**TÜRKÇEDEN İNGİLİZCEYE TERCÜME**

# PERSONAL DATA STORAGE AND DISPOSAL POLICY

## 1. PURPOSE

The purpose of this Policy on Storage and Destruction of Personal Data ("Policy") is to determine the processing periods of personal data processed by **YAZICI TURIZM YATIRIMLARI VE ISLETMELERI A.Ş. ("Grand Yazici Club Marmaris Palace" or "Data Controller"**), to set forth the criteria and methods for the deletion, destruction or anonymization of personal data whose processing period has expired and/or the purpose of processing has disappeared, and to define the roles and responsibilities of the persons who will take part in these processes.

This Policy also includes the technical and administrative measures taken to ensure data security in Article 6 of the Regulation on Deletion, Destruction or Anonymization of Personal Data, which entered into force on October 28, 2017. The provisions of the December 30, 2017 dated Regulation on the Data Controllers Registry and the Guideline on Deletion, Destruction and Anonymization of Personal Data have also been taken into consideration within this framework.

## 2. SCOPE

This Policy covers the deletion, destruction or anonymization of all personal data that **Grand Yazici Club Marmaris Palace**, as the "data controller" pursuant to Article 7 of the Law No. 6698 on the Protection of Personal Data ("KVKK"), processes in whole or in part by automatic or non-automatic means, provided that it is part of any data recording system, in electronic and/or paper media and whose processing conditions have expired.

## 3. DEFINITIONS

Specific definitions included in this document:

**Explicit consent:** Consent regarding a specific subject, based on information and expressed with free will,

**Grand Yazici Club Marmaris Palace / Data Controller:** Yazıcı Turizm Yatırımları Ve İşletmeleri A.Ş.

**Anonymization:** Making Personal Data impossible to be associated with an identified or identifiable natural person under any circumstances, even if it is matched with other data,

**Deletion :** Making Personal Data inaccessible and non-reusable in any way for the relevant users,

**Destruction:** Making Personal Data inaccessible, non-retrievable and non-reusable by anyone in any way,

**Disposal:** Deletion, destruction or anonymization of Personal Data,

**Law:** "Personal Data Protection Law" numbered 6698,

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

**Relevant Person:** The real person whose Personal Data is processed,

**Personal Data**

**Processing:** Any operation performed on Personal Data such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of Personal Data by fully or partially automated or non-automated means provided that it is part of any data recording system,

**Board:** The Personal Data Protection Board,

**Personal Data Processing**

**Inventory:** The inventory that the Data Controller creates by associating the Personal Data Processing activities carried out by the Data Controller depending on the business processes with the Personal Data Processing purposes, data category, transferred recipient group and data subject group and details the maximum period required for the purposes of Processing Personal Data, the Personal Data foreseen to be transferred to foreign countries and the measures taken regarding data security,

**Special Qualified Personal Data:** Data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data,

**Third Party:** A third real or legal person other than the company to which Personal Data is transferred domestically or abroad,

**Data Controller**

**Contact Person:** Refers to the real person appointed by the Data Controller who performs the administrative follow-up of the processes established within the scope of the Law.

## 4. EXPLANATION OF THE LEGAL, TECHNICAL OR OTHER REASONS FOR THE STORAGE AND DISPOSAL OF PERSONAL DATA

Grand Yazici Club Marmaris Palace processes the personal data of its employees, employee candidates, suppliers/contractors, visitors, online visitors and customers in order to carry out the business processes carried out by its departments in line with their job descriptions and the activities related to these processes. It stores this personal data for the periods stipulated in the legislation or determined by the relevant department within the framework of the purpose of personal data processing. All this flow is included in the Personal Data Processing Inventory. When the relevant retention periods expire, personal data whose purpose of processing has been eliminated by deletion, destruction or anonymization methods specified in this Policy are destroyed.

## 5. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR THE STORAGE OF PERSONAL DATA IN A SECURE MANNER AND FOR THE PREVENTION OF UNLAWFUL PROCESSING AND ACCESS TO IT

This section includes the technical and administrative measures taken by Grand Yazici Marmaris Palace. Grand Yazici Club Marmaris Palace keeps personal data under lock and key in paper and electronic media in accordance with its purpose and for the specified periods.

