

BELCEHAN TOURISM FOOD CONSTRUCTION IMPORT EXPORT TRANSPORT INDUSTRY AND TRADE LIMITED COMPANY
PRINCIPLES OF PERSONAL DATA PROTECTION AND PROCESSING

Target Audience: All natural persons whose personal data are processed by Belcehan Tourism Food Construction Import Export Transport Industry And Trade Limited Company

Prepared by: Personal Data Protection Committee of Belcehan Tourism Food Construction Import Export Transport Industry And Trade Limited Company

Version: 1.0

Approved by: Belcehan Tourism Food Construction Import Export Transport Industry And Trade Limited Company

CONTENTS

1. INTRODUCTION 1
 - 1.1. Purpose 1
 - 1.2. Scope 1
 - 1.3. Legal Basis 1
 - 1.4. Definitions 2
2. PROCESSING OF PERSONAL DATA 3
 - 2.1. Lawful Processing of Personal Data 3
 - 2.2. Conditions for Processing Personal Data 4
 - 2.3. Processing of Special Categories of Personal Data 4
 - 2.4. Informing the Data Subject and Obtaining Explicit Consent 5
 - 2.5. Transfer of Personal Data 5
3. PERSONAL DATA PARAMETERS AND INVENTORY 6
4. MEASURES TAKEN FOR THE PROTECTION OF PERSONAL DATA 6
5. STORAGE AND DESTRUCTION OF PERSONAL DATA 7
6. RIGHTS OF DATA SUBJECTS AND EXERCISE OF THESE RIGHTS 7
 - 6.1. Rights of the Data Subject 7
 - 6.2. Exercise of Rights by the Data Subject 8
 - 6.3. Response to Applications 8
 - 6.4. Rejection of the Data Subject's Application 8
 - 6.5. Right of the Data Subject to File a Complaint to the PDP Board 9
7. EXECUTION 9
8. EFFECTIVENESS AND ANNOUNCEMENT 9

1. INTRODUCTION

Belcehan Tourism Food Construction Import Export Transport Industry And Trade Limited Company ("BELCEHAN") places great importance on the protection of personal data in its operations and considers it a priority in its business processes. BELCEHAN's Personal Data Protection and Processing Policy ("Principles") constitutes the basic framework for aligning

BELCEHAN's organizational and business processes with the procedures and principles for processing personal data as stipulated by Law No. 6698 on the Protection of Personal Data ("Law"). In line with these Principles, BELCEHAN processes and protects personal data with high-level responsibility and awareness, ensuring transparency by informing the data subjects.

1.1. Purpose

The purpose of these Principles is to ensure that the procedures and principles foreseen in the Law and relevant legislation are effectively implemented by adapting them to BELCEHAN's organization and processes. BELCEHAN takes all administrative and technical measures, establishes necessary internal procedures, increases awareness, and provides all training required to ensure consciousness for the processing and protection of personal data. All necessary precautions are taken to ensure compliance of relevant persons with the Law, and appropriate and effective auditing mechanisms are established.

1.2. Scope

These Principles cover all personal data obtained through BELCEHAN's business processes, whether electronic or non-electronic, provided that they are part of any data recording system, including the attached Data Categories and Personal Data (Annex-1) and attached Personal Data Processing Purposes (Annex-2).

1.3. Legal Basis

The Principles are based on the Law and relevant legislation. Personal data are processed to fulfill the legal obligations arising from Law No. 2634 on the Promotion of Tourism, the Regulation on Certification and Qualifications of Tourism Facilities, Law No. 6502 on Consumer Protection, Law No. 1774 on Identity Notification, Labor Law No. 4857, Occupational Health and Safety Law No. 6331, Social Insurances and General Health Insurance Law No. 5510, Unemployment Insurance Law No. 4447, Turkish Commercial Code No. 6102, Tax Procedure Law No. 213, and other relevant legislation.

