

1. INTRODUCTION

This Personal Data Processing Policy establishes the procedures and principles to be applied by BEŞİK İNŞAAT TAAHHÜT TURZ. TİC. VE İTH. İHR. SAN. LTD. ŞTİ. ("BEŞİK TURİZM"), as data controller, for processing personal data in its possession under Personal Data Protection Law No. 6698 and other applicable legislation.

2. SCOPE

Personal data of employees, candidates, guests and all natural persons whose data are held by BEŞİK TURİZM for any reason are managed lawfully under this policy.

3. DEFINITIONS

Law / KVKK: Personal Data Protection Law No. 6698 dated 24 March 2016.

Board / Authority: The Personal Data Protection Board / Personal Data Protection Authority.

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

Data subject: The person whose personal data are processed.

Explicit consent: Consent on a specific matter, based on information and given freely.

Anonymisation: Rendering personal data incapable of association with an identified or identifiable natural person, even when matched with other data.

Deletion of personal data: Rendering personal data inaccessible and unusable by relevant users in any manner.

Destruction of personal data: Rendering personal data inaccessible, irretrievable and unusable by anyone in any manner.

Processing of personal data: Any operation on data, including obtaining, recording, storing, retaining, altering, reorganising, disclosing, transferring, receiving, making available, classifying or preventing use, performed wholly or partly by automated means or by non-automated means as part of a data filing system.

Authorised employee: A natural person processing personal data on the controller's behalf under its authority.

Data controller: A natural or legal person determining the purposes and means of processing and responsible for establishing and managing the data filing system.

Data processor: A natural or legal person outside the controller's organisation processing personal data on its behalf under its authority.

Special categories of personal data: Data relating to race, ethnic origin, political opinion, philosophical belief, religion, denomination or other beliefs, appearance and dress, association, foundation or trade union membership, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Duty to inform: When personal data are obtained, the controller or its authorised person informs data subjects of the identity of the controller and any representative, processing purposes, recipients and transfer purposes, collection methods and legal basis, and the other rights in Article 11 of the Law.

Elektraweb: The front office, accounting and purchasing automation system containing guest data.

Disposal: Deleting, destroying or anonymising personal data.

Disposal policy: The policy used by controllers to determine the maximum period required for processing purposes and as the basis for deletion, destruction and anonymisation.

Recording medium: Any electronic medium containing personal data processed wholly or partly by automated means or by non-automated means as part of a data filing system.

Netahsilat: Online payment system.

Company: BEŞİK İNŞAAT TAAHHÜT TURZ. TİC. VE İTH. İHR. SAN. LTD. ŞTİ.

4. PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

4.1. Lawfulness and Fairness

The Company protects data subjects' individual rights when processing personal data. Data are collected and processed lawfully and fairly.

4.2. Specific, Explicit and Legitimate Purposes; Relevance, Limitation and Proportionality

The Company determines processing purposes before processing begins and processes personal data solely to provide better services to data subjects. When data are obtained, the data subject is informed of the controller's and any representative's identity, processing purposes, potential recipients and transfer purposes, collection methods and legal basis, and the data subject's rights.

4.3. Retention for the Period Prescribed by Legislation or Required for the Purpose

The Company retains data only for the period prescribed by legislation or necessary for processing purposes. While retention is considered necessary for those purposes or required by regulators or applicable laws and regulations, the Company and its controlled affiliates continue to process and retain data for the purposes established by this policy.

4.4. Accuracy and Currency

The Company keeps processed data accurate, complete and, where necessary, current. Inaccurate or incomplete data are deleted, corrected, completed or updated when needed.

4.5. Confidentiality and Data Security

Personal data are subject to confidentiality and treated as confidential at an individual level. Necessary technical and administrative measures provide appropriate security, preventing unauthorised access, unlawful processing or distribution and accidental loss, alteration or destruction, and ensuring retention and protection.

5. SCOPE OF DATA PROCESSING

Personal data processing takes two forms.

Wholly or partly automated processing includes receiving, collecting, recording, photographing, making audio or video recordings, organising, storing, altering, restoring, retrieving or disclosing data from the data subjects or third parties identified in this policy, for transfer, dissemination or other provision, grouping or combination, blocking, deletion or destruction.

Non-automated processing / acquisition, where part of a filing system, includes recording, storing, retaining, altering, reorganising, disclosing, transferring, transferring abroad, receiving, making available, classifying or preventing use.

5.1. The Company has the right to process the data subject's personal information during use of its services and after the service relationship ends, in accordance with the purposes in this policy.

5.2. Company processing includes all operations on data, without limitation, using automated, semi-automated or non-automated means forming part of an automated system.

