



EMPLOYEE CLARIFICATION TEXT REGARDING THE PROCESSING AND PROTECTION OF PERSONAL DATA

In accordance with the **Personal Data Protection Law** No. 6698 (hereinafter referred to as the "Law"), for the purpose of providing clarification on the procedures and principles regarding the processing of personal data of its employees, CARYA TURİZM YATIRIMLARI A.Ş (hereinafter referred to as the "Company") as the data controller is obligated to inform the data subjects, as specified by Article 10 of the Law, about the following whilst collecting personal data;

- the identity of the controller and of its representative, if any,
- the purpose of data processing;
- to whom and for what purposes the processed data may be transferred,
- the method and legal reason of the collection of personal data,
- Other rights referred to in Article 11.

We declare that your personal data shall be processed within the scope of our commercial relations or our business relationship with you pursuant to the purpose that requires data to be processed and with regard to this purpose in a related, limited and restrained manner, shall be recorded, stored, retained, reorganized by maintaining the personal data which you have submitted or was submitted to us accurate and up-to-date, shall be shared with the institutions authorized by law to request such personal data, shall be transferred to domestic or foreign third parties as provided for by the Law and shall be transferred, classified or processed in other ways as specified in the Law.

The Company gives particular importance to the security of personal data and takes all necessary technical and administrative measures. Personal information is requested from our employees whilst job applications are made to our Company, while signing the employment contract and during the term of employment in order to provide better service to our employees, fulfils our legal obligations; improve our communication with our employees, and to better understand their needs and interests.

Your personal data shall be processed in accordance with the principles listed in Article 4 of the Law;

- In compliance with the Law and rules of good faith,
- Accurate and up-to-date,
- For specific, explicit and legitimate purposes,
- Being relevant, limited and restrained to the purpose for which it is processed,
- Stored for the period of time stipulated by the relevant legislation or for the purpose for which it is processed.

All kinds of data stored in electronic or printed form, specified in the below list titled "Processed Personal Data", that can be associated with a real person are defined as "Personal Data" according to the Law. Your personal data may be collected by our Company or legal or natural persons processing data on behalf of our Company based on legal reasons, verbally or in writing or electronically through such media including but not limited to the website, electronic mail, mobile communications, application and membership forms and various agreements.



Personal data may be shared with relevant institutions or organizations if necessitated by the laws and may be processed in compliance with the Law and rules of good faith, accurate and up-to-date, for specific, explicit and legitimate purposes, and being relevant, limited and restrained to the purpose for which it is processed.

All personal data stored in the employee's personal file or electronic file shall be kept in an electronic or non-electronic format for the duration of the employment contract but also for a specific period of time following the termination of the employment contract, for such purposes as fulfilling our obligations to our employees, supporting recruitment research processes, proof of work, determining working hours, determining the beginning and ending of the daily working hours, checking attendance, auditing payroll records, recording wage information, notifying the Social Security Institution and other institutions, enforcing occupational health and safety legislation, fulfilling legal obligations and determining working conditions,

Following the termination of the employment contract, personal files will be stored for 10 years by taking all necessary technical and administrative measures.

Processed Personal Data

Identification: Name, surname, date of birth, nationality, place of birth, gender, marital status, citizenship, Turkish Identification information (Turkish ID number, serial number, certificate number, father's name, mother's name, place of birth, city, district, county, volume number, family serial number, serial no, section number, page number, place of issue, date of issue, reason for issue, previous last name), copy of identification card, passport (passport number), residence permit, driver's licence, other identification (lawyer identity card etc.)

Communication: Phone number, full address, e-mail, company contact information (extension number, company e-mail)

Financial: Financial and salary information, payroll, premiums, premium amounts, file and debt information regarding execution for debt, passbook, IBAN, minimum living allowance

Sensitive Personal Data: Conviction/criminal record, disability status/ disability type/ disability percentage, religion, health data, blood type, health records, health check for infectious disease, temporary or permanent incapacity report, work based medical report, chest x-ray, hearing test, eye test, liver enzyme screening, Hepatitis tests, employment and periodic examination forms signed by the on-site doctor, drug test, pregnancy status, pregnancy report, health and maternity leave information, union, association / foundation memberships

Educational Data: Educational status, certificate and diploma information, foreign language skills, education and skills, resume, courses and seminars attended

