PERSONAL DATA PROCESSING AND PROTECTION POLICY

PREPARED BY	APPROVED BY
HUMAN RESOURCES DEPARTMENT AND LEGAL DEPARTMANT	IMS Officer

DOC.NO:HİTİT_PR_52-1 REV.05 / REV DATE: 01/07/2026 /RELEASE DATE: 15/05/2018

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

Table of Contents

PART ONE 4
§ 1. INTRODUCTION 4
1.1. Introduction 4
1.2. Purpose of the Policy 4
1.3. Scope of the Policy and Personal Data Subjects 4
1.4. Definitions 6
1.5. Effectiveness of Policy 7
PART TWO 7
§ 2. PROCESSING AND TRANSFER OF PERSONAL DATA 7
2.1. General Principles for Processing Personal Data 7
2.2. Terms of Processing Your Personal Data 8
2.3. Conditions for Processing Special Categories of Personal Data 9
2.4. Conditions of Transfer of Personal Data 11
2.4.1. Conditions for Transferring Personal Data Abroad 11
2.5. Conditions for Transfer of Special Categories of Personal Data 13
2.5.1. Transfer of Special Categories of Personal Data Abroad 14
PART THREE 16
§ 3. CLASSIFICATION OF PERSONAL DATA, PURPOSES OF PROCESSING AND TRANSFER, PERSONS TO WHOM PERSONAL DATA WILL BE TRANSFERRED 16
3.1. Classification of Personal Data 16
3.2. Purposes of Processing and Transferring Personal Data 18
PART FOUR 20
§ 4. METHOD AND LEGAL GROUNDS FOR COLLECTING PERSONAL DATA, DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA AND RETENTION PERIOD 20
4.1. Method and Legal Reason for Collecting Your Personal Data 20
4.2. Erasure, Destruction or Anonymisation of Personal Data 20
4.3. Retention Period of Personal Data 21
PART FIVE 21

§ 5. CONSIDERATIONS REGARDING THE PROTECTION OF PERSONAL DATA 21
5.1. Securing Personal Data 22
5.1.1. Technical and Administrative Measures Taken to Ensure Lawful Processing of Personal Data 22
5.1.2. Technical and Administrative Measures Taken to Prevent Unlawful Access to Personal Data 23
5.1.3. Storing Personal Data in Secure Environments 24
5.1.4. Supervision of Measures Taken for the Protection of Personal Data 25
5.1.5. Measures to be taken in case of unauthorised disclosure of personal data 25
5.2. Observing the Legal Rights of Personal Data Subjects 25
5.3. Protection Special Categories of Personal Data 25
PART SIX 26
§ 6. RIGHTS, EXERCISE AND EVALUATION OF PERSONAL DATA SUBJECTS 26
6.1. Disclosure of Personal Data Subject 26
6.2. Rights of the Data Subject under the Law 26
6.3. Cases where the Personal Data Subject cannot assert his/her rights 27
6.4. Exercise of Rights by the Data Subject 28
6.5. Procedure and Duration of the Company's Response to Applications 28
6.6. Data Subject's Right to File a Complaint to the Board 28
PART SEVEN 29
§ 7. MANAGEMENT STRUCTURE IN ACCORDANCE WITH THE COMPANY'S POLICY ON PROCESSING AND PROTECTION OF PERSONAL DATA 29
PART EIGHT 29
§ 8. UPDATE, HARMONISATION AND AMENDMENTS 29
8.1. Update and Compliance 29

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

PART ONE

§ 1. INTRODUCTION

1.1. Introduction

As Hitit Bilgisayar Hizmetleri A.Ş. ("Hitit") and/or Hitit SAAS (hereinafter collectively referred to as the "Companies"), we attach utmost importance to the processing and protection of personal data in accordance with the Law No. 6698 on the Protection of Personal Data ("Law") and we act with this care in all our planning and activities. With this awareness, in order to fulfil the obligation of disclosure under Article 10 of the Law and to inform you of all administrative and technical measures we have taken within the scope of processing and protection of personal data,this Policy on Processing and Protection of Personal Data ("Policy") has been drawn up.

1.2. Purpose of the Policy

The main purpose of this Policy is to provide explanations on the systems for the processing and protection of personal data in accordance with the law and the purpose of the Law, in this context, the Stakeholder of the Companies, the Real Person Business Partner of the Companies (Employee, Employee Relatives, Consultant, Intern, ...) Stakeholder of the Companies' Business Partners, Officials, Employees, Company Officials, Employee Candidate, Customer of the Companies, Customers of the Companies' Customers to the extent that they process personal data, Potential Customers, Employees of Suppliers, Visitors, Third Parties (Employee Relatives, Partner....) to inform the persons whose personal data are processed by our Companies. In this way, it is aimed to ensure full compliance with the legislation in the processing and protection of personal data carried out by our Companies and to protect all rights of personal data subjects arising from the legislation on personal data.

1.3. Scope of the Policy and Personal Data Subjects

This Policy has been prepared for the persons whose personal data are processed by our Company by fully or partially automated means or by non-automated means provided that they are part of any data recording system and will be applied within the scope of these specified persons. As the data of legal entities are not considered as "personal data" in accordance with the relevant legislation, they are also excluded from the scope of this Policy.
Our Company informs the Personal Data Subjects about the Law by publishing this Policy on its website and presenting it to the data subjects upon their request. Employees of our Company sign the explicit consent text for the necessary transactions and are informed about the provisions in the Personal Data Protection Policy applied to them. This Policy shall not apply

if the data is not included in the scope of "Personal Data" within the scope specified below or if the Personal.

