Daz Spor Aktiviteleri Ve Organizasyonlari Anonim Sirketi

Privacy Policy

and

Policy on Processing and Protection of Personal Data

According to paragraph 3 of Article 20 of the Constitution of the Republic of Türkiye, "*Everyone has the right to request the protection of his/her personal data. This right includes the right to be informed about his/her personal data, to access such data, to request their correction or deletion, and to learn whether they are used for their intended purposes. Personal data may only be processed in cases stipulated by law or with the explicit consent of the person...*"

The right to protection of personal data as a fundamental human right is included in Article 8 of the Charter of Fundamental Rights of the European Union and Article 16 of the Treaty on the Functioning of the European Union.

Article 4 of the LPPD lists the basic principles that must be complied with for the processing of personal data. These principles are taken into consideration and meticulously applied within the scope of all personal data processing activities carried out by Daz Spor Aktiviteleri Ve Organizasyonlari Anonim Sirketi ("COMPANY" or Company). The basic principles followed by the Company in data processing processes are as follows:

Processing in Accordance with the Law and Good Faith: The "COMPANY" acts in accordance with the general principles of law and the rule of honesty while fulfilling its obligation to process and protect personal data.

Accurate and Up-to-date Processing of Personal Data: The "COMPANY" is aware that the provision of accurate and up-to-date personal data about individuals is of great importance for the protection of the rights of individuals. It shows the utmost care to ensure that the personal data being processed is accurate and up-to-date.

Processing Personal Data for Specific, Explicit and Legitimate Purposes: LPPD requires data processing activities to be processed for specific, explicit and legitimate purposes. Within the framework of this principle, the "COMPANY" carries out personal data processing activities for specific, explicit and legitimate purposes required by its activities.

Processing in Line with, Limited to and Restrained with the Purpose They are Processed The "COMPANY" processes personal data within the limits sufficient to fulfill the purposes determined within the scope of its activities. The "COMPANY" acts in accordance with the principle of being limited and restrained by avoiding processing personal data that is not needed.

Retention for the Time Envisaged in the Relevant Legislation or Required for the Purposes for Which It is Processed Personal data processed by the "COMPANY" are retained for the period until the personal data processing conditions disappear. When the aforementioned purposes disappear, the "COMPANY" will terminate the retention of the relevant personal data. The Company transparently informs all relevant parties about all data processing processes with the necessary documents.

INTRODUCTION

Law No. 6698 on the Protection of Personal Data (LPPD/Law) was published in the Official Gazette dated April 7, 2016 in order to protect the fundamental rights and freedoms of individuals, especially the privacy of private life, in the processing of personal data belonging to natural persons, and to regulate the obligations of natural and legal persons who process personal data and the procedures and principles to be followed.

1. PURPOSE OF THE POLICY

Daz Spor Aktiviteleri Ve Organizasyonlari Anonim Sirketi's Policy on Processing and Protection of Personal Data (the Policy) has been prepared with the aim of disciplining the processing of personal data to be processed during the activities carried out in accordance with the legislation and protecting the fundamental rights and freedoms, especially the privacy of private life, stipulated in the Constitution.

While preparing the "Policy", it has been determined as a basic principle to determine which data and why the working units within the "COMPANY" organization collect and why they transfer this data to third parties and to understand the personal data processing procedure of the Company. In addition, with this Policy, it is aimed to determine the administrative and technical measures to be taken to protect data confidentiality within and outside the "COMPANY" organization, to explain these measures and to inform and enlighten the individuals whose data are processed.

2. SCOPE OF THE POLICY

The scope of the "Policy" includes all natural persons whose data are processed directly or indirectly due to the activities of the "COMPANY".

Within the scope of this "Policy", customized information about the data processed within the framework of the transactions and activities within the organization of the "COMPANY", data categorization, data recipient groups, legal reason and method of data collection, third party groups to which data is transferred, data processing periods, and data destruction periods are included.

3. DEFINITIONS

Explicit Consent: Refers to the consent with regard to a specific subject, based on information and expressed by free will.

Cookie: They are small files that are saved on the computers or mobile devices of the users and help store their choices and other information on the web pages they visit.

Relevant User: The persons who process personal data within the organization of the data supervisor or in line with the authorization and instruction received from the data supervisor, except for the person or unit responsible for the technical storage, protection and backup of the data.

Destruction: Deletion, destruction or anonymization of personal data.

