

Information on the Processing of Personal Data

Beşik İnşaat Taahhüt Turz. Tic. Ve İth. İhr. San. Ltd. Şti. (the "Company"), acting as data controller, provides this notice under Personal Data Protection Law No. 6698 (the "Law") to inform employees of the procedures and principles for processing their personal data. Under Article 10 of the Law, when personal data are obtained, the data controller or its authorised representative must inform data subjects of:

- The identity of the data controller and, where applicable, its representative.
- The purposes for which personal data will be processed.
- To whom and for what purposes the processed personal data may be transferred.
- The method and legal basis for collecting personal data.
- The other rights listed in Article 11.

Within our commercial or employment relationship with you, your personal data will be recorded, stored, retained, reorganised, shared with legally authorised institutions, transferred or assigned to third parties in Türkiye or abroad, categorised and otherwise processed as listed in the Law. Processing will be connected with, limited to and proportionate to the relevant purpose, and will preserve the accuracy and currency of the information you have provided or that has been provided to us.

The Company attaches particular importance to personal data security and takes all necessary technical and administrative measures. Personal information is requested from employees during job applications, at the signing of the employment agreement and during employment to provide better services to employees, fulfil legal obligations, improve communication and understand their needs and interests.

Under Article 4 of the Law, personal data will be processed:

- Lawfully and fairly.
- Accurately and, where necessary, kept up to date.
- For specific, explicit and legitimate purposes.
- In a manner connected with, limited to and proportionate to the purposes of processing.
- Retained for the period prescribed by the relevant legislation or required for the purpose of processing.

Under the Law, any information that can be associated with a natural person, whether kept electronically or in print, including the categories listed below, is personal data. The Company or natural or legal persons processing data on its behalf may collect personal data on different legal grounds, orally, in writing or electronically, through websites, email, mobile communications, mobile applications, application and membership forms, various contracts and other channels.

Personal data may be shared with relevant institutions and organisations where required by law. They are processed lawfully and fairly, accurately and, where necessary, kept current, for specific, explicit and legitimate purposes and in a manner connected with, limited to and proportionate to those purposes.

All personal data held in personnel files or electronically are retained electronically or otherwise during employment and for a period thereafter to fulfil obligations to employees, support recruitment checks, evidence work, establish working hours and daily start and end times, monitor absence, audit attendance records, record wages and wage-related information, make notifications to the Social Security Institution and other bodies, implement occupational health and safety legislation, fulfil statutory obligations and determine working conditions.

Personnel files will be retained for 10 years after the termination of employment, with all necessary technical and administrative measures.

Personal Data Processed

Identity: First and last names, date of birth, nationality, place of birth, gender, marital status, Turkish identity card details (identity number, serial number, card number, parents' names, place of birth, province, district, neighbourhood, register volume, family sequence, individual sequence, household, page and registration numbers, place, reason and date of issue, previous surname), identity card copy, passport and passport number, residence card, driving licence and other identification documents, such as a lawyer's identity card.

Personal Data Processing and Protection Employee Privacy Notice

Contact: Telephone number, full address, email address and internal Company contact details, including extension number and corporate email address.

Financial: Financial and salary details, payrolls, bonus entitlements and amounts, file and debt information relating to enforcement proceedings, bank account passbook, IBAN and minimum living allowance information.

Special Categories of Personal Data: Former-convict status or criminal record; disability status, description and percentage; religion; health data; blood group; medical reports; carrier screening reports; temporary or permanent incapacity reports; pre-employment medical report; chest X-ray; hearing and vision tests; liver enzyme screening; hepatitis tests; pre-employment and periodic examination forms signed by the occupational physician; drug tests; pregnancy status and reports; health and maternity leave information; and trade union, association or foundation memberships.

Education: Educational status, certificate and diploma information, foreign language knowledge, education and skills, CV, courses and seminars attended.

Visual and Audio Data: Photographs of the person, audio recordings, CCTV recordings and videos, such as birthday celebration videos.

Employee Performance and Career Development: Education and skills, training taken and dates, signed attendance forms, monthly performance assessment and target achievement, activity information and probation assessment forms.

Family and Relatives: Marriage certificate; spouse's and children's names, Turkish identity numbers, gender, birth dates, height, weight and occupation; and emergency contacts' names, telephone numbers and full addresses.

Employment: Personnel number, position, department and unit, title, latest employment start date, employment entry and exit dates, insurance entry or retirement allocation number, social security registration number, flexible working status, travel status, total monthly working hours, severance pay reference date and additional days.

Leave: Leave seniority reference date, additional seniority days, leave group, departure and return dates, number of days used, reason for leave, address and telephone number during leave and information on leave for personal reasons.