In this context, the relevant categories of persons within the scope of this Policy are as follows:

Company Stakeholder	**:**	Stakeholders of the Companies are real persons.
Company Real Person Business Partner (Employee, Employee Relatives, Consultant, Intern, ...)	**:**	Real persons with whom the Companies have all kinds of business relations.
Stakeholder, Officer, Employee of the Company's Business Partners	**:**	All real persons, including employees, Stakeholders and officials of real and legal persons (such as business partners, suppliers) with whom the Companies have all kinds of business relations.
Company Representative	**:**	Real persons who perform transactions on behalf and account of the Company based on verbal or written authorisation arising from the law or given by the Company.
Employee Candidate	**:**	Real persons who have applied for a job to the Company by any means or who have opened their CV and related information to the Company's review.
Company Customer	**:**	Real persons who use or have used the products and services offered by the Company, regardless of whether they have any contractual relationship with the Company.
Our Customers' Customers	**:**	Employees and passengers of airlines and tourism agencies
Potential Customer	**:**	They are real persons who have made a request or interest in using the products and services of the Companies or who have been evaluated in accordance with the commercial custom and honesty rules that they may have this interest.
Employees of Suppliers	**:**	Employees of supplier companies working together in the process
Visitor	**:**	All real persons who enter the physical premises owned by the Companies for various purposes or visit the websites for any purpose.
Third Party (Employee Relatives, Event Participant....	**:**	Other natural persons who are not included in the scope of the Personal Data Protection and Processing Policy prepared for the Employees of the Companies and who

		are not included in any category of data subjects in this Policy.

1.4. Definitions

The terms used in this Policy shall have the meanings set out below:

Companies / Our Companies	:	Hitit Bilgisayar Hizmetleri A.S. ("Hitit") and/or Hitit SAAS.
Personal Data/Data	:	Any information relating to a specific or identifiable natural person.
Special Categories of Personal Data	:	Biometric and genetic data and data related to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise, association or union membership, health, sex life, criminal conviction and security measures.
Processing of Personal Data	:	All kinds of processes performed on personal data including obtaining, recording, storing, keeping, changing, re-arranging, disclosure, transmission, acquisition, making available, classification or prevention of use in whole or in part, automatically or in non-automatic ways, being part of any data recording system
Data Subject	:	Company Stakeholder, Company Real Person Business Partner (Employee, Employee Relatives, Consultant, Intern, ...) Stakeholder, Official, Employee, Company Official, Employee Candidate, Company Customer, Customers of our Customers, Potential Customer, Employees of Suppliers, Visitor, Third Party (Employee Relatives, Partner....)
Data Recording System	:	It refers to the registration system where personal data is processed according to certain criteria.
Data Controller	:	Real or legal person responsible for identifying the purposes and methods of personal data processing and installing and managing data registry system.
Data Processor	:	The real or legal person who processes personal data on behalf of the data controller under the authority granted by the data controller.
Explicit Consent	:	Consent to a particular subject, based on information and disclosed with free will.

Anonymization	**:**	It is the process of making the data previously associated with a person impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.
Law	**:**	Refers to Personal Data Protection Law No. 6698.
Board	**:**	Personal Data Protection Board.
Authority:		Personal Data Protection Authority.

1.5. Effectiveness of Policy

It was issued by the Companies and entered into force on 15/05/2018. It is published on the website of the Companies (https://hitit.com/) and made available to the data subjects upon the request of the Personal Data Subjects. You can access Data Subject Application form via https://hitit.com/themes/hitit/documents/2026-02/ilgili-kisi-basvuru-formu.pdf URL connection.

PART TWO

§ 2. PROCESSING AND TRANSFER OF PERSONAL DATA

2.1. General Principles for Processing Personal Data

Personal Data is processed by the Company in accordance with the procedures and principles stipulated in the Law and this Policy. The Company acts with the following principles when processing Personal Data:

- Personal Data are processed in **accordance with the** relevant **rules of law and the requirements of good faith** .
- It is ensured that Personal Data is accurate and up-to-date. In this context, issues such as identifying the sources from which the data are obtained, confirming their accuracy, and assessing whether they need to be updated are carefully considered.
- Personal Data is processed **for specific, explicit and legitimate purposes** . The legitimacy of the purpose means that the Personal Data processed by the Company is related to and necessary for the work it does or the service it provides.
- Personal Data is related to the purpose in order to achieve the purposes determined by the Company, and the processing of Personal Data that is not related to the realisation of the purpose or is not needed is avoided. It keeps the processed data limited only to what is necessary for the realisation of the purpose. Personal Data processed within this scope **are relevant, limited and proportionate to the purpose for which they are processed**.

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

- If there is a period stipulated in the relevant legislation for the storage of data, it complies with these periods; otherwise, it **retains** Personal Data only **for the period required for the purpose for which they are processed** . In the event that there is no longer a valid reason for the further preservation of Personal Data, such data shall be deleted, destroyed or anonymised.

2.2. Terms of Processing Your Personal Data

The Company does not process Personal Data without the explicit consent of the data subject. In the presence of one of the following conditions, Personal Data may be processed without seeking the explicit consent of the data subject.

- The Company may process the Personal Data of Personal Data Subjects in cases expressly stipulated by law, even without explicit consent. For example, pursuant to Article 230 of the Tax Procedure Law, the explicit consent of the data subject will not be sought in order to include the name of the data subject on the invoice.
- Personal Data may be processed without explicit consent in order to protect the life or physical integrity of persons who are unable to disclose their consent due to actual impossibility or whose consent cannot be validated, or of another person. For example, in a situation where the person is unconscious or mentally ill and his/her consent is not valid, the Personal Data of the person concerned may be processed during medical intervention in order to protect his/her life or body integrity. In this context, data such as blood type, previous illnesses and operations, and medications used can be processed through the relevant health system.
- Provided that it is directly related to the establishment or performance of a contract by the Company, Personal Data of the parties to the contract may be processed. For example, the account number of the creditor party may be obtained for the payment of money in accordance with a contract.
- The Company may process the Personal Data of Personal Data Subjects if it is mandatory to fulfil its legal obligations as a data controller.
- Personal Data made public by the Company by the Personal Data Subjects themselves, in other words, Personal Data disclosed to the public in any way, can be processed as the legal benefit to be protected has disappeared.
- The Company may process the Personal Data of Personal Data Subjects without seeking explicit consent in cases where data processing is mandatory for the exercise or protection of a legitimate right.
- The Company may process the Personal Data of Personal Data Subjects in cases where the processing of Personal Data is mandatory for the provision of legitimate interests, provided that it does not harm the fundamental rights and freedoms of Personal Data Subjects protected under the Law and Policy. The Company shows the necessary sensitivity to comply with the basic principles regarding the protection of Personal Data and to observe the balance of interests of Personal Data Subjects.

