processed will be deleted, destroyed, or anonymized either ex officio or upon the request of the relevant person, in accordance with the data protection and destruction policy specially prepared for this purpose, applicable legislation, and the guidelines published by the "COMPANY." The retention periods for each type of data and process are clearly stated in the personal data inventory prepared by the "COMPANY," which governs all data processing processes.

In accordance with Article 7 of the Law, if the reasons for processing cease to exist, personal data will be deleted, destroyed, or anonymized by the "COMPANY" either ex officio or upon the request of the relevant person in accordance with the guidelines published by the "COMPANY."

9. Matters Concerning the Protection of Personal Data

"HERA CHARGE" takes the necessary technical and administrative measures to ensure an appropriate level of security to prevent unlawful processing of personal data, unlawful access to data, and to ensure the protection of data in accordance with Article 12 of the KVKK.

9.1. Technical Measures

The main technical measures taken by "HERA CHARGE" to ensure the lawful processing of personal data are as follows:

- The "COMPANY" utilizes external data storage offline.
- Personal data stored in external data storage is encrypted.

- Regular backups of systems containing data are taken and reported.
- File sharing containing personal data with external individuals or entities is done securely. Sensitive personal data transferred on portable drives, CDs, and DVDs is encrypted during transfer.
- The “COMPANY” has two physical servers, and virtualization is employed.
- Security measures are taken regarding the physical security of personal data environments, and measures against external risks (such as fire, flooding, etc.) are implemented.
- Employees of the “COMPANY” cannot access the system using personal devices.
- An authorization matrix has been established for employees, defining which employee can access which information and the limits of their authority. Employees who change roles or leave the organization have their access rights revoked.
- Personal data is backed up, and the security of the backed-up data is ensured.
- The software on servers is up to date and licensed.
- Anti-virus software and hardware on the devices are current.
- There is no department for the procurement, development, and maintenance of IT systems within the “COMPANY”; services are procured from outside.
- Access log records are maintained regularly, and data masking measures are applied when necessary.
- A firewall is installed on the systems within the “COMPANY.”
- External users/guests cannot access information sources when they log into the system.
- Active Directory or user account management and access control systems are utilized by the “COMPANY.”
- Log records are kept in a way that user intervention is not possible.
- Files and programs containing personal data are encrypted.
- Data loss prevention software is used within the “COMPANY.”
- There is no personal data on the “COMPANY” website.

9.2. Administrative Measures

The main administrative measures taken by “HERA CHARGE” to ensure the lawful processing of personal data are as follows:

- Employees of the “COMPANY” are informed and trained about personal data protection laws and the lawful processing of personal data.
- All personal data processing activities conducted by the “COMPANY” are carried out in accordance with the personal data inventory and its annexes, which are created by analyzing all business units in detail.

- The personal data processing activities of the relevant departments within the “COMPANY” are bound by written policies and procedures to ensure compliance with the conditions required by the KVKK, and each business unit has been informed about the relevant issues to be considered in the specific activities it conducts. Protocols and procedures for the security of special categories of personal data have been defined and implemented.
- The monitoring and management of personal data security within the “COMPANY” are organized by the Personal Data Protection Committee. Awareness is raised regarding the legal requirements determined for each business unit, and the necessary administrative measures are implemented through internal policies, procedures, and training to ensure compliance and continuity of application. Periodic and/or random internal audits are conducted.
- Records related to personal data security and confidentiality are included in service contracts and related documents between the “COMPANY” and employees, and additional protocols are established. Awareness-raising activities have been conducted for employees regarding this matter. Access rights are revoked for employees who change roles or leave the organization.
- Personal data security issues are reported promptly, and monitoring of personal data security is conducted.
- Necessary security measures are taken regarding access to physical environments containing personal data, ensuring the security of these environments against external risks (such as fire, flooding, etc.).
- The “COMPANY” minimizes the personal data processed as much as possible.
- Confidentiality agreements are established by the “COMPANY.”
- Monitoring of personal data security is carried out, and internal periodic and/or random audits are conducted.

10. Communication

You can submit your requests regarding your rights listed above by filling out the "Relevant Person Application Form" available on our website (www.heracharge.com) or by sending a written document with the same content to the address specified below. All your requests can be communicated in writing to the postal addresses provided below. When data subjects (relevant persons) submit requests related to their personal data in writing to “HERA CHARGE,” the “COMPANY” carries out the necessary processes to ensure that the request is concluded in accordance with Article 13 of the KVKK, as soon as possible and no later than thirty (30) days, depending on the nature of the request.

The “COMPANY” may request information to verify whether the person making the application is the owner of the personal data in question for the sake of ensuring data security. The “COMPANY” may also ask questions related to the application to ensure that the relevant person’s request is concluded appropriately. In cases where fulfilling the request may impede the rights and freedoms of other individuals, require disproportionate effort, or involve publicly available information, the “COMPANY” may deny the request with an explanation of the reasons.

HERA CHARGE ELEKTRONİK A.Ş.

(Mersis: 0461 1117 5740 0001)

Address: Güllübağlar Mah. Firketeci Sk. No: 2 P.K:34906 Pendik/İSTANBUL
Tel & Fax: +90 216 307 11 00 & +90 216 307 79 02
Kep Address: heracharge@hs01.kep.tr
Email: info@heracharge.com
Web: www.heracharge.com