Visual and Audio Data: Photographs, audio recordings, camera recordings (birthday celebration etc.) belonging to real persons

Employee Performance and Career Development Data: Training and skills, information regarding training and dates training, signed participation form, monthly performance evaluation and goal realization, activity information, trial period evaluation form

Family and Relatives Data: Marriage certificate, name and surname of spouse and children, Turkish Identity Number, gender, date of birth, height, weight, job title, and the name, surname, telephone number and full address of relatives who can be reached in case of emergency

Employment Data: Employer registration number, position, department and unit, title, last employment date, date of recruitment and termination, insurance / pension allocation number, social security registration number, flexible hours working status, travel status, monthly total overtime information , severance pay base date, severance pay additional days



Leave of absence: leave of absence seniority base date, leave of absence seniority extra days, type of leave, departure / return date, number of days used, reason for leave of absence, address / phone while on leave of absence , casual leave information,

Other: Military service deferment, shoe size, size, height, weight, vehicle license plate, vehicle km information, internship status, company service bus used, pick up-drop off location information, employee internet access logs, entry-exit logs, employee daily activity data , vehicle GPS tracking system records, personal protective equipment debit data

Human Resources Payroll and Salary Processes:

Your personal data is processed for the purpose of creating your personal file (all the documents included in the employment document list), executing employment and termination processes, calculating wages, fulfilling legal obligations for institutions such as SGK, İŞKUR, police department, and military police, following annual and casual leaves, executing all human resources processes, following legal processes such as litigation, enforcement etc., reporting occupational accidents, following the procedures required by the occupational health and safety legislation, fulfilling court rulings, complying with other data storage, reporting and information obligations stipulated by legislation, relevant regulatory institutions and other authorities.

PDKS (Employee Attendance Control System) for Entry - Exit tracking:

The system works with a facial recognition recording system. If the employee face recognition system does not execute the face recognition process, the entry and exit data of the employee concerned shall be tracked by the Human Resources department upon the official report of the employee explaining the situation.

Furthermore, the backup of the face recognition system is made by the Information Technologies Department. This system is used to ensure that entrances and exits are made from a single place and to determine who is inside the building in extraordinary emergencies such as fire etc.

Registration charts showing the start and end times of work hours are present in the human resources department in order to apply and track the leisure time application and the adjustment application. Adjustment and overtime calculations are calculated based on shift start and end times, not on entry and exit times to the workplace.

Training and career planning:

In order to determine training needs and for career planning purposes, personal information such as educational status, certificates obtained, participation forms / certificates of legally required trainings, in-house trainings and previous trainings are kept in your personal file and in the training portal.

Camera Surveillance System:

There are cameras in various locations within the Company (including employee housing). The cameras are used for the general safety of employees, prospective employees, guests, outsourced service providers, suppliers and visitors, and the premises is monitored by cameras 24/7 in order to respond to emergencies such as accidents relating to the workplace and occupational health and safety. Additional cameras may be used if necessary.



Company phone and company line:

In cases where a company phone and company line are provided, a delivery report of the company phone and line will be prepared. Upon termination of the employment contract, it may be possible for us to see the text messages and calls during the formatting process of the returned line and phone. In this context, we may read the text messages. Care must be taken to avoid personal, private and confidential correspondence and calls via the company phone.

Checking the company's mailbox, tracking internet traffic and keeping internet login logs during the continuation of the employment contract and upon its termination,:

Following the termination of the employment contract, the passwords of electronic devices (computer, telephone, etc.) used by the former employee are changed by the Information Technologies Department on the date of the termination of the employment contract. The mailbox will remain active for 2 (two) months, and incoming mails will be monitored by the Information Technologies Department and the relevant department manager in order not to adversely affect the guest and all parties with whom there is a business relationship with , and to provide services without interruption. Past dated e-mails may be opened with their attachments for the purpose of running the business.

In order to control inappropriate acts such as illegal copying, business execution, business research, unauthorized software installation and use, participation in online entertainment communities, chat rooms, forums, mass e-mailing, access to music sites, detection of infected sites, access to sites with inappropriate content in violation to general morals, customs and traditions, access to websites with inappropriate content, harassment, gambling, betting and the like, mail and internet traffic will always be monitored by the Information Technologies Department and the necessary restrictions will always be applied. The logs of the websites that are accessed within the framework of the company rules and related laws are kept by the Information Technologies Department.