2.3. Conditions for Processing Special Categories of Personal Data

Processing special categories of personal data is prohibited as a rule. However, Company processes special categories of personal data in accordance with the principles set forth in this Policy and in the existence of the following grounds specified in Article 6 of the Law and such data are protected in accordance with the Policy on the Security of Special Categories of Personal Data:

- **Explicit Consent of the data subject**
  One of the conditions for processing special categories of personal data is the explicit consent of the data subject. The explicit consent of the data subject must be related to a specific subject, based on information and freely given.

In the presence of the following special categories of personal data processing conditions, personal data may be processed without the explicit consent of the data subject:

- **Explicitly Stipulated by Laws**
  If the special categories of personal data of the data subject are explicitly stipulated in the law, in other words, if there is a clear provision in the relevant law regarding the processing of special categories of personal data, this data processing condition may be mentioned.

- **Failure to Obtain Explicit Consent of the Data Subject Due to Physical Disability**
  The personal data of the data subject may be processed if it is mandatory to process the personal data of the data subject in order to protect the life or physical integrity of the data subject or another person who is unable to disclose his/her consent due to actual impossibility or whose consent cannot be recognized as valid.

- **Publicization of Special Categories of Personal Data of the Data Subject**
  In the event that the data subject has made his/her special categories of personal data public in accordance with his/her own will to make it public, the relevant special categories of personal data may be processed limited to the purpose of making it public.

- **Data Processing is Mandatory for the Establishment or Protection of a Right**
  If data processing is mandatory for the establishment, exercise or protection of a right, the special categories of personal data of the data subject may be processed.

- **Processing is Necessary within the Scope of Relevant Purposes by Persons Under Secrecy Obligation or Authorized Institutions and Organizations**

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

Special categories of personal data of the data subject may be processed by persons under the obligation of confidentiality or authorized institutions and organizations; if necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of health services.

- **Processing for the Fulfillment of Legal Obligations Regarding Employment, Occupational Health and Safety, Social Security, Social Services and Social Assistance**
  In the event that it is mandatory to fulfill legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance, the special categories of personal data of the data subject may be processed.

- **Processing Regarding Foundations, Associations and Other Non-Profit Organizations or Entities Established for Political, Philosophical, Religious or Trade Union Purposes**
  Foundations, associations and other non-profit organizations or formations established for political, philosophical, religious or trade union purposes; provided that they comply with the legislation to which they are subject and their purposes, are limited to their fields of activity and are not disclosed to third parties; may process special categories of personal data of the data subject for their current or former members and members or persons who are in regular contact with these organizations and formations.

2.4. Conditions of Transfer of Personal Data

If one or more of the following data processing conditions ("Data Processing Conditions") are present, personal data may be transferred to third parties by our Company by taking all necessary measures and taking all necessary security measures, including the methods stipulated by the Board.

- Consent of the data subject to the transfer of his/her personal data to domestic third parties,
- Relevant activities regarding the transfer of personal data are expressly stipulated in the laws,
- Transfer of personal data by the Company is directly related to and necessary for the establishment or performance of a contract,
- Transfer of personal data is necessary for our Company to fulfill its legal obligations,
- Transfer of personal data by our Company limited to the purpose of making it public, provided that the personal data have been made public by the data subject,
- Transfer of personal data by the Company is necessary for the establishment, exercise or protection of the rights of the Company or the data subject or third parties,
- Transfer of personal data is necessary for the legitimate interests of the Company, provided that it does not violate the fundamental rights and freedoms of the data subject,
- It is necessary for the protection of the life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.

2.4.1. Conditions for Transferring Personal Data Abroad

The transfer of personal data abroad by our Company will be carried out in accordance with Article 9 of the Law and the principles set out in this Policy by taking technical and administrative measures in the scope described below:

(i) Transfer Based on the Adequacy Decision Made About the Relevant Country, International Organization or Sectors within the Country

Personal data may be transferred abroad by the Company if one of the conditions specified in Articles 5 and 6 of the Law exists and there is an adequacy decision issued by the Board

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

regarding the country, international organization or sectors within the country to which the transfer will be made.

The adequacy decision is issued by the Board and published in the Official Gazette. The Board may also seek the opinion of relevant institutions and organizations if necessary. The adequacy decision is evaluated every four years at the latest. The Board may modify, suspend or revoke the adequacy decision with prospective effect as a result of the assessment or as otherwise deemed necessary.

(ii) Transfer Based on Appropriate Safeguards

In the absence of an adequacy decision, personal data may be transferred abroad by the Company if one of the following appropriate safeguards is provided by the parties, provided that one of the personal data processing conditions specified in Articles 5 and 6 of the Law exists and the data subject has the opportunity to exercise his/her rights and apply for effective legal remedies in the country where the transfer will be made:

- **Special Transfer Reason for Public Institutions and Organizations or Professional Organizations of Public Nature:** Existence of an agreement that is not in the nature of an international agreement between public institutions and organizations or international organizations abroad and public institutions and organizations or professional organizations in the nature of a public institution in Türkiye and the Board's authorization of the transfer.
- **Binding Corporate Rules:** Existence of binding corporate rules approved by the Board and containing provisions on the protection of personal data, which companies within the group of undertakings engaged in joint economic activities are obliged to comply with.
- **Standard Contracts:** Existence of a standard contract announced by the Board, including data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures to be taken by the data importer, additional measures taken for special categories of personal data, and notifying the Board about this standard contract within the legal periods.
- **Undertaking:** Existence of a written undertaking containing provisions to ensure adequate protection and authorization of the transfer by the Board.