Personal data can only be accessed by persons authorized by Grand Yazici Club Marmaris Palace, and this authorization is graded according to the processing of personal data.

## 6. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR THE DESTRUCTION OF PERSONAL DATA IN ACCORDANCE WITH THE LAW

Personal Data stored within Grand Yazici Club Marmaris Palace shall be destroyed by subjecting it to deletion, destruction or anonymization processes, taking into account the confidentiality of the data, in the event that the purpose of processing is eliminated, the legal retention period stipulated in the legal regulations to which it is subject, the expiration of the period required by the purpose of processing, or upon the request of the Data Subject, without prejudice to legal regulations.

The retention periods of all data on the Personal Data Processing Inventory are determined by the Data Controller taking into account the relevant laws and legal regulations. The Human Resources Department is responsible for the retention periods and the destruction of Personal Data. The Human Resources Department ensures that personal data is deleted in such a way that personal data can only be processed by the relevant users and that the data cannot be processed for all other unrelated departments. For personal data in electronic media, masking methods are used to the extent necessary. For personal data on paper media, erasure is carried out by blacking out the personal data to be erased.

One or more of the following methods are used to destroy data:

### 6.1. Deletion of Personal Data

Deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users. The data controller is obliged to take all necessary technical and administrative measures to ensure that the deleted personal data is inaccessible and non-reusable for the relevant users.

#### 6.1.1. Process of Deletion of Personal Data

The process to be followed in the deletion of personal data is as follows:

- Determining the personal data that will be subject to deletion.
- Identify the relevant users for each personal data using an access authorization and control matrix or similar system.
- Determining the authorizations and methods of the relevant users such as access, retrieval and reuse.
- Closing and eliminating the access, retrieval, reuse authorizations and methods of the relevant users within the scope of personal data.

#### 6.1.2. Methods of Deletion of Personal Data

**a) Application-as-a-Service Type Cloud Solutions**

Data in the cloud system should be deleted by issuing the delete command. While performing the aforementioned operation, it should be noted that the relevant user does not have the authority to restore the deleted data on the cloud system.

**b) Personal Data on Paper Media**

Personal data on paper media must be erased using the blackout method. The blackout process is performed by cutting out the personal data on the relevant document, where possible, and making it invisible to the relevant users by using fixed ink in a way that cannot be reversed and cannot be read by technological solutions.

**c) Office Files on the Central Server**

The file must be deleted with the delete command in the operating system or the access rights of the user concerned must be removed on the file or the directory where the file is located. When performing the aforementioned operation, it should be noted that the user concerned is not also the system administrator.

**d) Personal Data on Portable Media**

Personal data on Flash-based storage media should be stored encrypted and deleted using software suitable for these media.

**e) Databases**

The relevant rows containing personal data should be deleted with database commands (DELETE etc.). While performing the aforementioned operation, it should be noted that the relevant user is not also the database administrator.

Personal data in paper and electronic media whose purpose of processing is completely eliminated are destroyed in accordance with the Guideline on Deletion, Destruction or Anonymization of Personal Data published by the Personal Data Protection Authority or anonymized by the methods stipulated in this Guideline. All deletion, destruction or anonymization operations performed by the Human Resources Department are logged and recorded electronically with a time stamp. In terms of personal data in paper media, a record of these transactions is prepared and kept by the Human Resources Department. Records regarding the deletion, destruction or anonymization of personal data in electronic and paper media are kept for three years. Grand Yazici Club Marmaris Palace uses the "deletion" method to ensure that only the relevant departments have access to personal data during the retention period. In the event that the retention periods expire and there is no other purpose that requires the retention of personal data, it uses the anonymization method.

### 6.2. Destruction of Personal Data

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way. Grand Yazici Club Marmaris Palace is obliged to take all necessary technical and administrative measures regarding the destruction of personal data.