Other: Military service deferment, shoe size, clothing size, height, weight, vehicle registration plate and mileage, internship status, shuttle services and stops used, employee internet access logs, entry and exit logs, daily activity data, vehicle GPS tracking records and personal protective equipment allocation records.

Human Resources, Payroll and Salary Processes

Personal data are processed to create personnel files containing all documents on the recruitment checklist; manage recruitment and termination; calculate wages; fulfil legal obligations to bodies such as the Social Security Institution, İŞKUR, Police Directorate and Gendarmerie; monitor annual and personal leave; conduct all HR processes; follow litigation, enforcement and other legal processes; report occupational accidents; carry out monitoring required by occupational health and safety legislation; comply with court decisions; and meet other retention, reporting and notification obligations prescribed by legislation, regulators and other authorities.

Personnel Attendance Control System (PDKS)

The system operates using facial recognition records. If it fails to recognise an employee, the employee writes a report explaining the situation at the Human Resources Department so that attendance can be recorded.

The IT Department backs up the facial recognition system. The system is used to ensure entry and exit through a single point and to identify who is inside the building in extraordinary emergencies, such as a fire.

The HR Department keeps records showing work start and finish times to implement and monitor time off in lieu and balancing of working hours. Balancing and overtime calculations are based on shift start and finish times rather than the times of entry into and exit from the workplace.

Training and Career Planning

To identify career planning and training needs, personal information such as educational status, certificates, legally required training attendance forms and certificates, internal training and previous training is retained in personnel files and the training portal.

Camera Surveillance System

Cameras are installed at various Company locations, including staff accommodation. They are used for the general security of employees, candidates, guests, outsourced service providers, suppliers and visitors. The workplace is also monitored twenty-four hours a day, seven days a week for occupational health and safety and to enable emergency intervention in accidents or similar situations. Additional cameras may be used if necessary.

Company Telephones and Telephone Lines

Where a Company telephone and line are provided, handover records are prepared. Following termination of employment, written messages and calls may be seen during the formatting of the returned telephone and line. Written messages may be examined in this context. Personal, private or confidential correspondence and calls should not be made using the Company telephone.

Company Mailbox Checks, Internet Traffic Monitoring and Access Logs

Upon termination of employment, the IT Department changes the passwords of the electronic devices used by the departing employee, such as computers and telephones, on the termination date. To avoid disruption to guests and business contacts and ensure uninterrupted services, the mailbox remains active for 2 (two) months. Incoming mail is monitored by the IT Department and the relevant department manager. Historical emails and attachments may be opened for business purposes.

The IT Department may inspect mail and internet traffic at any time and impose restrictions to monitor unlawful copying, business activities or research, unauthorised software installation or use, recreational participation in online communities, chat rooms and forums, bulk email, music sites, sites that may transmit viruses, inappropriate sites contrary to public morality or customs, harassment, gambling, betting and similar inappropriate conduct.

Internet access logs are kept by the IT Department under Company rules and applicable laws. Management may restrict access to sites it considers inappropriate, including to prevent unnecessary mail exceeding server capacity or the risk of viruses.

Personal, private and confidential correspondence or documents should therefore not be created or handled on Company computers.

Birthdays, Marriage and Parenthood

To support employees on happy occasions, such as birthdays, marriage and the birth of a child, and on difficult occasions, such as accidents or bereavement, information about these events may be announced through internal email and staff noticeboards.

Sharing Blood Group Information

If employees or their relatives need blood, the employee's name, telephone number and the required blood group may be communicated to all Company employees by email, mobile messages or internal noticeboards to meet the need quickly.

Reference Checks on Recruitment and Departure

The Company may exchange information with the references provided in an application and during probation to learn about work ethics. This applies during the 2 (two) month probation period. After employment ends, if a new workplace contacts the Company for a reference, information about the former employee may be exchanged with the requesting persons. If you do not permit reference checks, you must inform us when leaving employment.

Use of Employee Images and Audio for Hotel Promotion

We use internal and external communications to promote the hotel and its services, including services for congresses, weddings and meetings. Videos and photographs of these services are taken and used on the Company's social media accounts and in training. Employees' images or voices may need to be included solely for the promotion of these services.

Vehicle Tracking System

Company vehicles are obtained through purchased services or ownership. Vehicle entry and exit information, registration plates, mileage and driver details are recorded, monitored and reported at security and staff entrances. This is solely for vehicle safety, including emergency intervention in breakdowns and fuel monitoring, rather than obtaining information about employees' private lives.

Friendly Employee of the Month, Draws and Similar Events

Friendly employees of the month are selected in various departments and announced on staff noticeboards with their names, departments and photographs. Winners of suggestions, proposals, competitions and similar events may also be announced with this information.