(iii) Transfer Based on Derogations

Personal data may be transferred abroad by the Company in the absence of an adequacy decision and if one of the appropriate safeguards cannot be provided, provided that it is incidental, in the presence of one of the following situations:

- **Informed Special Explicit Consent for Possible Risks:** The explicit consent of the data subject to the transfer, provided that the data subject is informed about the possible risks.

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

- **Execution of the Contract and Implementation of Pre-Contractual Measures:** The transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken upon the request of the data subject.
- **Third Party Contracts for the Benefit of the Data Subject:** The transfer is necessary for the conclusion or performance of a contract between the controller and another natural or legal person for the benefit of the data subject.
- **Necessity for Important Reasons of Public Interest:** The transfer is necessary for an important reason of public interest.
- **Establishment, Exercise or Protection of a Right:** The transfer of personal data is mandatory for the establishment, exercise or protection of a right.
- **Vital Interest:** The transfer of personal data is mandatory for the protection of the life or physical integrity of the person or another person who is unable to disclose his consent due to actual impossibility or whose consent is not legally valid.
- **Transfer from Public Registers:** Transfer from a registry open to the public or persons with legitimate interests, provided that the conditions required to access the registry in the relevant legislation are met and the person with a legitimate interest requests it.

2.5. Conditions for Transfer of Special Categories of Personal Data

Transfer of special categories of personal data is prohibited as a rule. However, Company processes special categories of personal data in accordance with the principles set forth in this Policy and in the existence of the following grounds specified in Article 6 of the Law and such data are protected in accordance with the Policy on the Security of Special Categories of Personal Data:

- **Explicit Consent of the data subject**
  One of the conditions for processing special categories of personal data is the explicit consent of the data subject. The explicit consent of the data subject must be related to a specific subject, based on information and freely given.

In the presence of the following special categories of personal data processing conditions, personal data may be processed without the explicit consent of the data subject:

- **Explicitly Stipulated by Laws**
  If the special categories of personal data of the data subject are explicitly stipulated in the law, in other words, if there is a clear provision in the relevant law regarding the processing of special categories of personal data, this data processing condition may be mentioned.

- **Failure to Obtain Explicit Consent of the Data Subject Due to Physical Disability**

The personal data of the data subject may be processed if it is mandatory to process the personal data of the data subject in order to protect the life or physical integrity of the data subject or another person who is unable to disclose his/her consent due to actual impossibility or whose consent cannot be recognized as valid.

- **Publicization of Special Categories of Personal Data of the Data Subject**
  In the event that the data subject has made his/her special categories of personal data public in accordance with his/her own will to make it public, the relevant special categories of personal data may be processed limited to the purpose of making it public.

- **Data Processing is Mandatory for the Establishment or Protection of a Right**
  If data processing is mandatory for the establishment, exercise or protection of a right, the special categories of personal data of the data subject may be processed.

- **Processing is Necessary within the Scope of Relevant Purposes by Persons Under Secrecy Obligation or Authorized Institutions and Organizations**
  Special categories of personal data of the data subject may be processed by persons under the obligation of confidentiality or authorized institutions and organizations; if necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of health services.

- **Processing for the Fulfillment of Legal Obligations Regarding Employment, Occupational Health and Safety, Social Security, Social Services and Social Assistance**
  In the event that it is mandatory to fulfill legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance, the special categories of personal data of the data subject may be processed.

- **Processing Regarding Foundations, Associations and Other Non-Profit Organizations or Entities Established for Political, Philosophical, Religious or Trade Union Purposes**
  Foundations, associations and other non-profit organizations or formations established for political, philosophical, religious or trade union purposes; provided that they comply with the legislation to which they are subject and their purposes, are limited to their fields of activity and are not disclosed to third parties; may process special categories of personal data of the data subject for their current or former members and members or persons who are in regular contact with these organizations and formations.

2.5.1. Transfer of Special Categories of Personal Data Abroad

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

The transfer of special categories of personal data abroad by our Company will be carried out in accordance with Article 9 of the Law and the principles set out in this Policy by taking technical and administrative measures in the scope described below:

(i) Transfer Based on the Adequacy Decision Made About the Relevant Country, International Organization or Sectors within the Country

Personal data may be transferred abroad by the Company if one of the conditions specified in Articles 5 and 6 of the Law exists and there is an adequacy decision issued by the Board regarding the country, international organization or sectors within the country to which the transfer will be made.

The adequacy decision is issued by the Board and published in the Official Gazette. The Board may also seek the opinion of relevant institutions and organizations if necessary. The adequacy decision is evaluated every four years at the latest. The Board may modify, suspend or revoke the adequacy decision with prospective effect as a result of the assessment or as otherwise deemed necessary.

(ii) Transfer Based on Appropriate Safeguards

In the absence of an adequacy decision, personal data may be transferred abroad by the Company if one of the following appropriate safeguards is provided by the parties, provided that one of the personal data processing conditions specified in Articles 5 and 6 of the Law exists and the data subject has the opportunity to exercise his/her rights and apply for effective legal remedies in the country where the transfer will be made:

- **Special Transfer Reason for Public Institutions and Organizations or Professional Organizations of Public Nature:** Existence of an agreement that is not in the nature of an international agreement between public institutions and organizations or international organizations abroad and public institutions and organizations or professional organizations in the nature of a public institution in Türkiye and the Board's authorization of the transfer.
- **Binding Corporate Rules:** Existence of binding corporate rules approved by the Board and containing provisions on the protection of personal data, which companies within the group of undertakings engaged in joint economic activities are obliged to comply with.
- **Standard Contracts:** Existence of a standard contract announced by the Board, including data categories, purposes of data transfer, recipients and recipient groups, technical and administrative measures to be taken by the data importer, additional measures taken for special categories of personal data, and notifying the Board about this standard contract within the legal periods.
- **Undertaking:** Existence of a written undertaking containing provisions to ensure adequate protection and authorization of the transfer by the Board.

