

1. PURPOSE / SCOPE

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

Personal data of employees, candidates, guests, visitors, outsourced service providers, suppliers and all natural persons whose data are held by BEŞİK TURİZM for any reason are managed lawfully under the Personal Data Processing and Protection Policy and this Personal Data Retention and Disposal Policy.

2. DEFINITIONS AND ABBREVIATIONS

Data subject: The natural person whose personal data are processed.

Disposal: Deleting, destroying or anonymising personal data.

Law: Personal Data Protection Law No. 6698, published in the Official Gazette.

Regulation: The Regulation on the Deletion, Destruction or Anonymisation of Personal Data, published in the Official Gazette.

Board: The Personal Data Protection Board.

Relevant user: Persons who process personal data within the data controller's organisation or under the controller's authority and instructions, excluding the person or unit responsible for technical storage, protection and backup.

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

Personal Data Processing and Protection Policy: The policy establishing procedures and principles for managing personal data held by BEŞİK TURİZM.

Data filing system: A recording system in which personal data are structured and processed according to specified criteria.

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

Data controller: The 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 data on its behalf under its authority.

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

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.

Systems and Applications

System	Function
Elektraweb	Front office operating system.
Elektraweb	Accounting and Human Resources operating system.
SETROW	Bulk email system.
Elektraweb	Reporting program.
Elektraweb	Reservation and order program.
Elektraweb	À la carte reservation system.
Elektraweb	Stock management program.
WhatsApp	Multiple-notification platform.
AVISION	Identity information scanning system.
HAIKON	Camera recording system.
Brassco card lock	Room door identification system.
Elektraweb	Cloud-based operating system.
Xlog A Security	Firewall.
QNAP	Backup unit.
Kaspersky	Antivirus program.

3. STORAGE MEDIA AND SECURITY MEASURES

3.1. Media in Which Personal Data Are Retained

Personal data held by BEŞİK TURİZM are kept in a recording medium appropriate to the nature of the data and our legal obligations.

The media generally used are listed below. Some data may be held in other media because of their special characteristics or our legal obligations. BEŞİK TURİZM always acts as data controller and processes and protects data in accordance with the Law, the Personal Data Processing and Protection Policy and this policy.

- (a) Printed media: Media in which data are kept as printed records on paper.
- (b) Local digital media: Servers, fixed or portable drives, optical discs and other digital media within BEŞİK TURİZM.
- (c) Cloud media: Internet-based systems outside BEŞİK TURİZM that it uses, encrypted through cryptographic methods (Elektraweb).

3.2. Ensuring the Security of Storage Media

BEŞİK TURİZM takes all necessary technical and administrative measures appropriate to the data and the media to ensure secure retention and prevent unlawful processing and access. These include, without limitation, the following measures where suited to the nature of the data and media.

3.2.1. Technical Measures

- Only current, secure systems appropriate to technological developments are used in data storage media.
- Security systems are used for media holding personal data.
- Security testing and research identify IT vulnerabilities, and existing or potential risks found are remedied.

- Access to data storage media is restricted to authorised persons and limited to the processing purpose. All access is recorded.
- Sufficient technical staff are employed to ensure the security of storage media within BEŞİK TURİZM.

3.2.2. Administrative Measures

- All employees with access to data receive training to improve awareness of information security, personal data and privacy.
- Legal and technical consultancy is obtained to follow developments in information security, privacy and data protection and take necessary action.
- When technical or legal requirements require transfer to third parties, data protection protocols or agreements are signed, and due care is taken to ensure those parties comply.

3.2.3. Internal and External Audits

Under Article 12 of the Law, BEŞİK TURİZM commissions internal and external audits of compliance with the Law, this policy and the Personal Data Processing and Protection Policy.

Deficiencies or faults identified in applying these provisions are remedied immediately.

If an audit or another means reveals that personal data under BEŞİK TURİZM's responsibility have been obtained unlawfully by others, the data subject and the Board are notified as soon as possible.

