Protection of Personal Data and Processing Policy

1. PURPOSE AND SCOPE

The Datacore Personal Data Processing and Protection Policy ("Datacore Data Protection Policy") sets out the principles adopted by Datacore in the protection and processing of personal data.

In line with the importance Datacore attaches to the protection of personal data, the fundamental principles for ensuring compliance with the regulations set out in the Personal Data Protection Law No. 6698 ("Data Protection Law") in the activities carried out by Datacore and its business partners are determined, and what Datacore must do within this scope is put forward. The application of the Datacore Data Protection Policy regulations will make the data security principles adopted by Datacore sustainable.

2. OBJECTIVE

Datacore should create the necessary system to ensure awareness of personal data protection within the company and establish the necessary order to ensure compliance with the legislation on the protection and processing of personal data in internal operations.

The Datacore Data Protection Policy aims to guide the implementation of the regulations set out in the Data Protection Law and related legislation. With the Datacore Data Protection Policy, it is aimed to ensure the adoption and careful execution of the compliance process with the Data Protection Law, which is valued by Datacore.

3. DEFINITIONS

The definitions used and deemed significant in the Datacore Data Protection Policy are listed below:

- **Explicit Consent:** Consent based on information and expressed with free will regarding a specific issue.
- **Anonymization:** Rendering personal data in a way that it can no longer be associated with an identifiable or identifiable natural person, even if matched with other data.
- **Communiqué on the Principles and Procedures for Fulfilling the Obligation to Inform:** Communiqué on the Principles and Procedures for Fulfilling the Obligation to Inform, published in the Official Gazette dated March 10, 2018, and numbered 30356.
- **Employee Data Protection Policy:** The "Datacore Information Systems Industry and Trade Inc. Employee Personal Data Protection and Processing Policy" regulating the principles for the protection and processing of Datacore employees' personal data.
- **Regulation on the Processing of Personal Health Data:** Regulation on the Processing and Protection of Privacy of Personal Health Data, published in the Official Gazette dated October 20, 2016, and numbered 29863.
- **Personal Health Data:** All kinds of information related to the physical and mental health of an identifiable or identifiable natural person and information regarding the health service provided to the person.
- **Personal Data:** Any information relating to an identified or identifiable natural person.

- **Data Subject:** The natural person whose personal data is processed. For example, customers and employees.
- **Personal Data Protection Unit:** The unit within Datacore that will ensure the necessary coordination within the company for compliance with, preservation, and maintenance of the personal data protection legislation.
- **Processing of Personal Data:** Any operation performed on personal data, such as collecting, recording, storing, maintaining, altering, reorganizing, disclosing, transferring, taking over, making it obtainable, classifying, or preventing its use, by fully or partially automated means or non-automated means provided that they are part of a data recording system.
- **Data Protection Law:** Personal Data Protection Law No. 6698, published in the Official Gazette dated April 7, 2016, and numbered 29677.
- **Data Protection Board:** Personal Data Protection Board.
- **Data Protection Authority:** Personal Data Protection Authority.
- **Special Categories of Personal Data:** Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership of associations, foundations, or trade unions, health, sexual life, criminal convictions, and security measures, as well as biometric and genetic data.
- **Datacore/Company:** Datacore Information Systems Industry and Trade Inc.
- **Datacore Business Partners:** Parties with whom Datacore has established business partnerships for various purposes while conducting its commercial activities.
- **Datacore Data Protection Policy:** The "Datacore Information Systems Industry and Trade Inc. Personal Data Protection and Processing Policy."
- **Datacore Suppliers:** Parties providing services to Datacore based on a contractual relationship.
- **Datacore Data Subject Application Form:** The application form that data subjects will use for their applications regarding their rights listed in Article 11 of the Data Protection Law.
- **Legal Advisors:** Real and legal persons from whom Datacore Information Systems Industry and Trade Inc. receives consultancy for the execution of legal transactions.
- **Datacore Employee Data Protection Policy:** The "Datacore Employee Personal Data Protection and Processing Policy" regulating the principles adopted for the protection and processing of personal data of employees of companies affiliated with Datacore.
- **Constitution of the Republic of Turkey:** Constitution of the Republic of Turkey, published in the Official Gazette dated November 9, 1982, and numbered 17863; dated November 7, 1982, and numbered 2709.
- **Turkish Penal Code:** Turkish Penal Code, published in the Official Gazette dated October 12, 2004, and numbered 25611; dated September 26, 2004, and numbered 5237.
- **Data Processor:** A natural or legal person who processes personal data on behalf of the data controller based on the authority given by the data controller.
- **Data Controller:** A person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.
- **Communiqué on the Procedures and Principles of Application to the Data Controller:** Communiqué on the Procedures and Principles of Application to the Data Controller, published in the Official Gazette dated March 10, 2018, and numbered 30356.