### 6.2.1. Methods of Destruction of Personal Data

In order to destroy personal data, it is necessary to identify all copies of the data and destroy them one by one using one or more of the following methods depending on the type of systems in which the data is located:

**a) Local Systems**

One or more of the following methods can be used to destroy the data on these systems.

**i)** **Physical Destruction:** The physical destruction of optical media and magnetic media, such as melting, burning or pulverizing. By melting, burning, pulverizing, or passing the optical or magnetic media through a metal grinder, the data is rendered inaccessible. In the case of solid state disks, if overwriting or de-magnetizing is not successful, this media must also be physically destroyed.

ii) **Overwriting:** This is the process of preventing the recovery of old data by writing random data consisting of 0s and 1s at least seven times on magnetic media and rewritable optical media. This is done using special software.

**b) Environmental Systems**

Depending on the type of media, the destruction methods that can be used are listed below:

i) **Network devices (switches, routers, etc.):** The storage media inside these devices are fixed. Products often have a wipe command but not a destroy feature and must be destroyed using one or more of the appropriate methods specified in (6.1).

ii) **Flash-based media:** Flash-based hard disks with ATA (SATA, SSD, PATA, etc.), SCSI (SCSI Express, etc.) interfaces must be erased using the <block erase> command if supported, or if not supported, using the manufacturer's recommended erase method, or using one or more of the appropriate methods specified in (6.1).

iii) **Mobile phones** (Sim card and fixed memory spaces): Fixed memory spaces in portable smartphones have an erase command, but most do not have a destroy command. They should be destroyed using one or more of the appropriate methods described in (6.1).

iv) **Peripherals such as printers whose data recording media is removable:** All data recording media must be destroyed by verifying that they have been removed and using one or more of the appropriate methods specified in (6.1) according to their characteristics.

v) **Peripherals, such as printers, whose data recording medium is fixed:** Most of these systems have a delete command, but not a destroy command, and should be destroyed using one or more of the appropriate methods specified in (6.1).

**c) Paper Media**

Since the personal data on such media is permanently and physically written on the media, the main media must be destroyed. This is done by shredding or clipping the media with paper shredders or clipping machines into small pieces of incomprehensible size, if possible horizontally and vertically, so that they cannot be reassembled.

Personal data transferred from the original paper format to the electronic environment through scanning must be destroyed by using one or more of the appropriate methods specified in (a) depending on the electronic environment in which they are located.

**d) Cloud Environment**

During the storage and use of personal data in such systems, it should be encrypted by cryptographic methods and, where possible, encryption keys should be used for personal data, especially for each cloud solution from which services are received. When the cloud computing service relationship ends, all copies of the encryption keys necessary to make personal data usable must be destroyed.

In addition to the above environments, the destruction of personal data contained in devices that malfunction or are sent for maintenance is carried out as follows:

i) Destruction of the personal data contained in the relevant devices by using one or more of the appropriate methods specified in (6.1) before transferring them to third institutions such as manufacturers, sellers, services for maintenance and repair,

ii) In cases where destruction is not possible or appropriate, dismantling and storage of data storage media, sending other defective parts to third parties such as manufacturers, vendors, services,

iii) Taking the necessary measures to prevent personnel coming from outside for maintenance and repair purposes from copying personal data and taking them out of the organization,

are necessary.

**6.3. Anonymization of Personal Data**

Anonymization of personal data means making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even if the personal data is matched with other data.
In order for personal data to be anonymized; personal data must be rendered unassociated with an identified or identifiable natural person, even through the use of appropriate techniques for the recording medium and the relevant field of activity, such as the return of personal data by the data controller or recipient groups and / or matching the data with other data.
The data controller is obliged to take all necessary technical and administrative measures to anonymize personal data. Anonymization of personal data is carried out by the following methods in accordance with the principles specified in the personal data storage and destruction policy.

**7. DATA DESTRUCTION PROCESSES**

**7.1. STORAGE AND DISPOSAL PERIODS TABLE**

Retention periods according to data types are in the Personal Data Inventory. The retention periods in the relevant basic legislation, including but not limited to those specified, are in Annex: Retention Periods Table. However, if there is a change in the relevant legislation specified in the Retention Periods Table, the current new legislation will be taken into consideration.