Sharing Personal Data with Third Parties in Türkiye

For your safety and to fulfil the Company's legal obligations, personal data may be shared to the extent permitted and required by the Labour Law, occupational health and safety legislation, Social Insurance and General Health Insurance Law, the law regulating internet publications and combating offences committed through such publications, Turkish Commercial Code, Personal Data Protection Law No. 6698, Identity Notification Law and other legislation.

Recipients may include relevant institutions and organisations and public bodies such as the Personal Data Protection Authority, Ministry of Finance, Ministry of Customs and Trade, Ministry of Labour and Social Security, Turkish Employment Agency (İŞKUR) and Information and Communication Technologies Authority. For example, employee data are shared with the Social Security Institution to pay employee and employer contributions.

Sharing Personal Data with Business Partners

We use the SAP personnel payroll program and the Monthly Personnel Attendance Sheet for HR processes. Where support is needed, the service provider's support personnel may access and work on these programs locally or remotely. They may consequently see personnel information in the payroll program. A confidentiality agreement is in place with the provider to protect personal data.

Sharing under Occupational Health and Safety Legislation

During recruitment and periodic health examinations, personal data and special categories of personal data may be shared with our occupational physician and Cankurtaran Tıp Hizmetleri Ltd. Şti., Fethiye Tax Office number 2010372911, and Azize Aksoy.

Sharing with Company Lawyers

Where necessary during employment or after it ends, and in litigation or similar situations, personal data may be shared with Company lawyers solely for the purposes of the relevant case.

Sharing for IT Support and Archiving

When backup and support services are obtained from third-party companies, their backup and support teams may see personal data held electronically. Confidentiality agreements will be concluded with these companies.

Sharing for IT Support Services

Telephones and computers may occasionally malfunction and require intervention by the IT Department. Such intervention may reveal personal files, correspondence, calls, videos, images or Outlook correspondence. Please avoid using Company computers and telephones for personal, private or confidential correspondence or storing such files on them.

The IT Department also performs backups at all times to ensure uninterrupted work and enable recovery of data in the event of loss.

Sharing for Travel, Training, Meetings and Similar Events

For business travel arranged by us, training, Company meetings and other business events, personal data limited to what serves the purpose may be shared with third parties. Examples include providing names, telephone numbers and mailing addresses to a printer for business cards, or providing Turkish identity numbers, names and telephone numbers to an agency for ticketing for domestic or international business travel.

Sharing with Department Managers

During and after recruitment, personnel files may be shared with department managers solely to familiarise them with employees and learn about performance. Files are taken back after the process and kept in the archive room.

Employees' Responsibilities and Confidentiality

Processing personal data for personal reasons or purposes outside the authorised processing purpose, or sharing them with third parties by exceeding or misusing authority, including by staff without access rights for their position or duties, breaches Article 12(1) of Law No. 6698. Employees must carry out all activities under the Law in accordance with legislation, this agreement and employer and workplace instructions.

Employees must always take appropriate technical and administrative security measures to protect data against unauthorised or unlawful processing and accidental loss, copying, destruction or damage. They must not share personal data with a third party without the prior written approval of the employer and workplace.

Any unauthorised loss, copying, destruction, damage or sharing with third parties must be reported immediately to the authorised supervisor. The duty of confidentiality continues indefinitely after the employment agreement ends.

Your Rights under Article 11 of the Law

- (a) Learn whether your personal data are being processed.
- (b) Request information if your personal data have been processed.
- (c) Learn the purposes of processing and whether the data are used accordingly.
- (d) Learn the third parties to whom your data are transferred in Türkiye or abroad.
- (e) Request correction of incomplete or inaccurate data.
- (f) Request deletion or destruction of your data. (Please request a form from the Human Resources Department.)
- (g) Request notification to third-party recipients of the actions taken under subparagraphs (d) and (e).
- (h) Object to a result to your detriment arising from analysis exclusively by automated systems.
- (i) Request compensation for damage caused by unlawful processing.

Requests in your application will be concluded free of charge within thirty days at the latest, depending on their nature. If the procedure incurs an additional cost to the Company, the fee in the tariff set by the Personal Data Protection Board in the Communiqué on the Procedures and Principles for Applications to the Data Controller may be charged.

For matters concerning the processing of your data, complete the application form available through the Company and submit it in writing to Human Resources, by registered electronic mail, secure electronic signature, mobile signature or an email address previously notified to us and recorded in our records.

Depending on the nature of your request and submission method, the Company may request additional verification, such as messaging or calling your registered telephone number, to establish that the application is yours and protect your rights. For example, if you apply using your registered email address, we may contact you through another registered channel and ask you to confirm that you submitted the application.

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