In cases of conflict between applicable legislation and these Principles, the applicable legislation prevails. The provisions foreseen by relevant legislation are adapted into BELCEHAN's practices through these Principles.

1.4. Definitions

Recipient Group: Category of natural or legal persons to whom personal data are transferred by the data controller.

Explicit Consent: Consent given freely, based on information, regarding a specific subject.

Anonymization: The process of rendering personal data unidentifiable with any natural person, even when matched with other data.

Employee: Personnel of the Personal Data Protection Authority.

Electronic Environment: Environments where personal data can be created, read, modified, and written using electronic devices.

Non-Electronic Environment: All written, printed, visual, and other environments outside

electronic environments.

Service Provider: Natural or legal persons providing services under a specific contract with the Personal Data Protection Authority.

Data Subject: Natural person whose personal data is processed.

Relevant User: Persons processing personal data within the organization of the data controller or under authority and instructions received from the data controller, excluding those responsible for technical storage, protection, and backup.

Destruction: Deletion, destruction, or anonymization of personal data.

Law: Law No. 6698 on the Protection of Personal Data.

Recording Medium: Any environment where personal data are processed, whether fully or partially automatic, or as part of a non-automated data recording system.

Personal Data: Any information relating to an identified or identifiable natural person.

Personal Data Processing Inventory: Inventory created by data controllers detailing personal data processing activities, purposes, categories, recipient groups, retention periods, transfers abroad, and security measures.

Processing of Personal Data: All operations performed on personal data, including collection, recording, storage, alteration, disclosure, transfer, classification, or prevention of use, whether automated or not.

Board: Personal Data Protection Board.

Special Categories of Personal Data: Data on race, ethnicity, political opinions, philosophical beliefs, religion, attire, membership of associations/unions, health, sexual life, criminal convictions, biometric or genetic data.

Periodic Destruction: Repeated deletion, destruction, or anonymization as defined in retention and destruction policy after all processing conditions have ceased.

Policy: Personal Data Retention and Destruction Policy.

Data Processor: Natural or legal person processing personal data on behalf of the data controller based on authority given by the data controller.

Data Recording System: Structured system for processing personal data.

Data Controller: Natural or legal person determining purposes and means of processing personal data and responsible for establishing and managing data recording systems.

Data Controllers' Registry Information System (VERBIS): Internet-based system for registration and related processes, managed by the Presidency.

Regulation: Regulation on Deletion, Destruction, or Anonymization of Personal Data, published in Official Gazette on October 28, 2017.

2. PROCESSING OF PERSONAL DATA

2.1. Lawful Processing of Personal Data

Personal data are processed in compliance with the following principles:

i. Processing in Compliance with Law and Fairness

Personal data are processed only to the extent required by business processes, without harming fundamental rights and freedoms, and in accordance with law and fairness.

ii. Ensuring Personal Data are Accurate and Up-to-Date

Necessary measures are taken to keep personal data accurate and current, with planned and programmed efforts.

iii. Processing for Specific, Explicit, and Legitimate Purposes

Personal data are processed in line with legitimate purposes identified and disclosed in business processes.

iv. Relevant, Limited, and Proportional to the Purpose

Personal data are collected and processed only to the extent necessary for the identified purposes.

v. Retention for the Necessary Period

Personal data are retained for at least the period required by applicable law or, if no period is specified, as necessary for the purpose of processing.

Personal data is retained for the duration necessary for the purpose. At the end of the retention periods, personal data is destroyed in accordance with periodic destruction schedules or upon the request of the data subject, using appropriate methods (deletion, eradication, or anonymization).