**7.2. Periodic Destruction Period**

Grand Yazici Club Marmaris Palace deletes/destroys/anonymizes personal data whose retention period has expired and for which there is no other data processing purpose that requires the retention of personal data within 6 (six) months following the expiration of the retention period. It is monitored by the Human Resources Department within the scope of the periodic destruction process.

**7.3. Destruction of personal data upon request of the Data Subject**

When the relevant person requests the deletion or destruction of his/her personal data by applying to Grand Yazici Club Marmaris Palace;

a) If all of the conditions for processing personal data have disappeared; Grand Yazici Club Marmaris Palace deletes, destroys or anonymizes the personal data subject to the request. Grand Yazici Club Marmaris Palace finalizes the deletion or destruction requests of the relevant persons within **"thirty days"** at the latest.

b) If all the conditions for processing personal data have disappeared and the personal data subject to the request have been transferred to third parties; Grand Yazici Club Marmaris Palace notifies the third party and requests the deletion or destruction of the personal data in question.

c) If all the conditions for processing personal data have not been eliminated, this request may be rejected by Grand Yazici Club Marmaris Palace by explaining the reason in accordance with the third paragraph of Article 13 of the Personal Data Protection Law, and the rejection response shall be notified to the relevant person in writing or electronically within **"thirty days"** at the latest.

## POLICY ON ADEQUATE MEASURES FOR THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

### 1 INTRODUCTION

**"YAZICI TURIZM YATIRIMLARI VE ISLETLMELERI A.Ş.** ("Grand Yazici Club Marmaris Palace" or "Company") departments process special categories of personal data within the scope of the relevant personal data processing processes and activities within the meaning of Article 6 of the Law No. 6698 on the Protection of Personal Data ("KVKK"). These special categories of personal data processed by the Company are included in the personal data processing inventory in the light of data processing purposes and conditions. Art. 6 of the LPPD regulates the conditions for processing special categories of personal data in the second and third paragraphs. The fourth paragraph emphasizes that in the processing of special categories of personal data, in addition to all kinds of technical and administrative measures required to be taken pursuant to Article 12 of the LPPD, adequate measures to be determined by the PDP Board ("Board") must also be taken. This Board decision referred to by Article 6/f.4 of the LPPD was published in the Official Gazette dated 7.3.2018.

**Purpose and Scope of the Policy**

Pursuant to the Board's decision, this Policy explains the adequate measures that Grand Yazici Club Marmaris Palace must take in terms of the personal data of special nature that it processes, in relation to the Personal Data Security published by the Personal Data Protection Authority ("Authority").

This Policy covers electronic and paper media where special categories of personal data are processed.

**Policy Framework**

1. **Actions Taken for Employees and Customers in the Processing of Specially Qualified Personal Data**

   a. **Training:** Employees should be regularly trained on the security of Sensitive Personal Data in line with the LPPD and related secondary legislation, Board Decisions and Guidelines.

   b. **Confidentiality Agreement or Privacy Policy :** In addition to the employment contract, a confidentiality agreement or commitment letter should be made with the employees who are authorized to access sensitive personal data, specifically within the scope of sensitive personal data. An indefinite confidentiality obligation regarding personal data should be included in both the employment contract and the confidentiality agreement or commitment letter. In case of breach of confidentiality agreements, a process for reporting violations and a procedure detailing this process and necessary actions should be taken in case of breach of the confidentiality agreement. Grand Yazici Club Marmaris Palace should sign confidentiality agreements with all suppliers, third parties, contracted employees and subcontractors of suppliers who are given access to critical information assets for the protection of information assets.

   c. **Access Authorization and Controls:** The scope and duration of authorization of employees authorized to access sensitive personal data must be clearly defined. In addition, these authorizations should be checked periodically. For this purpose, an access authorization and control matrix should be created within the framework of the Data Security Guide published by the PDP Authority. Employees who leave their jobs or change their duties should immediately remove their authorization to access sensitive personal data and ensure that the electronic equipment registered on them is returned. When defining roles and responsibilities in the organizational structure, the principles of segregation of duties and minimum access rights should be taken into account wherever possible. With this structure, incompatible roles should not be assigned to the same person. In the event that the responsibilities of Grand Yazici Club Marmaris Palace employees change, changes must be made to their old authorities before new/additional authorities are assigned according to the new responsibilities. Grand Yazici Club Marmaris Palace must ensure that dismissals for