- **Data Controllers' Registry:** Data Controllers' Registry, kept by the Presidency of the Personal Data Protection Authority under the supervision of the Data Protection Board and publicly available.
- **Regulation on the Data Controllers' Registry:** Regulation on the Data Controllers' Registry, published in the Official Gazette dated December 30, 2017, and numbered 30286, which entered into force on January 1, 2018.

4. RESPONSIBILITIES

The regulations, procedures, guidelines, standards, and training activities prepared in accordance with the Datacore Data Protection Policy will be applied within Datacore. Legal Advisors will be the source of advice and guidance. All employees, stakeholders, guests, visitors, and related third parties across Datacore are obliged to cooperate with Legal Advisors in ensuring compliance with the Datacore Data Protection Policy and preventing legal risks and imminent danger. All organs and departments of Datacore are responsible for ensuring compliance with the Datacore Data Protection Policy.

5. POLICY PRINCIPLES

5.1. BASIC PRINCIPLES ADOPTED BY DATACORE

Datacore must adopt the following basic principles to ensure and maintain compliance with personal data protection legislation:

5.1.1. Processing Personal Data in Accordance with the Law and the Rules of Honesty

Datacore must carry out personal data processing activities in accordance with the personal data protection legislation, primarily the Constitution of the Republic of Turkey, and the rules of law and honesty.

5.1.2. Ensuring the Accuracy and Up-to-dateness of Processed Personal Data

Datacore must ensure the accuracy and up-to-dateness of the processed personal data and must take the necessary administrative and technical measures and carry out the necessary processes in this context. Datacore must establish mechanisms to correct and verify the accuracy of personal data if it is inaccurate.

5.1.3. Processing Personal Data in a Connected, Limited, and Measured Manner

Datacore must process personal data in a manner connected to, limited to, and proportionate to the data processing conditions. This requires determining the purpose of the data processing before starting the data processing activity. In other words, personal data must not be processed (including data retention) with the assumption that it may be used in the future. Datacore must consider the fundamental rights of data subjects and their legitimate interests.

5.1.4. Retaining Personal Data for the Period Stipulated in the Relevant Legislation or Required for the Purpose for Which They Are Processed

Datacore must retain personal data for the period stipulated in the relevant legislation or required for the purpose for which they are processed. In this context, Datacore must comply

with the time limits stipulated by Article 138 of the Turkish Penal Code and Articles 4 and 7 of the Data Protection Law. Datacore must delete, destroy, or anonymize personal data when the time period stipulated in the legislation expires or when the reasons for processing personal data no longer exist.

5.2. COMPLIANCE WITH PERSONAL DATA PROCESSING CONDITIONS

Datacore must act in accordance with the data processing conditions set out in Articles 5 and 6 of the Data Protection Law and the Regulation on the Processing of Personal Health Data, while conducting personal data processing activities, provided that they comply with the basic principles.

Datacore must determine whether the data processing conditions exist for the personal data processing activities conducted and must not conduct personal data processing activities if the conditions do not exist.