4. DISPOSAL OF PERSONAL DATA

4.1. Grounds for Retention and Disposal

4.1.1. Grounds for Retention

Personal data held by BEŞİK TURİZM are retained for the purposes and reasons stated in the Law and its Personal Data Processing and Protection Policy.

4.1.2. Grounds for Disposal

Personal data are deleted, destroyed or anonymised under this policy at the data subject's request or on the Company's initiative when the grounds listed in Articles 5 and 6 of the Law cease to apply. Those grounds are:

- Processing being expressly provided for by law.
- Processing being necessary to protect the life or physical integrity of a person unable to express consent because of factual incapacity, or whose consent is not legally valid, or of another person.
- Processing of contracting parties' data being necessary and directly related to the establishment or performance of a contract.
- Processing being necessary for the controller to fulfil a legal obligation.
- The data having been made public by the data subject.
- Processing being necessary to establish, exercise or protect a right.
- Processing being necessary for the controller's legitimate interests, provided that the data subject's fundamental rights and freedoms are not harmed.

4.2. Disposal Methods

When the grounds requiring processing cease to apply, BEŞİK TURİZM deletes, destroys or anonymises personal data retained under the Law, other legislation and the Personal Data Processing and Protection Policy, at the data subject's request or on its own initiative within the periods specified in that policy.

The most commonly used techniques are set out below.

4.2.1. Deletion Methods

Personal data in printed media - blacking out: Data are deleted by cutting the personal information out of the document where possible, or by making it invisible using permanent ink so that it cannot be recovered or read using technological solutions.

Personal data in cloud and local digital media - secure software deletion: Data are deleted by a digital command in a manner that prevents recovery. Data deleted in this manner cannot be accessed again.

4.2.2. Destruction Methods

Printed media - physical destruction: Printed documents are destroyed by shredding machines so that they cannot be reassembled.

Local digital media - physical destruction: Optical and magnetic media holding data are physically destroyed by melting, burning, pulverising or passing through a metal shredder, making the data inaccessible.

Cloud media - secure software deletion: Data are deleted by digital command so they cannot be recovered. When the cloud service relationship ends, all copies of the encryption keys needed to make the data usable are destroyed. Data deleted in this manner cannot be accessed again.

4.2.3. Anonymisation Methods

Anonymisation makes personal data incapable of association with an identified or identifiable natural person, even when matched with other data. Anonymised data are data that have been rendered incapable of such association.

Removing variables: Removing one or more direct identifiers that could identify the data subject. This may be used for anonymisation or for deleting information that is not relevant to the processing purpose.

Local suppression: Removing information that could distinguish an exceptional entry within a table containing aggregated anonymised personal data.

Generalisation: Combining data from many persons and removing distinguishing information to produce statistical data.

Lower and upper bound coding / global coding: Defining ranges for a variable and categorising it. Where the variable is not numerical, similar values are categorised. Values in the same category are combined.

Micro-aggregation: All records are first placed in a meaningful order and the dataset is divided into a specified number of subsets. The value of a selected variable in each subset is replaced by the subset's mean for that variable. This changes indirect identifiers and makes association with a data subject more difficult.

Data shuffling and perturbation: Direct or indirect identifiers are mixed with other values or altered to break the connection to the data subject and remove their identifying character.

4.2.4. Retention and Disposal Periods

4.2.4.1. Retention Periods

Employee: Recruitment documents and personnel data underlying Social Security Institution notifications on service length and wages are retained during employment and for 10 (ten) years after its termination.

Other employee personnel data are retained during employment and for 10 (ten) years from the beginning of the calendar year following termination.

Data in workplace personal health files are retained during employment and for 10 (ten) years after termination.

Business partner: Identity, contact and financial information, audio recordings of telephone calls and data about employees of business partners, solution partners and consultants relating to the commercial relationship with BEŞİK TURİZM are retained throughout the relationship and for 10 years after it ends under Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code.

Visitor: Names, Turkish identity or other identity numbers, vehicle registration plates, CCTV recordings and audio recordings of telephone calls collected in connection with entry to BEŞİK TURİZM premises are retained for 2 years.