2.2. Conditions for the Processing of Personal Data

Personal data is processed based on the explicit consent of the data subject or on one or more of the other conditions listed below.

i. Processing Personal Data Without Explicit Consent

Personal data may be processed if any of the following conditions exist:

a. Explicit Regulation in Laws

If there is a clear provision in the law regarding the processing of personal data, the data may be processed without obtaining the consent of the data subject.

b. Impossibility of Obtaining Explicit Consent

If it is physically impossible for the person to express consent, or the consent is not legally valid, and processing the personal data is necessary to protect the life or physical integrity of the person or another individual, the personal data may be processed.

c. Direct Relevance to the Establishment or Performance of a Contract

If the processing of personal data is directly related to the establishment or performance of a contract to which the data subject is a party, their personal data may be processed.

d. Fulfillment of a Legal Obligation

BELCEHAN may process personal data if it is necessary to fulfill legal obligations.

e. Disclosure by the Data Subject

Personal data of data subjects who have made their data public may be processed, limited to the purpose of disclosure.

f. Mandatory Processing for the Establishment or Protection of a Right

If processing is necessary for the establishment, exercise, or protection of a right, the personal data of the data subject may be processed.

g. Mandatory Processing for Legitimate Interests

If processing is necessary for BELCEHAN's legitimate interests, without harming the fundamental rights and freedoms of the data subject, personal data may be processed.

ii. Processing Personal Data Based on Explicit Consent

If none of the above conditions are present, personal data is processed based on the explicit consent of the data subject.

2.3. Processing of Special Categories of Personal Data

BELCEHAN processes special categories of personal data in accordance with the principles set forth in the Law and Principles, taking all necessary administrative and technical measures determined by the Board, under the following procedures and principles:

- i. Explicitly stipulated in the laws,**
- ii. Necessary due to impossibility of obtaining consent from a person who cannot express consent or whose consent is not legally valid, for the protection of their own or another person's life or physical integrity,**
- iii. Concerning personal data made public by the data subject and in accordance with their will to disclose,**
- iv. Necessary for the establishment, exercise, or protection of a right,**
- v. Required to fulfill legal obligations in employment, occupational health and safety, social security, social services, and social assistance.**

If processing is required outside these cases, explicit consent of the data subject is obtained.

2.4. Informing the Data Subject and Obtaining Explicit Consent

BELCEHAN informs data subjects about the purposes for which their personal data is processed, with whom it is shared and for what purposes, how it is collected, the legal basis, and the rights of data subjects in the processing of their personal data, in accordance with applicable legislation. Accordingly, our disclosure texts prepared for business processes, such as the "Customer Disclosure Text" (Annex-3.1), "Supplier Disclosure Text" (Annex-3.2), "Employee Disclosure Text" (Annex-3.3), "Job Applicant Disclosure Text" (Annex-3.4), "Website Cookie Disclosure Text" (Annex-3.5), "Camera Disclosure Text" (Annex-3.6), and "Card-Based Employee Tracking Disclosure Text" (Annex-3.8), are used.

The explicit consent of personal data and special category personal data subjects is obtained after being informed about the relevant matter and freely expressing their will. The consent is obtained in addition after informing the relevant person via the disclosure text.

2.5. Transfer of Personal Data

i. Transfer of Personal Data Within the Country

BELCEHAN transfers personal data, with necessary security measures, to real persons or private legal entities, shareholders, business partners, affiliates and subsidiaries, suppliers, group companies, and authorized public institutions, in a lawful, purpose-bound, and proportional manner, based on one or more of the conditions specified in sections 2.2 and 2.3, according to the attached "Table of Recipients and Purposes of Personal Data Transfers" (Annex-4).

Recipients within the country sign the attached "Corporate Confidentiality Undertaking" (Annex-5) to ensure confidentiality and prevent violations of personal data.

iii. Transfer of Personal Data Abroad

Currently, no personal data is transferred abroad. If data transfer abroad occurs, it must be carried out under the following principles:

a. Personal data and special category personal data may only be transferred abroad if one of the conditions above exists and one of the following cases occurs:

1. There is a sufficiency decision regarding the country, sectors within the country, or international organizations where the transfer will be made.
2. If no sufficiency decision exists, one of the appropriate safeguards (Binding Corporate Rules – Undertaking – Standard Contract) is provided, provided the data subject can exercise their rights and effective legal remedies in the country where the transfer will take place.
3. If neither sufficiency nor safeguards are available, personal data may only be transferred abroad in the following cases:
 - The data subject gives explicit consent after being informed of potential risks.
 - The transfer is necessary for the execution of a contract between the data subject and the data controller or for pre-contractual measures at the data subject's request.
 - The transfer is necessary for the establishment or performance of a contract in favor of the data subject between the data controller and another real or legal person.
 - The transfer is required for an overriding public interest.
 - The transfer is necessary for the establishment, exercise, or protection of a right.
 - The transfer is necessary to protect the life or physical integrity of the person who cannot give consent due to impossibility or whose consent is not legally valid.
 - The transfer is made from a public registry or a registry accessible to persons with legitimate interests, provided legal conditions are met and requested by the interested party.

Personal data may be transferred abroad only with Board permission and after consulting the relevant public institution when international treaty provisions apply or if Turkey's or the data subject's interests would otherwise be seriously harmed.

3. PERSONAL DATA PARAMETERS AND INVENTORY

BELCEHAN processes the personal data of data subjects, including job applicants, employees, shareholders/partners, potential product or service buyers, supplier representatives, service recipients, and visitors, according to the purposes of processing in management, administrative (personnel), financial (accounting), accommodation services, quality, planning, sales and marketing, warehouse, procurement, logistics, and IT (outsourced) business processes. Details on processing purposes and data subject groups are declared in the BELCEHAN field on <https://verbis.kvkk.gov.tr/>.

All personal data processing activities are carried out according to the attached Personal Data Processing Inventory (Annex-6). Disclosure texts, explicit consent texts, and other documents are prepared in accordance with the Inventory and updated when any personal data changes occur.

4. MEASURES FOR THE PROTECTION OF PERSONAL DATA

BELCEHAN implements the technical and administrative measures specified in the attached Personal Data Retention and Destruction Policy (Annex-7) to protect personal data processed in accordance with the law, conducts necessary audits, and carries out awareness and training activities.

Even if all technical and administrative measures are taken, if personal data is unlawfully accessed by third parties, the attached "Personal Data Breach Response Plan" (Annex-8) is applied.

BELCEHAN provides necessary training to employees at the start of employment and annually to ensure lawful processing, access, retention, and awareness of rights regarding personal data. Employees sign the attached "Personal Data Protection Training Participation Form" (Annex-9).

BELCEHAN establishes business processes to increase employees' awareness of protecting personal data, seeks consultant support if needed, evaluates shortcomings, and organizes new training as required by changes in legislation.

Employees sign the attached "Employee Confidentiality Undertaking" (Annex-10) to ensure the confidentiality of personal data obtained. Employees also annually sign the attached "Employee Information Security Awareness Statement" (Annex-11).

Audits of personal data are conducted annually using the attached "KVKK Audit Document" (Annex-12), and deficiencies are corrected promptly.

Security camera monitoring areas, numbers, and timing are implemented to achieve the intended purposes and do not monitor areas that would excessively interfere with personal privacy.

5. RETENTION AND DESTRUCTION OF PERSONAL DATA

BELCEHAN retains personal data for the period necessary for the processing purpose and at least for the minimum period prescribed by law. If a period is defined in relevant legislation, data is retained in accordance with it; if not, data is retained for the period necessary for the processing purpose. At the end of retention periods, personal data is destroyed according to periodic destruction schedules or upon the request of the data subject using the specified method (deletion, eradication, or anonymization). Retention and destruction practices are carried out according to the attached Personal Data Retention and Destruction Policy (Annex-7).