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

(iii) Transfer Based on Derogations

Personal data may be transferred abroad by the Company in the absence of an adequacy decision and if one of the appropriate safeguards cannot be provided, provided that it is incidental, in the presence of one of the following situations:

- **Informed Special Explicit Consent for Possible Risks:** The explicit consent of the data subject to the transfer, provided that the data subject is informed about the possible risks.
- **Execution of the Contract and Implementation of Pre-Contractual Measures:** The transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken upon the request of the data subject.
- **Third Party Contracts for the Benefit of the Data Subject:** The transfer is necessary for the conclusion or performance of a contract between the controller and another natural or legal person for the benefit of the data subject.
- **Necessity for Important Reasons of Public Interest:** The transfer is necessary for an important reason of public interest.
- **Establishment, Exercise or Protection of a Right:** The transfer of personal data is mandatory for the establishment, exercise or protection of a right.
- **Vital Interest:** The transfer of personal data is mandatory for the protection of the life or physical integrity of the person or another person who is unable to disclose his consent due to actual impossibility or whose consent is not legally valid.
- **Transfer from Public Registers:** Transfer from a registry open to the public or persons with legitimate interests, provided that the conditions required to access the registry in the relevant legislation are met and the person with a legitimate interest requests it.

PART THREE

§ 3. CLASSIFICATION OF PERSONAL DATA, PURPOSES OF PROCESSING AND TRANSFER, PERSONS TO WHOM PERSONAL DATA WILL BE TRANSFERRED

3.1. Classification of Personal Data

Within the Company; In line with the legitimate and lawful personal data processing purposes of the Company, based on and limited to one or more of the personal data processing conditions specified in Article 5 of the Law, in compliance with the general principles specified in the Law, in particular the principles specified in Article 4 regarding the processing of personal data, and all obligations regulated in the Law, and limited to the subjects within the scope of this Policy, personal data in the categories specified below are processed by informing the data subjects in accordance with Article 10 of the Law. It is also stated in this section which data

subjects the personal data processed in these categories are related to within the scope of this Policy.

PERSONAL DATA CATEGORIZATION	PERSONAL DATA CATEGORISATION EXPLANATION
Identification Information	Data that clearly belongs to an identified or identifiable natural person; processed partially or completely automatically or non-automatically as part of a data recording system; containing information about the identity of the person; documents such as driver's licence, identity card and passport containing information such as name-surname, Turkish ID number, nationality, mother's name-father's name, place of birth, date of birth, gender, and tax number, SSI number, signature information, vehicle license plate, etc.
Communication Information	Information such as telephone number, address, e-mail address, fax number, IP address, which clearly belongs to an identified or identifiable natural person; processed partially or completely automatically or non-automatically as part of the data recording system.
Transaction Security Information	Personal data processed regarding the technical, administrative, legal and commercial security of both the Data Subject and the Company while carrying out the activities of the Company.
Physical Space Safety Information	Personal data clearly belonging to an identified or identifiable natural person; processed partially or completely automatically or non-automatically as part of a data recording system; personal data relating to records and documents taken at the entrance to the physical space, during the stay in the physical space; camera recordingsand records taken at the security point etc.
Customer Transaction	Call centre records, Invoice, promissory note, cheque information, Order information, Request information etc.
Audio/Visual Information	Data in the form of photographs and camera recordings (except for recordings within the scope of Physical Space Security Information)and copies of documents containing personal data, which clearly belong to an identified or identifiable natural person.
Personal Information	Regarding the identity information of the employee, a copy of the identity card or a sample of the population registration, residence certificate, a document showing the education status of the employee, employment contract, health report to be taken at the time of employment, a report stating that they have

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

	undergone periodic health examinations for some lines of work, a health report if the employee is disabled, the application registration document at the Provincial Directorate of Labour and Employment Agency for the disabled employee, criminal record, a copy of the account receipts for the wages paid, a letter stating the reason for the deductions made if a wage deduction penalty is applied for any legal reason, the letter in which the approval of the worker for overtime work is obtained (approval letters received at the beginning of each calendar year), the letter stating that the workers have been informed about occupational health and safety and the occupational risks they face, the necessary measures to be taken and their legal rights and responsibilities, work certificate (for workers who leave the job), SSI employment and termination notifications, annual paid leave book, temporary incapacity reports received by the worker during the employment relationship, all kinds of minutes kept during the employment relationship and according to the requirements of the work
Legal Process Consent	Data processed within the scope of the determination and follow-up of the Company's legal receivables and rights and the performance of its debts and legal obligations.
Professional Experience	Diploma information, courses attended, in-service training information, Certificates, Transcript information etc.
Marketing	Survey, Cookie records, Information obtained through campaigns, etc.
Health Information	Information on disability status, Blood group information, Personal health information, Information on devices and prostheses used
Criminal Convictions and Security Measures	Information on criminal convictions, Information on security measures

3.2. Purposes of Processing and Transferring Personal Data

Personal Data; in accordance with the law and the purpose of the Law,

- Execution of Emergency Management Processes
- Execution of Information Security Processes
- Execution of Employee Candidate / Intern / Student Recruitment and Placement Processes
- Execution of Employee Candidate Application Processes