Website visitor: Names, email addresses and browsing activity information are retained for 2 (two) years.

Candidate: CV and job application information are retained for as long as the CV remains current, up to a maximum of 2 (two) years.

Intern (student): Information in the internship file is retained throughout the internship and for 10 (ten) years from the beginning of the calendar year following its termination.

Guest: Names, Turkish identity or other identity numbers, contact details, payment details and methods, location information, audio recordings of telephone calls, service preferences, transaction history and special occasion information are retained for 10 years from the provision of each purchased service under Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code.

Guest security camera images are retained for a maximum of 60 (sixty) days; in-vehicle camera images for 2 (two) days; and vehicle registration plate information for 2 (two) years.

Institutions / companies cooperating with BEŞİK TURİZM (suppliers): Identity, contact and financial information, audio recordings of telephone calls and employee data relating to the commercial relationship are retained throughout the business or commercial relationship and for 10 years after it ends under Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code.

4.2.4.2. Disposal Periods

BEŞİK TURİZM deletes, destroys or anonymises data for which it is responsible under the Law, legislation and these policies at the first periodic disposal following the date on which the obligation arises.

When a data subject applies under Article 13 of the Law to request deletion or destruction:

- If all processing conditions have ceased to apply, BEŞİK TURİZM deletes, destroys or anonymises the requested data using an appropriate method within 30 (thirty) days of receipt, explaining its reasons. For the request to be considered received, it must be submitted in accordance with the Personal Data Processing and Protection Policy. The data subject is informed of the action taken in all cases.
- If not all processing conditions have ceased to apply, the request may be rejected with reasons under Article 13(3). The rejection is notified in writing or electronically within thirty days at the latest.

4.2.5. Periodic Disposal

When all conditions for processing under the Law cease to apply, BEŞİK TURİZM deletes, destroys or anonymises the data on its own initiative at the recurring intervals specified in this policy. The data are disposed of in the first periodic deletion, destruction or anonymisation cycle.

4.3. Monitoring the Lawfulness of Disposal

BEŞİK TURİZM performs disposal, whether requested or initiated during periodic disposal, in accordance with the Law, other legislation, the Personal Data Processing and Protection Policy and this policy. It takes administrative and technical measures to ensure compliance.

4.3.1. Technical Measures

- Suitable technical tools and equipment are maintained for every disposal method in this policy.
- The location where disposal takes place is secured.
- Access records of the persons carrying out disposal are kept.
- Qualified, experienced personnel are employed or services are obtained from competent third parties where necessary.

4.3.2. Administrative Measures

- Employees performing disposal receive awareness training on information security, personal data and privacy.
- Legal and technical consultancy is obtained to follow developments in information security, privacy, data protection and secure disposal techniques and take necessary action.
- When disposal is outsourced because of technical or legal requirements, data protection protocols are signed and due care is taken to ensure third-party compliance.
- Disposal is regularly audited for compliance with the Law and the conditions and obligations in this policy, and necessary action is taken.

- All deletion, destruction and anonymisation operations are recorded. These records are retained for at least three years, without prejudice to other legal obligations.

5. PERSONAL DATA PROTECTION COMMITTEE

BEŞİK TURİZM establishes an internal Personal Data Protection Committee. It is authorised and responsible for carrying out or arranging the necessary actions and supervising processes to ensure data are retained and processed under the Law, the Personal Data Processing and Protection Policy and this policy.

The committee comprises three persons: a manager, an administrative specialist and a technical specialist. The titles and job descriptions of its BEŞİK TURİZM employee members are listed in the Personal Data Protection Committee Member List.

6. UPDATES AND COMPLIANCE

BEŞİK TURİZM reserves the right to amend the Personal Data Processing and Protection Policy or this policy because of changes in the Law, decisions of the Authority, or developments in the sector or information technology.

Changes to this policy are incorporated into the text immediately, and explanations of the amendments are provided at the end of the policy.



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