5.3. The Company processes data of the data subject and persons under the data subject's parental custody.

5.4. Processing also includes sharing data supplied with the explicit consent of the data subject or third parties under the Company's instructions, or when the Company acts as processor for and on the instructions of a third party.

5.5. Explicit consent also covers the Company recording and processing activities when the data subject uses electronic channels, including web browsers, websites, the internet, mobile applications, payment processes and technical means and channels for sending and receiving money. Examples include determining location, identifying and analysing input data, product selection frequency and other statistical data.

6. BASES FOR DATA PROCESSING

6.1. The data subject accepts that, during use of Company services and after the contractual relationship ends, the Company needs to process information about the data subject or third parties identified by them for:

- (a) Providing or implementing a service for the data subject.
- (b) Processing necessary to protect the legal rights of the Company or third parties.
- (c) Fulfilling the Company's legal obligations.
- (d) Processing the data subject's personal data where necessary and directly related to the establishment or performance of a contract between them and the Company.
- (e) Processing necessary to establish, exercise or protect a right.
- (f) Other matters to which the data subject explicitly consents.
- (g) Other matters expressly prescribed by legislation.

6.2. The data subject's explicit consent means that they accept the policy and its provisions.

7. PURPOSES OF DATA PROCESSING

The Company and third parties processing data shared with data subjects' consent may process data about data subjects or persons under their parental custody for:

- (a) Providing accommodation as described and delivering and conducting services for guests more effectively and reliably.
- (b) Enabling online payments and collections through Netahsilat using guest names, birth dates, email addresses, telephone numbers and credit card information; conducting information research and evaluating surveys; providing planning, statistical, archiving and retention services; and conducting customer satisfaction studies.
- (c) Reviewing accommodation history or behaviour patterns where needed to optimise and improve services.
- (d) Offering a new or additional service or a product outside the service offering.
- (e) Changing the current conditions of a service offered by the Company.
- (f) Analysing statistical data and preparing and presenting reports, research or presentations.
- (g) Ensuring security and detecting or preventing misuse and other criminal activities.
- (h) Responding to complaints, questions and requests.
- (i) Verifying identity information.
- (j) Conducting advertising, marketing, promotional and campaign activities for accommodation services.
- (k) Achieving other purposes prescribed by national and international laws and legislation.

8. PROCESSING, TRANSFER OR DISCLOSURE OF DATA

The Company fulfils obligations imposed by applicable legislation and the Board's principle decisions concerning processing, transfer and disclosure. For the purposes in this policy, and depending on the content and variety of accommodation services, information about data subjects and third parties may be processed, transferred or disclosed, including, without limitation:

- First and last names; personal identity number or a distinctive identifier on an identity card; registered or residential address; telephone or mobile telephone number; and email address.
- Employer data and employment conditions, such as workplace, pay and working hours.
- Activities of the data subject or third parties identified by them when using electronic channels or the internet, including cookies, channel authentication, actions and transaction history.
- Data about persons staying with the data subject during the service period.

8.1. Where a data subject provides third-party data, including personal data or special categories of data of family members, employers or others, to benefit from Company services, the person providing the data is responsible for

obtaining the necessary consent for processing.

8.2. If the data subject supplies this information to the Company or authorised staff, the necessary explicit consent is deemed given and the Company's obligation to obtain that explicit consent ceases.

8.3. If personal data or special categories of data are processed without explicit consent and the data subject suffers damage as a result, the Company is obliged to compensate that damage.

8.4. Explicit consent also covers recording and processing activities when using electronic channels, including browsers, websites, the internet, mobile applications, payments and technical means for money transfers and receipts. Examples include determining location and identifying and analysing input data, product selection frequency and other statistical data.

8.5. Until the data subject exercises the right to refuse, the Company may use provided telephone numbers, mobile numbers, email addresses and other contact details to send commercial electronic communications under Law No. 6563 on the Regulation of Electronic Commerce, including SMS, voice or other marketing messages (direct marketing).

8.6. The data subject grants the Company the right to share personal data with its subsidiaries or shareholders to make marketing offers.

8.7. Advertising or information messages at Company service points, such as brochures, promotional visuals and verbal offers, or content displayed when using electronic channels such as the internet and mobile marketing by the Company or its subsidiaries, are not considered direct marketing. The data subject has no right to request that publication or display of such content cease.

9. PROCESSING APPLICANTS' OR EMPLOYEES' DATA

9.1. Establishing, Performing, Maintaining and Terminating Employment Agreements

The Company may process personal information disclosed when a person starts employment, probation or an internship to fulfil and maintain employment rights; provide occupational health and safety services; carry out work permit procedures; assess job applications and conduct research and recruitment; assess and monitor performance; conduct training; improve working conditions; and carry out personal development, HR and training processes.