6. RIGHTS OF DATA SUBJECTS AND EXERCISE OF THESE RIGHTS

6.1. Rights of the Data Subject

Data subjects have the following rights under the Law:

- i. To learn whether personal data is being processed,
- ii. To request information if personal data has been processed,
- iii. To learn the purpose of processing personal data and whether it is used in accordance with its purpose,
- iv. To know the third parties to whom personal data is transferred domestically or abroad,
- v. To request the correction of incomplete or inaccurate personal data and to notify third parties to whom personal data has been transferred,
- vi. To request deletion or destruction of personal data even if lawfully processed when the reasons requiring processing no longer exist, and to notify third parties,
- vii. To object to a result arising against themselves through automatic processing of the data,
- viii. To claim compensation in case of damage due to unlawful processing of personal data.

6.2. Exercise of the Data Subject's Rights

Data subjects and those entitled to apply on their behalf may submit their requests regarding the rights listed in Article 6.1 to BELCEHAN by a petition prepared in accordance with Article 13 of the Law and Article 5 of the Communiqué on the Procedures and Principles of Application to the Data Controller, or by filling out the "Data Subject Application Form" (Annex-13), using one of the methods described below:

APPLICATION TYPE	METHOD OF APPLICATION	APPLICATION ADDRESS	APPLICATION DETAILS
1. Written Application	Personal application with wet signature or via Notary	Ölüdeniz Mah. Kıdrak (Old) Cad. Ölüdeniz Otel 1-3 No: 1 C Fethiye/Muğla	The envelope/notification should be marked as "Request for Information within the Scope of the Law on the Protection of Personal Data."

APPLICATION TYPE	METHOD OF APPLICATION	APPLICATION ADDRESS	APPLICATION DETAILS
2. Via Registered Electronic Mail (KEP)	Using KEP address	belcehanturizm@hs01.kep.tr	The subject of the email should be "Request for Information within the Scope of the Law on the Protection of Personal Data."
3. Application Using an Email Address Registered in Our System	Using the email address registered in the company's system	info@belcehanhotel.com	The subject of the email should be "Request for Information within the Scope of the Law on the Protection of Personal Data."
4. Application Using an Email Address Not Registered in Our System	Using an email address not registered in the company's system, including mobile/e-signature	info@belcehanhotel.com	The subject of the email should be "Request for Information within the Scope of the Law on the Protection of Personal Data."

6.3. Response to Applications

BELCEHAN concludes the applications made by the data subject in accordance with the Law and other regulations. Requests submitted to BELCEHAN in compliance with the procedure are processed free of charge as soon as possible and no later than thirty (30) days. However, if the process requires an additional cost, a fee may be charged according to the tariff determined by the Board.

6.4. Rejection of the Data Subject's Application

BELCEHAN may reject the request of the applicant in the following cases, providing justification:

- i. Processing personal data for research, planning, and statistical purposes by anonymizing them for official statistics,
- ii. Processing personal data for artistic, historical, literary, scientific purposes or under freedom of expression, provided that national defense, national security, public safety, public order, economic security, privacy, or personal rights are not violated or constitute a crime,
- iii. Processing personal data within preventive, protective, and intelligence activities carried out by public institutions and organizations authorized by law to maintain national defense, national security, public safety, public order, or economic security,
- iv. Processing personal data in relation to investigation, prosecution, trial, or enforcement procedures by judicial authorities or enforcement offices,
- v. Processing personal data when necessary for preventing the commission of a crime or for the investigation of a crime,

- vi. Processing personal data made public by the data subject themselves,
- vii. Processing personal data by competent public institutions and organizations or professional organizations with public institution status for the execution of audit or regulatory duties, or for disciplinary investigation or prosecution,
- viii. Processing personal data for the protection of the State's economic and financial interests in matters related to budget, tax, and finance,
- ix. If fulfilling the request may infringe on the rights and freedoms of others,
- x. If the request requires disproportionate effort,
- xi. If the requested information is publicly available.

6.5. Right of the Data Subject to Complain to the Personal Data Protection Board

Pursuant to Article 14 of the Law, in the event that the application is rejected, the response is found inadequate, or no reply is given within the legal period, the data subject may complain to the Board within thirty (30) days from the date BELCEHAN's response is learned, and in any case, within sixty (60) days from the date of application.

