CARYA TOURISM YATIRIMLARI

PERSONAL DATA STORAGE AND DESTRUCTION POLICY

1. PURPOSE / SCOPE

The purpose of this policy is to set forth the procedures and principles regarding the deletion, destruction and anonymization of personal data stored by *CARYA TURİZM YATIRIMLARI A.Ş.* ("CARYA") as the data controller in accordance with the **"Personal Data Protection Law"** No.6698 and other legislations.

Within this scope, the personal data of our employees, prospective employees, guests, visitors, outsourced service providers, suppliers and all other natural persons whose personal data are held by CARYA for whatever purpose, are managed in accordance with the **"Personal Data Processing and Protection Policy"** and the **"Personal Data Storage & Destruction Policy"** herein.

2. DEFINITIONS & ABBREVIATIONS

The main definitions and their abbreviations may be found in the **"Definitions and Abbreviations List"**.

For the purposes of this policy the following definitions shall apply:

Data subject: the natural person whose personal data is processed

Destruction: The deletion, removal or anonymization of personal data

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

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

Board: The Personal Data Protection Board

User concerned: Persons who process personal data within the organization of the Data Controller or upon authorization and instructions received from the Data controller, other than the person or department which is responsible for the technical storage, protection and back up of personal data,

Recording medium: Any medium, where personal data is fully or partially processed through automated means or provided that the process is a part of any data registry system, through non-automated means

Personal Data Processing and Protection Policy: The policy, setting out the principles and procedures for the management of personal data in CARYA's possession, which can be reached at **http://www.regnumhotels.com/d/regnum/media/PDF/KVKK.pdf**

Data registry system: the registry system, in which personal data is structured and processed according to certain criteria,

Authorized Employee: the natural person who processes personal data on behalf of the Data Controller upon his/her authorization,

Data Controller: Natural person or legal entity who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

Data processor: Any natural person or legal entity outside the Data Controller's organization who processes personal data on behalf of the Data Controller upon his/her authorization

Fidelio: Front Office Operating System

SAP: Accounting and Human Resources Operating System

Lapis: Golf and Spa Operating System

eBa - QDMS – Ensemble: Workflow and Integrated Quality Management Operating System

MEYER: Employee entry-exit registration system

REVIEWPRO: Integrated tools and processes to increase guest satisfaction and revenue.

SETROW: Bulk mail delivery system

CLIK VIEW: Reporting program

MICROS: Reservation-order program

Destech Mini Club: Kids club entry-exit recording system

Prest: A La Carte reservation system

MC: Stock Management Program

Conexease Whatsapp: Whatsapp multiple notification platform

Eraysoft Güvenlik: Identification Information scanning system

SYSVIASES: Call Centre recording operating system

NEVOTEK: Camera Recording System

Kale Card Lock: Room Door Identification System

Office 365: Cloud-based operating system

VDO: Digital tachograph recording system

Explicit consent: Consent that is related to a specific issue, based on information and expressed with free will.

Sensitive personal data: Personal data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance or clothing, affiliation to associations, foundations or trade-unions, health, sexual life, convictions, data relating to security measures, biometric and genetic data

3. MEDIUMS AND SECURITY MEASURES

3.1. Mediums For Personal Data Storage

Personal data stored by CARYA shall be kept in a recording medium in accordance with the nature of the relevant data and our legal obligations.

The recording mediums used for storing personal data are in general as stated below. However, some data may be kept in different mediums other than the ones specified here due to their particular qualifications or our legal obligations. CARYA acts as a data controller by all manner of means and processes and protects personal data in accordance with the Personal Data Protection Law, "Personal Data Processing and Protection Policy and the " Personal Data Storage and Destruction Policy " herein.

a) Printed Mediums: the medium where data is printed and kept on paper
b) Local Digital Mediums: Servers within CARYA, hard or removable discs, optical discs and other such digital media
c) Cloud Mediums: internet-based systems used by CARYA that are encrypted with cryptographic methods. (Office 365-VDO)

3.2. Ensuring Security of The Mediums

CARYA shall take all required technical and administrative measures as appropriate to the nature of the relevant personal data and the medium in which it is kept to ensure the safe storage of personal data and to prevent illegal processing and access to the data.

These measures include, but are not limited to, the following administrative and technical measures relevant to the nature of the personal data and the medium in which it is held.