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

- Execution of Employee Satisfaction and Engagement Processes
- Fulfillment of Employment Contract and Statutory Obligations for Employees
- Execution of Employee Benefits and Entitlements Processes
- Execution of Audit / Ethical Activities
- Execution of Training Activities
- Execution of Access Authorization Processes
- Execution of Activities in Compliance with Legislation
- Execution of Finance and Accounting Affairs
- Execution of Company / Product / Service Loyalty Processes
- Ensuring Physical Space Security
- Execution of Assignment Processes
- Management of Visual and Audio Records
- Follow-up 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
- Receiving and Evaluating Suggestions for Business Process Improvement
- Execution of Business Continuity Activities
- Execution of Logistics Activities
- Execution of Procurement Processes for Goods / Services
- Execution of After-Sales Support Services for Goods / Services
- Execution of Sales Processes for Goods / Services
- Execution of Production and Operation Processes for Goods / Services
- Execution of Customer Relationship Management Processes
- Execution of Customer Satisfaction Activities
- Organization and Event Management
- Execution of Marketing Analysis Activities
- Execution of Performance Evaluation Processes
- Execution of Advertising / Campaign / Promotion Processes
- Execution of Risk Management Processes
- Execution of Retention and Archiving Activities
- Execution of Social Responsibility and NGO Activities
- Execution of Sponsorship Activities
- Execution of Strategic Planning Activities
- Execution of Contract Processes
- Follow-up of Requests / Complaints
- Ensuring Security of Movable Property and Resources
- Execution of Supply Chain Management Processes
- Execution of Compensation Policy
- Execution of Marketing Processes for Products / Services

- Ensuring Security of Data Controller Operations
- Execution of Work and Residence Permit Procedures for Foreign Personnel
- Execution of Investment Processes
- Execution of Talent / Career Development Activities
- Providing Information to Authorized Persons, Institutions and Organizations
- Execution of Management Activities
- Creation and Monitoring of Visitor Records

limited to the purposes and within the scope of the personal data processing conditions specified in Articles 5 and 6 of the Law. If the processing activity carried out for the aforementioned purposes does not meet any of the conditions stipulated under the Law, your explicit consent is obtained by the Company regarding the relevant processing process.

PART FOUR

§ 4. METHOD AND LEGAL GROUNDS FOR COLLECTING PERSONAL DATA, DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA AND RETENTION PERIOD

4.1. Method and Legal Reason for Collecting Your Personal Data

For the purpose of checking compliance with Article 1 regulating the purpose of the Law and Article 2 regulating the scope of the Law, Personal Data is collected in all kinds of verbal, written, electronic media; by technical and other methods, through various means such as call center, Company website, mobile application, in order to fulfill the responsibilities arising from the law within the framework of legislation, contract, request and optional legal reasons in order to fulfill the purposes set out in the Policy, and is processed by the Company or data processors assigned by the Company.

4.2. Erasure, Destruction or Anonymisation of Personal Data

Without prejudice to the provisions of other laws regarding the erasure, destruction or anonymisation of Personal Data, the Company deletes, destroys or anonymises Personal Data ex officio or upon the request of the data subject in the event that the reasons requiring its processing disappear, although it has processed it in accordance with the provisions of this Law and other laws. With the erasure of Personal Data, this data is removed from daily active systems and areas visible to users. When destroying Personal Data, they are removed from the

documents, files, CDs, floppy disks, hard discs, etc. in such a way that they cannot be used and retrieved in any way again, and the materials suitable for data storage are destroyed. By anonymisation of data, it is meant that Personal Data cannot be associated with an identified or identifiable natural person even if it is matched with other data.

4.3. Retention Period of Personal Data

The Company stores Personal Data for the period specified in this legislation, if stipulated in the legislation. If a period of time is not regulated in the legislation regarding how long personal data should be kept, Personal Data is processed for the period required to be processed in accordance with the practices and customs of the Company's practices and commercial life, depending on the activity carried out by the Company while processing that data, and then deleted, destroyed or anonymized.

If the purpose of processing personal data has ended and the retention periods determined by the relevant legislation and the Company have come to an end; personal data may be stored only for the purpose of constituting evidence in possible legal disputes or for the assertion or defence of the relevant right related to personal data. In the establishment of the periods herein, retention periods are determined based on the statute of limitations for the assertion of the aforementioned right and the examples of the requests previously addressed to the Company on the same issues despite the expiry of the statute of limitations. In this case, the stored personal data is not accessed for any other purpose and access to the relevant personal data is provided only when it is required to be used in the relevant legal dispute. Here, too, personal data are deleted, destroyed or anonymised after the aforementioned period expires.

PART FIVE

§ 5. CONSIDERATIONS REGARDING THE PROTECTION OF PERSONAL DATA

In accordance with the Law and within the scope of the Communiqué on the Procedures and Principles to be Followed in Fulfilment of the Disclosure Obligation ("Communiqué"), the Companies take the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent unlawful processing of the Personal Data it processes, to prevent unlawful access to the data and to ensure the preservation of the data, and to carry out or have the necessary audits carried out within this scope. In their position as data processors, companies shall not disclose the personal data they have learnt within the scope of 12 (4) of the Law to anyone else in violation of the provisions of this Law and shall not use them for purposes other than processing.

5.1. Securing Personal Data

5.1.1. Technical and Administrative Measures Taken to Ensure Lawful Processing of Personal Data

The Company takes technical and administrative measures to ensure that Personal Data is processed in accordance with the law, according to technological possibilities and implementation cost.

(i) Technical Measures Taken to Ensure Lawful Processing of Personal Data

The main technical measures taken by the Company to ensure the lawful processing of Personal Data are listed below:

- Personal Data processing activities carried out within the Company are supervised by the technical systems established.
- The technical measures taken are periodically reported to the data subject as required by the internal audit mechanism.
- The Company employs knowledgeable and experienced persons to ensure data security and provides the necessary KVK trainings to its personnel.