6.6. Information That May Be Requested from the Applicant Data Subject

BELCEHAN may request information from the applicant to verify whether the applicant is the data subject. BELCEHAN may also ask questions to clarify matters stated in the data subject's application.

7. IMPLEMENTATION

The Principles, together with the annexes, have been approved by the Board of Directors and put into effect.

The Board of Directors is responsible for the implementation and, if necessary, updating of the Law and the Principles, as well as monitoring, coordination, and supervision of all related work and processes through the BELCEHAN Personal Data Protection Committee. The duties, authorities, and working procedures of the Committee are determined in the "Internal Directive of the Personal Data Protection Committee" (Annex-14).

8. EFFECTIVE DATE AND PUBLICATION

The Principles came into effect on 01.12.2025. Any amendments to the Principles are published on BELCEHAN's website (www.belcehanhotel.com) and made accessible to data subjects. Amendments enter into force on the date of publication.

ANNEXES

Annex 1 – Data Categories and Personal Data

Annex 2 – Purposes of Personal Data Processing

Annex 3 – Disclosure Texts

Annex 3.1 – Customer Disclosure Text

Annex 3.2 – Supplier Disclosure Text

Annex 3.3 – Employee Disclosure Text

Annex 3.4 – Job Candidate Disclosure Text

Annex 3.5 – Website Cookie Disclosure Text

Annex 3.6 – Camera Disclosure Text

Annex 3.7 – Transportation Note Disclosure Text

Annex 4 – Recipients of Personal Data and Purpose of Transfer

Annex 5 – Corporate Confidentiality Agreement

Annex 6 – Personal Data Processing Inventory
Annex 7 – Personal Data Retention and Deletion Policy
Annex 8 – Personal Data Breach Response Plan
Annex 9 – Personal Data Protection Training Participation Form
Annex 10 – Employee Confidentiality Undertaking
Annex 11 – Employee Information Security Awareness Declaration
Annex 12 – Personal Data Protection Audit Report
Annex 13 – Data Subject Application Form
Annex 14 – Internal Directive of the Personal Data Protection Committee

ANNEX 1 – Categorical Purposes of Personal Data Processing

- Protection of public health, preventive medicine, conducting medical diagnosis, treatment, and care services
- Implementation of Emergency Management Processes
- Implementation of Information Security Processes
- Conducting Employee Candidate / Intern / Student Selection and Placement Processes
- Managing Employee Candidate Application Processes
- Conducting Employee Satisfaction and Engagement Processes
- Fulfillment of Employment Contract and Legal Obligations for Employees
- Management of Employee Benefits and Perquisites Processes
- Conducting Audit / Ethical Activities
- Implementation of Training Activities
- Management of Access Authorizations
- Ensuring Compliance of Activities with Legislation
- Conducting Finance and Accounting Operations
- Ensuring Physical Facility Security
- Managing Assignment Processes
- Conducting Legal Affairs and Monitoring
- Conducting Internal Audit / Investigation / Intelligence Activities
- Management of Communication Activities
- Planning Human Resources Processes
- Conducting / Supervising Business Operations
- Implementation of Occupational Health / Safety Activities
- Receiving and Evaluating Recommendations for Business Process Improvement
- Ensuring Business Continuity Activities
- Managing Logistics Activities
- Conducting Goods / Services Procurement Processes
- Conducting Goods / Services Sales Processes
- Conducting Production and Operational Processes for Goods / Services
- Organization and Event Management
- Conducting Performance Evaluation Processes

- Conducting Advertising / Campaign / Promotion Processes
- Conducting Risk Management Processes
- Managing Retention and Archiving Activities
- Conducting Contractual Processes
- Tracking Requests / Complaints
- Managing Supply Chain Processes
- Implementation of Compensation Policy
- Ensuring Security of Data Controller Operations
- Conducting Talent / Career Development Activities
- Providing Information to Authorized Persons, Institutions, and Organizations
- Conducting Management Activities