Datacore must establish the necessary mechanisms within their internal systems to ensure the lawful processing of personal data, raise internal awareness regarding personal data protection, and implement the necessary audit mechanisms.

Datacore must comply with the rules set out in the Constitution of the Republic of Turkey, the Turkish Penal Code, the Data Protection Law, and other relevant legislation, as well as the Datacore Data Protection Policy, within the scope of personal data processing activities.

5.3. COMPLIANCE WITH PERSONAL DATA TRANSFER CONDITIONS

Datacore must comply with the personal data transfer conditions stipulated in Articles 8 and 9 of the Data Protection Law while conducting personal data transfers (actively sharing personal data with third parties or making personal data accessible to third parties).

5.4. ENSURING THE SECURITY OF PERSONAL DATA

Datacore must take all necessary measures within the scope of available means and in accordance with the nature of the data to be protected to prevent the unlawful disclosure, transfer, access, or other security deficiencies that may occur concerning personal data.

In this context, Datacore must take necessary (i) administrative and (ii) technical measures, establish (iii) an audit system within the company, and take the measures stipulated in the Data Protection Law in case of unlawful disclosure of personal data.

5.4.1. Administrative Measures to Ensure Lawful Processing and Prevent Unlawful Access to Personal Data

- Datacore must train and raise awareness among its employees regarding the protection of personal data.
- In cases where personal data is subject to transfer, Datacore must include provisions in the contracts concluded with the parties to whom the personal data is transferred, ensuring that the transferred party will fulfill its obligations to ensure data security and undertake to take all necessary measures and implement these measures within their organization.

- Datacore must thoroughly examine the processes it conducts, identify the personal data processing activities carried out within each unit, and determine the steps to be taken to ensure compliance with the personal data processing conditions stipulated in the Data Protection Law.
- Datacore must identify the necessary practices to ensure compliance with the Data Protection Law according to their organizational structures and regulate these practices through internal policies.

5.4.2. Technical Measures to Ensure Lawful Processing and Prevent Unlawful Access to Personal Data

- Datacore must take technical measures to the extent allowed by technology to ensure the protection of personal data and update and improve these measures in line with developments.
- Datacore must employ expert personnel in technical matters.
- Datacore must conduct regular audits to ensure the implementation of the measures taken.
- Datacore must establish software and systems to ensure security.
- Datacore must restrict access to personal data processed by Datacore to the relevant company employee according to the specified processing purpose.

5.4.3. Datacore's Audit Activities Related to Personal Data Protection

The compliance, functionality, and effectiveness of the technical and administrative measures and applications taken by Datacore to ensure the protection and security of personal data must be audited by Datacore's Internal Audit Units. Datacore may carry out the audit activity with its organization or outsource it to external audit firms by obtaining the opinion of the Datacore Board of Directors. If deemed necessary, the Datacore Board of Directors may directly carry out the audit activity within Datacore with its organization.

The results of the audit activities must be reported to the relevant Datacore Board of Directors and the relevant function managers. The planned actions related to the audit results must be regularly followed up by the process owners. The relevant Datacore must follow up, verify, and audit the actions taken within the scope of this report.

In addition to the audit results, the activities aimed at improving and enhancing the measures taken for the protection of personal data must be carried out by the relevant executive units within Datacore.

5.4.4. Measures to Be Taken in Case of Unlawful Disclosure of Personal Data

Datacore must notify the Data Protection Board and the relevant data subjects as soon as possible if personal data is unlawfully obtained by unauthorized persons. The necessary internal structure to fulfill this obligation must be established within each Datacore.

5.5. OBLIGATIONS REGARDING PERSONAL DATA PROCESSING ACTIVITIES

Datacore must comply with the obligations stipulated for data controllers in the Data Protection Law. The main issues that Datacore must comply with are listed below:

5.5.1. Obligation to Register and Notify the Data Controllers' Registry

Datacore must register with the Data Controllers' Registry in accordance with Article 16 of the Data Protection Law and the procedures and principles of the Regulation on the Data Controllers' Registry.