3.2.1. Technical Measures

CARYA takes the following technical measures for all mediums where personal data is stored, for all relevant data and in accordance with the characteristics of the medium where the data is kept.

- Up-to-date and secure systems that are in line with the current technological developments are used in mediums where personal data is stored.
- The appropriate security systems are used for mediums where personal data is stored.
- Security tests and checks are conducted on the information systems for detecting weaknesses in the security systems, and the existing or potential risks identified by these tests and checks are eliminated.
- Access to data in mediums where personal data is kept is restricted, only authorized persons are allowed access to this data for the purpose of processing personal data and all access is recorded.
- CARYA employs sufficient technical personnel to ensure the security of the mediums where personal data is stored.

3.2.2. Administrative Measures

CARYA takes the following administrative measures for all mediums where personal data is stored, for all relevant data and in accordance with the characteristics of the environment where the data is kept.

- Trainings are provided to all CARYA employees who have access to personal data to create and raise awareness about data security, personal data and the right to privacy.
- CARYA receives legal and technical consultancy services to follow the developments and to take necessary actions in the fields of information security, the right to privacy and protection of personal data.
- In the case that personal data is transferred to third parties due to technical or legal requirements, protocols or contracts shall be signed with the relevant third parties to protect personal data and all

necessary care shall be taken to ensure that the relevant third parties comply with their obligations under these agreements or protocols.

3.2.3. Internal and External Audit

Pursuant to Article 12 of the Law, CARYA undertakes internal and external audits regarding the implementation of the provisions of the Law and the implementation of the Personal Data Storage & Destruction Policy herein and the Personal Data Processing and Protection Policy.

In case of deficiencies or negligence relating to the application of these provisions are identified by internal and external audits, such deficiencies or negligence shall be promptly rectified.

If during audit or by any other ways it is understood that the personal data under the responsibility of CARYA is obtained by others by unlawful means, CARYA shall notify the related person and the Board in the soonest time possible.

4. DESTRUCTION OF PERSONA DATA

4.1. Reasons For Storage and Destruction

4.1.1. Reasons For Storage

Personal data kept by CARYA is stored for the purposes and reasons set forth herein, in accordance with the Law and CARYA's Personal Data Processing and Protection Policy.

4.1.2. Reasons For Destruction

Personal data kept by CARYA shall be deleted, destroyed or anonymised in accordance with the destruction policy set forth herein upon the request by the data subject or ex officio if all the conditions specified within Article 5 and 6 of the Law cease to exist.

The conditions listed in Articles 5 and 6 of the Law consist of the following:

- It is clearly provided for by the laws.
- It is mandatory for the protection of the life or physical integrity of the data subject or any other person where the data subject is physically incapable of giving his/her consent or whose consent is not deemed legally valid.
- It is necessary to process the personal data belonging to the parties of a contract, provided that it is directly related to the execution or fulfilment of that contract.
- It is mandatory for the data controller to be able to perform his/her legal obligations
- The relevant data is revealed to the public by the data subject himself/ herself
- Data processing is mandatory for the establishment, exercise, or protection of a right;
- It is mandatory for the legitimate interests of the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

4.2. Destruction Methods

Personal data stored by CARYA in accordance with the Law or relevant other laws and the “Personal Data Processing and Protection Policy”, shall be deleted, destroyed or anonymised either ex officio or upon request by the data subject within the durations as specified in the Personal Data Processing and Protection Policy herein in case the reasons necessitating their processing cease to exist.

The most common deletion, destruction and anonymization techniques used by CARYA are as follows:

4.2.1. Methods for Deletion

- **Methods for Deleting Personal Data Stored in Printed Medium**

    - **Blanking**: The data stored in printed media shall be deleted by way of blanking. Blanking is performed by way of trimming, where possible, of the personal data on the relevant document, and in cases where this is not possible, by rendering such data invisible for the relevant user by using fixed ink so that it cannot be reversed or read by way of technological solutions.

- **Methods for Deleting Personal Data Stored in Cloud Systems or Local Digital Mediums**
    - **Secure Deletion from Software:** Data stored in Cloud systems or local digital mediums shall be irrevocably deleted by using a delete command. Data deleted this way will be irretrievable.