ANNEX 2 – Data Categories and Personal Data

Data Category	Personal Data Examples
Identity	First Name, Last Name, Parent Names, Date of Birth, Place of Birth, Marital Status, ID Card Serial & Number, National ID Number, Passport Number, Temporary ID Number, Gender, Patient Tracking Number, Driver License
Contact	Address, Email Address, Registered Electronic Mail Address (KEP), Phone Number
Employment	Payroll Records, Disciplinary Records, Employment Entry-Exit Documents, CV / Resume Information
Legal	Legal Procedures (information in correspondence with judicial authorities, case files, etc.)
Customer Transactions	Invoice and Check Details, Entry-Exit Records, Appointment Information
Physical Security	Entry-Exit Records of Employees and Visitors, CCTV Footage
Operational Security	IP Address Information, Website Login Records, Password Information
Risk Management	Information processed for managing commercial, technical, and administrative risks
Financial	Financial Statements, Financial Performance Information, Credit and Risk Information, Bank Account Number, IBAN Number
Professional Experience	Diplomas, Courses Attended, In-Service Training, Certificates
Marketing	Customer History, Survey Data, Cookie Records
Promotional Activities	Audio-Visual Materials Collected for Promotional Purposes, Closed-Circuit Camera Footage, Audio Recordings
Health	Disability Status, Blood Type, Personal Health Data, Device and Prostheses Usage, Laboratory and Imaging Results, Test Results

Data Category	Personal Data Examples
Criminal & Security Measures	Information Related to Convictions and Security Measures

ANNEX 4 – Recipients of Personal Data and Purposes of Transfer

In accordance with Articles 8 and 9 of the Law, BELCEHAN may transfer the personal data of participants, customers, and employees to the following categories of recipients:

Recipient Category	Definition	Purpose and Scope of Data Transfer
Natural Persons or Private Legal Entities	<ul style="list-style-type: none"> • Hotel guests (visitors, those who make reservations, event participants) • Employees (staff, interns, temporary workers) • Visitors (individuals entering the hotel premises without staying) • Third-party service providers (drivers, catering staff, private security personnel) 	<ul style="list-style-type: none"> • Execution of reservation and payment processes • Provision of services such as accommodation, restaurant, spa • Customer satisfaction surveys, loyalty programs, and marketing activities • Ensuring security and access control
Authorized Public Institutions and Organizations	<ul style="list-style-type: none"> • General Directorate of Security (guest registration notifications) • Ministry of Finance (tax audits, invoice information) • Social Security Institution (employee insurance records) • Ministry of Health (data sharing for COVID-19 or other health measures) • Municipalities (business licenses and inspection processes) 	<ul style="list-style-type: none"> • Fulfillment of legal obligations (reporting guest information to the police) • Ensuring compliance with tax, insurance, and social security regulations • Implementation of public health and safety measures
Shareholders	<ul style="list-style-type: none"> • Direct or indirect owners of the hotel business • Investors and financial partners • Officials within the parent company or holding structure 	<ul style="list-style-type: none"> • Financial reporting and performance analysis • Board decisions and strategic planning processes • Shareholder information and transparency obligations
Suppliers	<ul style="list-style-type: none"> • Food and beverage suppliers • Cleaning and hygiene product providers 	<ul style="list-style-type: none"> • Management of goods and service procurement processes • Fulfillment of contractual

Recipient Category	Definition	Purpose and Scope of Data Transfer
	<ul style="list-style-type: none"> • Technology and software companies (reservation systems, security software) • External private security companies 	<p>obligations</p> <ul style="list-style-type: none"> • Improving operational efficiency and coordinating logistics processes
Business Partners	<ul style="list-style-type: none"> • Travel agencies and tour operators • Online booking platforms • Airlines or credit card companies involved in joint marketing • Congress and meeting organizers 	<ul style="list-style-type: none"> • Integration of reservation and payment processes • Joint promotions and customer benefit programs • Event management and coordination of group accommodations