The information that must be submitted to the Data Controllers' Registry during the registration application is as follows:

1. The identity and address information of Datacore as the data controller and, if any, its representative,
2. The purpose of processing personal data,
3. Information on the groups of data subjects and the categories of personal data processed for these persons,
4. The persons or groups of persons to whom personal data may be transferred,
5. Personal data that may be transferred abroad,
6. The measures taken to ensure the security of the processed personal data,
7. The maximum retention period required for the purpose of processing personal data.

5.5.2. Obligation to Inform the Data Subject

Datacore must carry out the necessary processes to ensure that data subjects are informed during the collection of personal data, in accordance with Article 10 of the Data Protection Law and the Communiqué on the Principles and Procedures for Fulfilling the Obligation to Inform. The information that must be provided to data subjects within the scope of the obligation to inform is as follows:

1. The identity of the data controller and, if any, its representative,
2. The purpose for which personal data will be processed,
3. The persons to whom the processed personal data may be transferred and the purpose for which they may be transferred,
4. The method and legal reason for collecting personal data,
5. The rights of the data subject, which are:

- To learn whether personal data is processed or not,
- To request information if personal data has been processed,
- To learn the purpose of processing personal data and whether they are used in accordance with their purpose,
- To know the third parties to whom personal data is transferred domestically or abroad,
- To request the correction of personal data in case of incomplete or incorrect processing and to request the notification of the correction to the third parties to whom the personal data has been transferred,
- To request the deletion or destruction of personal data, despite being processed in accordance with the provisions of the Data Protection Law and other relevant laws, in the event that the reasons requiring processing are no longer valid, and to request the notification of the deletion or destruction to the third parties to whom the personal data has been transferred,
- To object to the occurrence of a result against the person himself by analyzing the processed data exclusively through automated systems,

- To request the compensation of the damage in case of damage due to the unlawful processing of personal data.

5.5.3. Obligation to Ensure the Security of Personal Data

Datacore must take all necessary technical and administrative measures to ensure the appropriate level of security to prevent the unlawful processing, unlawful access, and safeguarding of personal data, in accordance with Article 12 of the Data Protection Law.

Datacore must also carry out or have carried out the necessary audits within the scope of operating the mechanisms to ensure data security.

5.5.4. Obligation to Comply with the Decisions of the Personal Data Protection Board

Datacore must act in accordance with the decisions of the Personal Data Protection Board, which operates as the executive body of the Data Protection Authority to ensure that personal data is processed in compliance with fundamental rights and freedoms.

5.5.5. Obligation to Respond to Data Subject Applications

Datacore, as a data controller, must conclude the requests of data subjects regarding their personal data as soon as possible and within thirty (30) days at the latest, depending on the nature of the request, in accordance with Article 13 of the Data Protection Law. Data subjects must submit their requests regarding their personal data in accordance with the Communiqué on the Procedures and Principles of Application to the Data Controller.

In accordance with Article 11 of the Data Protection Law, personal data subjects can make requests to data controllers regarding the following matters:

1. To learn whether their personal data is processed or not,
2. To request information if their personal data has been processed,
3. To learn the purpose of processing personal data and whether they are used in accordance with their purpose,
4. To know the third parties to whom personal data is transferred domestically or abroad,
5. To request the correction of personal data in case of incomplete or incorrect processing and to request the notification of the correction to the third parties to whom the personal data has been transferred,
6. To request the deletion or destruction of personal data, despite being processed in accordance with the provisions of the Data Protection Law and other relevant laws, in the event that the reasons requiring processing are no longer valid, and to request the notification of the deletion or destruction to the third parties to whom the personal data has been transferred,
7. To object to the occurrence of a result against the person himself by analyzing the processed data exclusively through automated systems,
8. To request the compensation of the damage in case of damage due to the unlawful processing of personal data.