4.2.2. Methods For Destruction

- **Methods for Destructing Personal Data Stored in Printed Medium**
    - **Physical destruction**: Documents kept in printed medium shall be destroyed in such a way that they cannot be reassembled with the document shredders

- **Methods for Destructing Personal Data Stored in Local Digital Mediums**
    - **Physical destruction**: It is the physical destruction of the personal data stored in magnetic or optical medium by means of dissolving, burning, or dusting. Data stored in optical or magnetic media shall be rendered inaccessible by processes such as dissolving, burning, dusting or grinding through a metal shredder.

- **Methods for Destructing Personal Data Stored in Cloud Systems**
    - **Secure Deletion from Software:** The data stored in cloud systems shall be rendered irrevocable by using a delete command and when the cloud computing service relationship ends all copies of the encryption keys required to make personal data available shall be destroyed.

4.2.3. Anonymization Methods

Anonymization is the process of rendering personal data so that it can no longer be associated with an identified or identifiable natural person under any circumstances even by way of matching with other data.

Anonymized Data refers to data that cannot be associated with an identified or identifiable natural person under any circumstances, even by way of matching with other data.

- **Removing variables:** It is the removal of one or more direct identifiers in the personal data of the relevant person which can be used for identifying the person in any way.

This method may be used to anonymize personal data as well as to delete data within personal data which is found not suitable for data processing purposes.

- **Sectional masking**: It is the process of deleting information that may be characteristic of identifying exceptional data in the data table where personal data is collectively anonymous.

- **Generalization:** It is the process of gathering personal data belonging to many people and turning this data into statistical data by removing distinctive information.

- **Upper and lower limit coding / Global coding:** For a given variable, the ranges of that variable are defined and categorized. If the variable does not contain a numeric value, then similar data within the variable may be categorized.

Values that fall within the same category are combined.

- **Micro combination**: With this method, all records in the data set are first sorted in a meaningful order and then the whole set is subdivided into a certain number of subsets. Then the average value of each subset of the specified variable is taken and the value of the subset of that variable is replaced with the average value. In this way, the indirect identifiers in the data will be distorted, making it difficult to associate the data to the relevant person.

- **Data hash and distortion**: Direct or indirect identifiers in personal data are mixed or distorted with other values to break the link with the person identified with the data and to lose their descriptive qualities.

4.2.4. Time Periods For Storage and Destruction

4.2.4.1. Time Period For Storage

- **Employee**

Employee, recruitment documents and personal data regarding duration of service and salary that is declared to the Social Security Institution, shall be kept during the duration of the service contract and for 10 (ten) years as of the dissolution of the contract.

Employee, recruitment documents and personal data other than the personal data regarding the duration of service and salary that is declared to the Social Security Institution, shall be kept during the duration of the service contract and 10 (ten) years from the beginning of the calendar year following the dissolution of the service contract.

Data in the Employee, Workplace Personal Health File shall be kept during the duration of the service contract and for a period of 10 (ten) years following the dissolution of the service contract.

- **Business Partner**

The identification of the execution of the commercial relationship between the Business Partner and CARYA, contact information, financial information, telephone voice records, Business Partner/ Solution Partner/ Consultant data

In accordance with Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code, the data of the Business Partner shall be kept during the business / commercial relationship with CARYA and as of its termination for a period of 10 (ten) years.

- **Visitor**

The visitor's name, surname, Turkish identification number, identification number and license plate taken at the entrance to the physical grounds of CARYA and camera recordings, telephone voice recordings, shall be kept for 2 years.

- **Website Visitor**

The name, surname, e-mail address and navigation information of the Website Visitor shall be kept for 2 (two) years.

- **Prospective Employee**

Curriculum Vitae(CV) of the Prospective Employee and the information on the application form shall be kept until the CV is out of date for a maximum of 2 (two) years.

- **Intern (student)**

The information contained in the internship file of the intern shall be kept during the course of the internship and for 10 (ten) years from the beginning of the calendar year following the completion of the internship.

- **Guest**

The guest's name, surname, Turkish Identification number, identification number, contact information, payment information and methods, location information, telephone voice recordings, service preferences, transaction history, special days information,

In accordance with Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code, the data relating to the service purchased by the guest shall be kept for 10 (ten) years as of the date of the purchase.
Guest security camera images shall be kept for a maximum of 60 (sixty) days, in-car camera images for 2 (two) days, and vehicle license plate information for 2 (two) years.