Information about applicants collected from third parties during recruitment is obtained under Law No. 6698. Explicit consent is required for processing employment-related data that are not initially part of performing the employment agreement.

9.2. Processing Special Categories of Personal Data

Special categories of personal data may be processed only with the data subject's explicit consent. Categories other than health and sexual life may be processed where provided for by law. Health and sexual-life data are processed by persons bound by confidentiality or authorised institutions and organisations for public health protection, preventive medicine, medical diagnosis, treatment and care, and planning and management of health services and their financing.

10. TRANSFER / SHARING OF INFORMATION TO / FROM THIRD PARTIES

Within processing necessary to provide services, this policy is transferred or shared with the data subject or third parties identified by them. The data subject grants the Company the right to obtain, record, store, retain, alter, reorganise, disclose, transfer, transfer abroad, receive, make available, classify or use personal data, wholly or partly by automated means or by non-automated means as part of a filing system, through its departments, the internet, call centres, public bodies and suppliers or parties providing complementary services or extensions of its activities.

11. OBLIGATIONS OF THE DATA CONTROLLER AND PROCESSOR

11.1. Under this policy, the Company may act as processor for certain types of data on a controller's behalf, including for third parties. A controller may also act as processor for third parties for certain data. Each party to such a relationship, whether controller or processor, complies with the Personal Data Protection Law. Accordingly:

- (a) Data are processed in accordance with statutory principles.
- (b) Explicit consent is obtained and the necessary information and notices are provided.

When a data subject requests information about their data or submits a complaint or statement concerning the controller's compliance with legal obligations, the controller notifies them as soon as possible and within 30 days at the latest.

Where one party acts as processor and the other as controller, the processor must:

- (i) Process data supplied or disclosed by the other party within the limits and scope in this policy and permitted by legislation, or at a regulator's request.
- (ii) Take all reasonable technical and administrative measures and necessary action against unauthorised processing, loss, destruction, damage, alteration or disclosure of data supplied by the controller, and inform the controller of each measure.
- (iii) Allow the Company, through authorised staff, to audit the measures and practices implemented for data security.
- (iv) Cooperate and assist in examining complaints or statements supplied or disclosed by the Company, including the matters below.
- (v) Provide the Company, within 7 business days of request, with detailed information concerning the complaint or statement, including electronic data about data subjects supplied by the controller to the processor.
- (vi) Prevent processing or transfer to a country or international organisation outside the European Economic Area that is not on the list of countries offering adequate personal data protection, or for which transfer has not been permitted by the data subject or the Personal Data Protection Board.
- (vii) Not transfer or disclose data to third parties without the Company's prior explicit written consent.
- (viii) Even with that consent, transfer or disclose data only under a written agreement requiring the third party and its subcontractors to take all necessary technical and administrative measures against unauthorised processing, loss, destruction, damage, alteration or disclosure.
- (ix) Compensate all damage or loss suffered by the Company because the processor fails to take or fully perform the actions required by this policy and legislation. The processor expressly consents and agrees with the controller to remedy and indemnify all damage or loss, including consequential loss, complaints, expenses including those of exercising legal rights, legal proceedings and other obligations arising from a breach.
- (x) Unless otherwise agreed in the contract, after the contractual relationship ends, return all data, including personal data, transferred or disclosed by the Company; take all necessary measures to prevent unauthorised third-party access; destroy personal data supplied by the Company; and notify the Company to confirm those actions.

12. DATA UPDATES, PROCESSING, RETENTION PERIOD AND DISPOSAL

12.1. During use of Company services and afterwards, processing continues for the purposes in this policy for a period consistent with Company purposes and interests, supervisory or regulatory requirements and legislation.

12.2. Data transmitted when using Company electronic channels, including browsers, websites, the internet, mobile applications or other electronic transfer tools, continue to be processed even after the data subject deletes them from those channels.

12.3. At the data subject's request, information about their data held by the Company is provided within the scope permitted by legislation.

12.4. Incomplete or inaccurate data held by the Company are completed or corrected when the data subject notifies the Company in writing.

12.5. Personal data are retained for the period prescribed by legislation or required for the processing purpose and, in any event, for 10 years. Even if lawfully processed, they are deleted, destroyed or anonymised by the controller on its own initiative or at the data subject's request when the grounds requiring processing cease and the Company's retention period expires.

12.6. The following criteria are used to determine retention and disposal periods:

- (a) The applicable exceptions in Articles 5 and 6 are identified, and an access authorisation and control matrix is used. Relevant users are determined for each item of data, along with their rights and methods for access, retrieval and reuse. On termination of employment, position changes or similar events, these permissions and methods are updated, disabled or removed.
- (b) When a statutory retention period expires, or legislation does not prescribe a period, the controller deletes, destroys or anonymises the data in 10-year cycles.