5.5.6. Obligation to Transfer and Obtain Personal Data Lawfully

Datacore must process personal data lawfully and fairly, in accordance with Article 4 of the Data Protection Law. This includes the activities of obtaining and transferring personal data.

5.5.7. Obligation to Comply with Regulations on the Retention of Personal Data

Datacore must establish the necessary internal systems to ensure the deletion, anonymization, or destruction of personal data, despite being processed lawfully, when the reason for processing no longer exists, in accordance with Article 7 of the Data Protection Law.

6. MAIN ISSUES TO BE IMPLEMENTED BY DATACORE COMPANIES TO COMPLY WITH THE DATACORE DATA PROTECTION POLICY AND THE PERSONAL DATA PROTECTION LAW

Datacore must establish certain systems within its organization to ensure compliance with the Data Protection Law and the guiding Datacore Data Protection Policy. The primary issues that Datacore must implement are listed below:

6.1. IMPLEMENTING THE OBLIGATIONS EXPLAINED IN THE DATACORE DATA PROTECTION POLICY

Datacore must act in accordance with the fundamental obligations explained under the title 5.5. of the Datacore Data Protection Policy.

6.2. CREATING THE BASIC POLICIES FOR PERSONAL DATA PROTECTION AND PROCESSING

Datacore must create the Personal Data Protection and Processing Policy by considering its internal operations and the regulations set out in the Data Protection Law.

The language of this policy, created by Datacore, must be simple and understandable by data subjects.

6.3. PREPARING POLICIES, REGULATIONS/INTERNAL REGULATIONS, PROCEDURES, AND GUIDELINES RELATED TO PERSONAL DATA PROTECTION AND PROCESSING

To ensure compliance with personal data protection law, Datacore must prepare the necessary documents for public disclosure or internal use.

These documents must be prepared in accordance with the documentation model implemented by Datacore.

Changes in the policies to be disclosed to the public by Datacore must be made accessible to data subjects easily.

6.4. IDENTIFYING THE UNIT RESPONSIBLE FOR PERSONAL DATA PROTECTION AND PROCESSING

A Personal Data Protection Unit must be established within each Datacore organization, or a person responsible for the protection and processing of personal data must be appointed. The primary activities to be carried out by the relevant unit or person are listed below:

(1) Monitoring the preparation of documentation related to the protection and processing of personal data and submitting the documents for approval, (2) Ensuring the implementation of documents related to the protection and processing of personal data and conducting necessary audits, (3) Monitoring whether Datacore fulfills its obligations (Datacore Data Protection Policy Title 5.5.), (4) Monitoring the relations with the Data Protection Authority and the Data Protection Board.

The formation and task distribution of the unit will be determined by Datacore's top management. If it is decided to appoint a person responsible for the protection and processing of personal data instead of establishing a unit, the appointment process will be carried out by the company's top management. In addition to the minimum tasks mentioned above, additional duties and responsibilities may be assigned to the unit and the appointed responsible person, considering Datacore's needs and activities.

7. REVIEW

This Policy document will come into effect upon approval by the Datacore Board of Directors. Apart from the issue of abolishing this Policy, the Datacore Board of Directors has authorized the Chairman of the Board to make changes to this Policy and put it into effect. Changes to this Policy can be made and put into effect with the approval of the Chairman of the Datacore Board of Directors.

Implementation rules to specify how certain issues mentioned in this Policy will be carried out will be regulated as regulations. The regulations will be published and put into effect with the approval of the Chairman of the Datacore Board of Directors.

This Policy will be reviewed at least once a year, and necessary changes will be updated and submitted for approval by the Chairman of the Datacore Board of Directors if required.

The Datacore Data Protection Policy has been published on Datacore's website and presented to the public. In case of a conflict between the regulations in this Policy and the applicable legislation, the provisions of the legislation will apply.

Datacore reserves the right to make changes to the Datacore Data Protection Policy in parallel with legal regulations. The current version of the Datacore Data Protection Policy is accessible on Datacore's website (www.datacore.com.tr).