3rd party employees are carried out in an orderly manner and that relevant responsibilities are defined within Grand Yazici Club Marmaris Palace for this purpose. All access rights of the dismissed employee must be removed before interviewing the 3rd party employees who are dismissed from the job or project, and then all assets belonging to Grand Yazici Club Marmaris Palace on the person must be taken back. 3rd party employees must deliver Grand Yazici Club Marmaris Palace assets in their possession to the relevant Grand Yazici Club Marmaris Palace personnel in case of resignation or at the end of their contract period. All access to information systems and services that contain sensitive personal data must be provided through a user registration procedure that ensures that the right of access is approved before access is granted. An access deletion process that will also provide automatic or timely notification for the removal of access to information systems and services should be followed. Third party access to information systems containing sensitive personal data should only be granted after a detailed analysis of this requirement and an assessment of the risks involved.

**2. Adequate Measures to be Taken in Electronic Environments where Sensitive Personal Data are Processed, Stored and Accessed**

a. Electronic media containing sensitive personal data should be stored using cryptographic methods.

b. In order to ensure the security of the keys used for this purpose, it is necessary to ensure key security by keeping them in different and secure environments.

c. All transaction activities and records performed on sensitive personal data must be logged. Audit trails of user activities, exceptions and security events must be maintained and monitored. Audit trails should include the following:

* Start and end times
- System errors or failures and corrective actions taken
- Verification and correct processing of data files and system outputs
- Name or username of the person whose audit trail is kept

The activities of users with high levels of access (privileged users such as system administrators and system operators) should be logged and regularly reviewed by an independent person.
Access to applications containing sensitive personal data and access to Grand Yazici Club Marmaris Palace network should be monitored against any security breach. Appropriate mechanisms must be established for such cases. Remote access should only be provided on a limited basis and should be carried out in accordance with the authorizations given through the systems.
Audit trails should be maintained according to record keeping and retention needs. Audit trail retention mechanisms and audit trails should be protected against unauthorized access.

d. In cases where special categories of personal data are accessed through a software or the environments where these data are located, security updates must be continuously monitored. It is necessary to periodically carry out or have the

necessary security tests carried out and the necessary actions should be planned by recording the results.

e. Where remote access to this data is required, at least two-factor authentication is required.
f. It is important to conduct a **"DATA PROTECTION IMPACT ANALYSIS"** in cases where the processed special categories of personal data are biometric data, health data and genetic data.

**3. Adequate Measures to be Taken in Physical Environments where Sensitive Personal Data are Processed, Stored and Accessed**

a. If the environment where sensitive personal data is located is an archive or data center, it is necessary to take the necessary security measures to ensure the technical and physical security of these environments.
b. Physical security controls should be designed and implemented for offices, rooms and facilities according to the sensitive personal data they contain.
c. Unauthorized entry and exit to these environments must be prevented.

**4. Adequate Measures to be Taken in the Transfer of Sensitive Personal Data**

a. In cases where this data must be transferred via e-mail, it must be transferred encrypted with a corporate e-mail address or using a KEP address. In addition, within this scope, it should be ensured that e-mails containing sensitive personal data are labeled with data classes called "confidential" or "sensitive & confidential".
b. In cases where it needs to be transferred via media such as portable memory, CD, DVD, encryption with cryptographic methods and ensuring key management and security by keeping the keys in different media.
c. If a transfer is to be made between servers in different physical environments, the transfer should be realized by setting up a VPN or similar methods.
d. If paper transmission is required, necessary precautions must be taken against risks such as theft, loss or unauthorized viewing of the document, and the document must be sent with confidentiality.

** In case of any discrepancy between the Turkish language version of this policy and any translation, the Turkish text should be taken into account.