12.7. Deletion, destruction and anonymisation comply with the principles in Article 4 (General Principles), measures under Article 12 (Data Security Obligations), applicable legislation, Authority decisions and this policy.

12.8. The Company records every deletion, destruction and anonymisation operation. Records are retained for at least 10 years, without prejudice to other legal obligations.

12.9. Unless the Personal Data Protection Authority decides otherwise, the Company chooses the appropriate deletion, destruction or anonymisation method.

12.10. Personal data are stored in various recording media and deleted using suitable methods. Digital data are deleted by a deletion command or manually. Paper data are deleted by blacking out: cutting out the information where possible, or using permanent ink to make it invisible to relevant users and incapable of recovery or reading through technological solutions.

Office files on the central server are deleted using the operating system's deletion command or by removing the relevant user's access rights to the file or its directory.

Use of portable storage is restricted by authorisation. Databases holding personal data are protected by authorisation levels, and deletion requires permission. It is taken into account whether the relevant user is also the database administrator.

Destruction renders data inaccessible, irretrievable and unusable by anyone in any manner. The Company, as controller, takes all necessary technical and administrative measures. All copies are identified, and systems holding data, optical media and magnetic media are physically destroyed by melting, burning, pulverising or metal shredding, ensuring data cannot be accessed.

Network devices such as switches and routers are handled using deletion commands. Mobile telephone SIM cards and fixed memory areas, including smartphone memory, are handled through deletion commands and physical destruction. Optical storage such as CDs and DVDs is destroyed by burning, breaking into small pieces or melting.

For faulty devices or devices sent for maintenance, storage media holding personal data are removed and retained, while other faulty parts are sent to manufacturers, sellers or service providers. Measures prevent external maintenance or repair staff from copying data and taking them outside the organisation. Necessary confidentiality agreements are in place with maintenance companies.

Anonymisation removes or changes all direct or indirect identifiers in a dataset to prevent identification or distinguishing a person within a group in a way that can be associated with a natural person. Its purpose is to break the link between data and the person described. A suitable method is selected from automated or non-automated grouping, masking, generalisation, randomisation or similar methods applied to filing-system records.

13. DATA SUBJECT RIGHTS

Every data subject has the right to learn whether their data are processed; request information if processed; learn the purposes and whether use is consistent with them; learn third-party recipients in Türkiye or abroad; request correction of incomplete or inaccurate data; request deletion or destruction; request notification of transfers to third parties in Türkiye or abroad; object to a detrimental result arising exclusively from automated analysis; and request compensation for damage caused by processing contrary to the Law.

14. CONFIDENTIALITY OF DATA PROCESSING

14.1. Personal data are subject to data security. Unauthorised access by employees of the Company, affiliates or subsidiaries is prevented, and processing or use by unauthorised persons is strictly prohibited. Processing by an employee not authorised under their job description is unauthorised processing. Employees may access data only where their job description includes that authority.

14.2. Employees are prohibited from using data for private or commercial purposes, sharing them with unauthorised persons or otherwise making them available. The controller informs employees at the start of employment of their duty to protect confidentiality and provides or arranges training.

14.3. Subject to Law No. 6698, video and audio recordings are made around buildings and workplaces, at their entrances, in kitchens, service back-of-house areas and similar locations to protect property and confidentiality and monitor and measure service quality.

14.4. Data subjects are informed that video recording and surveillance using appropriate tools take place at relevant Company service points and when communicating with the Company. They acknowledge the importance of video and audio recordings and, under this clause, give explicit consent to the Company processing their data in this respect.

15. DATA PROCESSING SECURITY

Data are protected against unauthorised access, unlawful processing or disclosure and accidental loss, alteration or destruction, whether processed electronically or on paper. New and advanced processing methods and IT systems are monitored for technical and administrative protection measures.

16. DATA PROTECTION CONTROL

Authorised persons in the relevant Company units regularly monitor compliance with this policy and applicable data protection laws. To the extent permitted by national laws, the Personal Data Protection Authority may itself audit compliance by the Company, affiliates and subsidiaries.

17. CONTACT

When a data subject submits written requests concerning application of this policy or the Personal Data Protection Law to the controller, the controller concludes them free of charge as soon as possible, depending on their nature, and within 30 days at the latest. If the procedure requires an additional cost, fees under the tariff determined by the Personal Data Protection Board are charged.

CONTACT INFORMATION

Address : Ölüdeniz Mahallesi Ata Cad. No:6
Hisarönü FETHİYE / MUĞLA
Phone : +90 (252) 616 76 46
Fax : +90 (252) 616 82 07

Responsible Person : Ali Tunç
Contact Person : Ali Tunç
E-mail : info@oceanbluehotel.com.tr
Website : www.oceanbluehotel.com.tr