(ii) Administrative Measures Taken to Ensure Lawful Processing of Personal Data

The main administrative measures taken by the Company to ensure the lawful processing of Personal Data are listed below:

- Employees are informed and trained about the law on the protection of Personal Data and the processing of Personal Data in accordance with the law.
- All activities carried out by the Company are analysed in detail specific to all business units, and as a result of this analysis, Personal Data processing activities are revealed specific to the activities carried out by the relevant business units.
- Personal Data processing activities carried out by the business units of the Company; The requirements to be fulfilled in order to ensure that these activities comply with the Personal Data processing conditions required by the Law are determined specifically for each business unit and the detailed activity it carries out.
- In order to ensure the legal compliance requirements determined on a business unit basis, awareness is raised and implementation rules are determined for the relevant business units; the necessary administrative measures are implemented through internal policies and trainings to ensure the supervision of these issues and the continuity of the implementation.
- In the contracts and documents governing the legal relationship between the Company and the employees, records that impose the obligation not to process, disclose and use

Personal Data, except for the Company's instructions and the exceptions imposed by law, are included in the contracts and documents governing the legal relationship between the Company and the employees, and the obligations arising from the Law are fulfilled by raising employee awareness on this issue and conducting audits.

5.1.2. Technical and Administrative Measures Taken to Prevent Unlawful Access to Personal Data

The Company takes technical and administrative measures according to the nature of the data to be protected, technological possibilities and cost of implementation in order to prevent imprudent or unauthorised disclosure, access, transfer or any other unlawful access to Personal Data.

(i) Technical Measures Taken to Prevent Unlawful Access to Personal Data

The main technical measures taken by the Company to prevent unlawful access to Personal Data are listed below:

- Technical measures are taken in accordance with the developments in technology, and the measures taken are periodically updated and renewed.
- Access and authorisation technical solutions are implemented in accordance with the legal compliance requirements determined on a business unit basis.
- Access authorisations are limited and authorisations are regularly reviewed.
- The technical measures taken are periodically reported to the data subject as required by the internal audit mechanism, and the issues that pose a risk are re-evaluated and necessary technological solutions are produced.
- Software and hardware including virus protection systems and firewalls are installed.
- Personnel knowledgeable in technical issues are employed.
- Regular security scans are carried out to identify security vulnerabilities in applications where Personal Data is collected. It is ensured that the deficits found are closed.

(ii) Administrative Measures to Prevent Unlawful Access to Personal Data

The main administrative measures taken by the Company to prevent unlawful access to Personal Data are listed below:

- Employees are trained on the technical measures to be taken to prevent unlawful access to Personal Data.
- In accordance with the legal compliance requirements for processing Personal Data on a business unit basis, access and authorisation processes for Personal Data are designed and implemented within the Company.

- Employees are informed that they cannot disclose the Personal Data they have learnt to others in violation of the provisions of the Law and cannot use them for purposes other than processing, and that this obligation will continue after their resignation and necessary commitments are obtained from them in this direction.
- In the contracts concluded by the Company with the persons to whom Personal Data is transferred in accordance with the law; Provisions are added that the persons to whom Personal Data is transferred will take the necessary security measures to protect Personal Data and ensure that these measures are complied with in their own organisations.

5.1.3. Storing Personal Data in Secure Environments

The Company takes the necessary technical and administrative measures according to technological possibilities and implementation cost in order to store Personal Data in secure environments and to prevent its destruction, loss or alteration for unlawful purposes.

(i) Technical Measures Taken for Storing Personal Data in Secure Environments

The main technical measures taken by the Company to store Personal Data in secure environments are listed below:

- Systems in accordance with technological developments are used to store Personal Data in secure environments.
- Specialised personnel are employed in technical matters.
- Technical security systems are installed for storage areas, security tests and researches are conducted to identify security vulnerabilities on information systems, and existing or potential risk issues identified as a result of the tests and researches are eliminated. The technical measures taken are periodically reported to the data subject as required by the internal audit mechanism.
- Back-up programmes are used in accordance with the law to ensure the safe storage of Personal Data.
- Access to the environments where Personal Data is kept is restricted and only authorised persons are allowed to access this data limited to the purpose of storing personal data, and access to the data storage areas where Personal Data is stored is logged and inappropriate access or access attempts are instantly communicated to the data subjects.

(ii) Administrative Measures Taken for Storing Personal Data in Secure Environments

The main administrative measures taken by the Company to store Personal Data in secure environments are listed below:

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım

- Employees are trained to ensure that Personal Data is stored securely.
- Legal and technical consultancy services are obtained in order to follow the developments in the field of information security, privacy of private life and protection of personal data and to take necessary actions.
- In the event that an external service is obtained by the Company due to technical requirements for the storage of Personal Data, the contracts concluded with the relevant companies to which Personal Data is transferred in accordance with the law include provisions stating that the persons to whom Personal Data is transferred will take the necessary security measures to protect Personal Data and ensure that these measures are complied with in their own organisations.
- The Information Security Management System and Board have been established, shared with all employees, and the effectiveness and sustainability of the work carried out through periodic meetings are ensured.

5.1.4. Supervision of Measures Taken for the Protection of Personal Data

In accordance with Article 12 of the Law, the Company conducts or has the necessary audits performed within its own organisation. The results of these audits are reported to the relevant department within the scope of the internal functioning of the Company and necessary actions are taken to improve the measures taken.

5.1.5. Measures to be taken in case of unauthorised disclosure of personal data

In the event that Personal Data processed in accordance with Article 12 of the Law is obtained by others illegally, the Company operates the system that ensures that this situation is notified to the relevant Data Subject and the Board as soon as possible. If deemed necessary by the PDP Board, this situation may be announced on the Board's website or by another method.

5.2. Observing the Legal Rights of Personal Data Subjects

The Company observes all legal rights of Personal Data Subjects with the implementation of the Policy and the Law and takes all necessary measures to protect these rights. Detailed information on the rights of Personal Data Subjects is provided in the sixth section of this Policy.