- **Institutions/Companies in collaboration with CARYA (Suppliers)**

The identification of the execution of the commercial relationship between CARYA and its collaborating institutions/companies, contact information, financial information, telephone voice records, the data of the institutions/companies

In accordance with Article 146 of the Turkish Code of Obligations and Article 82 of the Turkish Commercial Code, the data of the institutions/companies shall be kept during the business / commercial relationship with CARYA and as of its termination for a period of 10 (ten) years.

4.2.4.2. Time Periods for Destruction

In accordance with the Law or relevant other laws, the Personal Data Processing and Protection Policy and the Personal Data Storage and Destruction Policy herein, CARYA shall delete, destroy or anonymize personal data in the first periodic destruction process following the date upon which the obligation to delete, destroy or anonymize personal data occurs.

In the event that the data subject files a request with CARYA for the deletion or destruction of her/his personal data on the basis of Article 13 of the Law;

In the event that all of the conditions for the processing of personal data no longer exist, CARYA shall delete, destruct or anonymize the personal data which is subject to the request within 30 (thirty) days of the request using the appropriate destruction methods and with its justified grounds. For CARYA to be deemed to have received the request, the data subject shall convey the request in accordance with the Personal Data Storage and Destruction Policy. In any case, CARYA shall inform the data subject accordingly of the action taken.

If all of the conditions for the processing of personal data have not been eliminated, the request may be rejected by CARYA in accordance with Article 13 of the Law together with its justified grounds and such rejection shall be communicated to the data subject in writing or by electronic means at the latest within 30 (thirty) days.

4.2.5. Periodic Destruction

In the event that all conditions for processing of personal data as set forth by the Law no longer exist, CARYA shall delete, destroy or anonymize the personal data in question ex officio within the recurring periods as specified in the Personal Data Processing and Protection Policy herein.

CARYA shall delete, destroy or anonymize personal data in the first periodic destruction following the date upon which the obligation to delete, destroy or anonymize data occurs.

4.3. Monitoring The Lawful Destruction of Data

CARYA shall destroy personal data ex officio or upon request by the data subject in accordance with the Law or relevant other laws and the "Personal Data Processing and Protection Policy" and Personal Data Storage and Destruction Policy herein.

CARYA shall take a number of administrative and technical measures to ensure that the destruction processes are carried out in accordance with these regulations.

4.3.1. Technical Measures

- CARYA maintains the appropriate technical means and equipment suitable for each method of destruction stated in the policy herein.
- CARYA ensures the safety of the place where the destruction process is carried out.
- CARYA maintains the access records of the persons involved in the destruction process.
- CARYA employs competent and experienced personnel to carry out the destruction process or receives services from competent third parties when necessary.

4.3.2. Administrative Measures

- CARYA provides training to its employees to raise and create awareness about data security, personal data and the right to privacy.
- CARYA receives legal and technical consultancy services in order to follow the developments in the field of data security, right to privacy, protection of personal data and techniques for safe destruction.
- In cases where the destruction process is carried out by third parties due to technical or legal requirements, CARYA signs protocols for the protection of personal data with the relevant third

parties, and takes all due care to ensure that the third parties comply with their obligations under these protocols.

- CARYA regularly inspects whether the destruction processes are carried out in accordance with the Law and the conditions and obligations set forth in the Personal Data Storage and Destruction Policy herein and takes the necessary actions.
- CARYA records all transactions relating to the deletion, destruction and anonymization of personal data and, excluding other legal obligations, keeps such records for at least 3 (three) years.

5. DATA SECURITY BOARD

CARYA shall establish a "Data Security Board within its organization. The Data Security Board shall be authorized and responsible for carrying out and implementing the necessary procedures for storing and processing the data of the data subjects in accordance with the Law, the Personal Data Processing and Protection Policy and the Personal Data Storage and Destruction Policy.

- The Personal Data Committee consists of three persons: a manager, an administrative expert and a technical expert. The titles and job descriptions of CARYA employees in the Personal Data Committee are stated in the "**Data Security Board Member List**":

6. UPDATE AND COMPLIANCE

CARYA reserves the right to make changes in the **"Personal Data Processing and Protection Policy"** or the Personal Data Storage and Destruction Policy originating from the amendments in the Law, in accordance with the decisions of the Organization or in line with the developments in the sector or in the field of information technology.

Amendments to the Personal Data Storage and Disposal Policy herein shall be immediately inserted in the text of the policy and the necessary explanations of any changes shall be provided at the end of the policy.