The company management may restrict access to websites which it deems inappropriate to prevent the server from exceeding its capacity due to spam mail and because of virus risks.

In this context, your personal, private and confidential correspondences and documents should not be made or kept on company computers.

Organizations such as birthdays, marriages, birth of children:

In order to celebrate happy events such as birthdays, marriages, birth of children and to offer support on sad occasions like funerals and accidents, such announcements may be made within in the company via email and employee bulletin boards.

Sharing Information on Blood Type

In the event that our employees or their relatives need blood, to quickly obtain the required blood all company employees are notified via email or text messages or by bulletin boards within the company of the name, surname, telephone number, the required blood type of the employee.



Reference check when starting or leaving the job

During your job application and your trial work period our Company shall exchange information with the person/ persons you have stated as references in order to obtain information about your business ethics. This will be valid for the 2 (two) months trial period. Also, in case your employment contract is terminated, and upon your application to a new job, information shall be exchanged with the person/ persons who may contact our Company for reference check of our former employee. If you do not give permission for a reference check, we must be informed at the time of your exit.

Using visuals and audio recording of employees for promoting the hotel

We use internal and external communication mediums for the promotion of our hotel and our services. We promote our services for organizations such as conferences, weddings, meetings etc.. Video or photo shoots of the related organizations are made. These images are used in our Company's social media accounts and for training. Limited to only promoting our services, it may be necessary to use the audio or visuals of our relevant employees in these promotions.

Vehicle Tracking System

Company vehicles are procured by means of purchasing services or through ownership. Entry-exit information of the vehicles, license plates, mileage and driver information are recorded, tracked and reported at the security gate and at the employee entrance. The purpose of this implementation is solely for the safety of our vehicles in circumstances such as emergency intervention in case of malfunctioning of the vehicles and for fuel tracking, thus it is not about obtaining information about the personal lives of our employees.

Organizations Such As Employee of the Month, Lotteries Etc.

In various departments of our Company, the employee of the month is selected and those selected are announced on the employee bulletin boards with their name, surname, department and photographs. Also, the employees who are the winners of such organizations as competitions, suggestions, and proposals are announced with their name, surname, department and photographs.

Sharing Personal Data with Third Parties

For your security and to fulfil our Company's legal obligations, your personal data shall be shared with public legal entities such as the Personal Data Protection Authority, Ministry of Finance, Ministry of Customs and Trade, Ministry of Labour and Social Security, Turkish Employment Agency (İş-Kur), Information and Communication Technologies Authority, relevant institutions or organizations to the extent permitted and required by other legislative provisions including but not limited to the Labour Law, Occupational Health and Safety Law, Social Security and Universal Health Insurance Law, Law on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications, Turkish Commercial Code, Personal Data Protection Law No. 6698 and the Identity Notification Law. For example; personal data of employees are shared with the Social Security Institution in order to pay employee and employer premiums.



Sharing Personal Data with Our Business Partners

We use the SAP Employee payroll program and the "Employee Monthly Score Chart" to implement the Human Resources processes. The support staff of the software company may connect to the programs on-site or remotely to intervene if there is any need for technical support. In this context, your personal information in the payroll program may inevitably be seen by the relevant support staff. We have a confidentiality agreement with the aforesaid company regarding the protection of your personal data.

Sharing your personal and sensitive personal data with regard to the Occupational Health and Safety Legislation:

Your personal and sensitive personal data may be shared with our on-site doctor during the recruitment process and for periodic health checks, as well as Kemer Medical Center Özel Sađ.Hiz.Tur.Tic. ve A.Ş. (Anadolu Hastanesi), the businesses within Carya Turizm Yatırımları A.Ş, Güvenok Lojistik Akaryakıt ve Turizm San.Tic. A.Ş. and Öztürk Group.

Sharing Personal Data with Our Internal Lawyers

In the duration or following the termination of the employment contract or in other cases such as lawsuits etc., your personal data may be shared with our internal lawyers provided that it is limited to the purpose of the case.

Sharing Your Personal Data within the Scope of Information Technologies (Information Processing) Support and Archiving:

In the event of receiving backup and support services from third companies in terms of information technologies, electronically stored personal data may be seen by the backup and support teams hence confidentiality agreements will be made with the relevant companies.