5.3. Protection Special Categories of Personal Data

The Law attributes special importance to certain Personal Data due to the risk of causing victimisation and/or discrimination when processed unlawfully. These data include data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs,

appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data. The Company shows maximum sensitivity to the protection of special quality Personal Data, which is determined as "special quality" by the Law and processed in accordance with the law. In this context, the technical and administrative measures taken by the Company for the protection of personal data are also implemented with the utmost care in terms of Special Categories of Personal Data and necessary audits are provided within the Company in this regard.

PART SIX

§ 6. RIGHTS, EXERCISE AND EVALUATION OF PERSONAL DATA SUBJECTS

6.1. Disclosure of Personal Data Subjects

The Company informs Personal Data Subjects during the acquisition of Personal Data within the scope of Article 10 of the Law and the Communiqué. In this context, if any, the identity of the Company 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 and legal reason for collecting Personal Data and the rights of the Personal Data Subjects.

6.2. Rights of the Data Subject under the Law

Pursuant to Article 10 of the Law, the Company informs you of your rights; provides guidance on how to exercise such rights and carries out the necessary internal functioning, administrative and technical arrangements for all these. Pursuant to Article 11 of the Law, the Company may provide Personal Data to the persons whose Personal Data are received;

- Acquiring whether personal data is being processed,
- Requesting information if their Personal Data has been processed,
- Acquiring the purpose of processing Personal Data and whether they are used in accordance with their purpose,
- Getting to know the third parties to whom Personal Data is transferred domestically or abroad,
- Requesting correction of Personal Data in case of incomplete or incorrect processing,
- Requesting the erasure or destruction of Personal Data within the framework of the conditions stipulated in Article 7 of the Law,
- 11. Requesting notification of the transactions made pursuant to subparagraphs (d) and (e) of the Article to third parties to whom personal data are transferred,

- Objecting to the emergence of a result to the detriment of the person himself/herself by analysing the processed data exclusively through automated systems,
- In case of damage due to unlawful processing of Personal Data, to demand the compensation of the damage

.

In the event of any change, withdrawal or objection regarding the shared personal data, as the data controller, with the responsibility of informing the third parties with whom we have shared personal data, the necessary correspondence will be structured in accordance with the provisions of the law by obtaining legal advice, depending on the circumstances of the case.

When requested by the Data Subject, a copy of the personal data processed, in response to the request, legal the data is given to the data subject by Hitit with documentation in accordance with the law, after obtaining the opinion of the data subject.

6.3. Cases where the Personal Data Subjectcannot assert his/her rights

Since the following cases are excluded from the scope of the Law pursuant to Article 28 of the Law, Personal Data Subjects cannot assert their rights listed in Article (6.2.) of this Policy in the following cases:

- Processing of Personal Data by natural persons within the scope of activities related to themselves or their family members living in the same residence, provided that they are not disclosed to third parties and the obligations regarding data security are complied with.
- Processing of personal data for purposes such as research, planning and statistics by anonymizing them with official statistics.
- Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate or constitute a crime against national defense, national security, public security, public order, economic security, privacy or personal rights.
- Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
- Processing of Personal Data by judicial authorities or enforcement authorities in relation to investigation, prosecution, judgement or execution procedures.

Pursuant to Article 28/2 of the Law; In the cases listed below, Personal Data Subjects cannot assert their rights listed in Article (6.2.) of this Policy, except for the right to claim compensation for damages:

- Processing personal data being required for prevention of committing an illegal act or criminal investigation.
- Processing of personal data made public by the Personal Data Subject himself/herself.
- Processing personal data being required for disciplinary investigation or prosecution and conducting supervisory or regulatory duties by the authorized state institutions and organizations and professional public organizations by the power granted by the law.
- Processing personal data being required for protecting economic and financial interest of the State in relation to the budget, tax and financial matters.

6.4. Exercise of Rights by the Data Subject

Personal Data Subjects submit their requests regarding their rights listed in Article (6.2.) of this Policy to the Company address through a notary public by filling out and signing the Application Form, which can be accessed from the link https://hitit.com/themes/hitit/documents/2026-02/ilgili-kisi-basvuru-formu.pdf, with the information and documents that will identify their identities.

Company Address Hitit Bilgisayar Hizmetleri A.S. Reşitpaşa Mahallesi, Katar Cad. No:4/1 Arı Teknokent 2 Interior Door No:601 Maslak 34469 Sarıyer/İstanbul

In order for third parties to request an application on behalf of personal data subjects, a special power of attorney issued by the data subjects through a notary public should be available.

6.5. Procedure and Duration of the Company's Response to Applications

The Company shall finalise the requests in the application free of charge as soon as possible, within thirty days at the latest, depending on the nature of the request. However, if the said transaction requires an additional cost, the fee in the tariff determined by the Board may be charged. The Company may either accept the request or reject it by explaining its reasoning and notify its response in writing or electronically. If the request in the application is accepted, the Company fulfils the requirements of the request.

6.6. Data Subject's Right to File a Complaint to the Board

In cases where the application is rejected, the response is found insufficient or the application is not responded to in due time; the data subject has the right to file a complaint to the PDP Board within thirty days from the date of learning the response and in any case within sixty days from the date of application.

PART SEVEN

§ 7. MANAGEMENT STRUCTURE IN ACCORDANCE WITH THE COMPANY'S POLICY ON PROCESSING AND PROTECTION OF PERSONAL DATA

The Company has appointed a Personal Data Communication Officer in accordance with the decision of the senior management of the Company to manage this Policy and other policies related and related to this Policy. The Personal Data Communication Officer is authorised and responsible for taking the necessary actions for the storage and processing of the data of the Data Subjects in accordance with the law, this Policy and other policies connected and related to this Policy

PART EIGHT

§ 8. UPDATE, HARMONISATION AND AMENDMENTS

8.1. Update and Compliance

The Company reserves the right to make changes in this Policy and other policies related and related to this Policy due to amendments to the Law, in accordance with the decisions of the PDP Board or in line with the developments in the sector or in the field of informatics.

Classification: Hitit Partners Use | Sınıflandırma: Hitit İş Ortağı Kullanım