Sharing Your Personal Data within the Scope of Information Technologies (Information Processing) Support Services:

Phones and computers may malfunction from time to time and our Information Technologies Department may need to intervene. It should be taken into account that personal files, correspondence, calls, videos and images or Outlook correspondence may be seen within the scope of this intervention. For this reason, we kindly request that you are careful to avoid personal, private and confidential correspondence from company computers and phones and that you do not keep such files.

In addition, we would like to inform you that backups are always made by our IT Department to restore lost data so as to ensure that work can be carried out without interruption in the event of data loss.

Sharing your personal data for organizations such as travel, education, meetings etc.

Your personal data may be shared with third parties in a limited manner for all business-related organizations such as business travel, company organizations, trainings, company meetings. For example:



Transferring information such as name-surname, telephone, postal address to the printing house for printing business cards. Transferring information such as Turkish ID number, name-surname, and telephone number to the travel agency for domestic or international business travel ticketing services.

Sharing Your Personal Data with Department Managers:

During and after recruitment, your personal file is shared with your department managers solely for purposes such as getting to know the employee and obtaining information about his/her performance, after the transaction your personal file is retrieved and stored in the archive room.

Unauthorized / Accidental Use of Personal Data:

The processing of personal data and/or sharing personal data with third parties by employees, including those who are not authorized to access personal data due to their job position or task, by means of exceeding their authorization and / or abusing their authority, with the exception of processing data for personal reasons or purposes, shall be in violation of paragraph (1) of Article 12 of Personal Data Protection Law No.6698, hence employees must conduct their work and transactions within the scope of the Personal Data Protection Law No.6698 in accordance with the legislation, the terms of this contract, and the instructions of the employer and the workplace.

Employees should always take appropriate technical and administrative security measures to protect personal data against unauthorized or illegal processing and accidental loss, copying, destruction or damage.

Employees should not share personal data with a third party without the prior written consent of the employer and the workplace.

Employees should immediately notify the authorized supervisor in the event that personal data is lost, copied, destroyed or damaged unlawfully, or in case personal data is shared with third parties without authorization.

The confidentiality obligation of the employees shall continue indefinitely even if the Employment Contract expires.

According To Article 11 Of The Law, You Have The Following Rights:

- a) To learn whether personal data has been processed or not,
- b) To request information regarding personal data if it has been processed,
- c) To learn the purpose of the processing of personal data and whether it is used for its intended purpose,
- d) To know the third parties to whom personal data has been transferred to at home or abroad,
- e) To request the rectification of incomplete or incorrect personal data, if any,
- f) To request the deletion or destruction of personal data,
- g) To request the notification of operations carried out as per subparagraphs (d) and (e) to third parties to whom personal data has been transferred,
- h) Object to the occurrence of any result that is detrimental to your interests by means of analysis of personal data exclusively through automated systems,



- i) To request compensation for the damage arising from the unlawful processing of your personal data.

Your requests in your application shall be concluded free of charge within thirty days at the latest, depending on the nature of the request. However, if the transaction necessitates an additional cost for the Company, the fee determined by the Personal Data Protection Board in the “Communique on the Procedures and Principles on the Application to the Data Controller” may be charged.

You are required to submit your application to our Company regarding the processing of your personal data by filling out the application form on our Company's internet address, in writing to our Human Resources department or by using your registered e-mail address, secure electronic signature, mobile signature or by using your e-mail address which you have previously submitted to us and which is kept in our records. Depending on the reason of your request and your application method, additional verifications (such as sending a message to your registered phone, or a phone call) may be requested by our Company in order to determine whether the application belongs to you and thus to protect your rights. For example; if you apply through your e-mail address registered at the Company, we may contact you using another contact method registered in the Company and request confirmation of whether the application belongs to you.

DATA CONTROLLER IDENTITY

CARYA TURİZM YATIRIMLARI A.Ş.

Address: Kısıklı Mahallesi Alemdağ Caddesi No: 60d/6 Üsküdar İstanbul

KEP Address: caryaturizm@hs01.kep.tr

CONTACT INFORMATION

Address: Regnum Carya- Kadriye Bölgesi Üçkumtepesi Mevkii, Belek Antalya

Phone: +90 (242) 710 3434

Fax: +90 (242) 710 3400

Contact Person: Nevin EMEKLİ

Mobile phone: +90 534 595 02 20

E-Mail: kvkk@regnumhotels.com