Contact Person: The natural person notified by the data controller during the registration to the Registry for the communication to be established with the Authority regarding

the obligations of the legal entities resident in Türkiye and the non-resident legal entity data controller representative within the scope of the Law and the secondary regulations to be issued based on this Law.

(The contact person is not authorized to represent the Data Controller. As is evident from its name, s/he is the person assigned to establish “contact” amongst the data controller, data subjects and the Authority.)

LPPD: Law No. 6698 on the Protection of Personal Data dated March 24, 2016, published in the Official Gazette dated April 7, 2016 and numbered 29677.

Recording Media: Any media where personal data is processed wholly or partially automatically or non-automatically, provided that it is a part of any data recording system.

Personal Data: Any information related to the person whose identity is identified or identifiable.

Processing of Personal Data: All kinds of operations performed on data such as obtaining, recording, storing, maintaining, altering, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the using of personal data through fully or partially automated or non-automatic means provided that it is part of any data recording system.

Anonymization of Personal Data: Making data in no way to be associated with an identified or identifiable natural person, even by matching with other data.

Deletion of Personal Data: Making personal data inaccessible and unusable for Relevant Users in any way.

Destruction of Personal Data: The process of making personal data inaccessible, unrecoverable and reusable in any way.

Board: Personal Data Protection Board

Authority: Personal Data Protection Authority.

Private Personal Data: Data with respect to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance, foundation or trade union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data.

Periodic Destruction: The deletion, destruction or anonymization process to be carried out ex officio at recurring intervals specified in the personal data storage and disposal policy in the event that all the conditions sought for the processing of personal data are eliminated.

Policy: The policy on the processing and protection of personal data created by the Data Controller.

VERBIS: It is a registration system that natural and legal persons who process personal data must register before starting to process personal data and enter information on a categorical basis about the personal data they process.

Data Processor: Natural or legal person who processes personal data on behalf of the data controller basing on the authority given by him/her.

Data Recording System: The recording system where personal data are structured and processed based on certain criteria.

Data Owner/Data Subject: The natural person whose personal data is processed.

Data Controller: Natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

5. PURPOSES OF PROCESSING YOUR PERSONAL DATA, YOUR PERSONAL DATA WE PROCESS, METHODS OF COLLECTION AND LEGAL REASONS

i. Purposes of Processing

Your personal data will be used in compliance with the limits stipulated in the LPPD and in order to realize the purposes shown in the legislation related to the "COMPANY". The purposes of processing are as follows;

- Execution of Emergency Management Processes
- Execution of Information Security Processes
- Execution of Employee Candidate / Intern / Student / Volunteer Selection and Placement Processes
- Execution of Application Processes of Employee / Volunteer Candidates
- Fulfillment of Obligations Arising from Employment Contract and Legislation for Employees
- Execution of Fringe Benefits Processes for Employees
- Execution of Access Authorizations
- Execution of Activities in Compliance with the Legislation
- Execution of Finance and Accounting Affairs
- Execution of Company / Product / Service Loyalty Processes
- Ensuring Physical Space Security
- Execution of Assignment Processes
- Follow-up and Execution of Legal Affairs
- Execution of Communication Activities
- Planning of Human Resources Processes
- Execution / Supervision of Business Activities
- Execution of Occupational Health / Safety Activities
- Receiving and Evaluating Suggestions for Improvement of Business Processes
- Execution of Business Continuity Ensuring Activities
- Execution of Goods / Service Procurement Processes
- Execution of Goods / Services After Sales Support Services
- Execution of Goods / Service Sales Processes
- Execution of Goods / Services Production and Operation Processes
- Execution of Customer Relationship Management Processes
- Execution of Activities for Customer Satisfaction
- Organization and Event Management
- Exexution of Marketing Analysis Studies
- Execution of Advertising / Campaign / Promotion Processes
- Execution of Risk Management Processes
- Execution of Storage and Archive Activities

- Execution of Contract Processes
- Execution of Sponsorship Activities
- Execution of Strategic Planning Activities
- Ensuring the Security of Movable Properties and Resources
- Execution of Marketing Processes of Products / Services
- Ensuring the Security of Data Controller Operations
- Execution of Talent / Career Development Activities
- Providing Information to Authorized Persons, Institutions and Organizations
- Execution of Management Activities
- Creating and Tracking Visitor Records

ii. Your Personal Data We Process

- Identity (such as name, surname, mother's and father's name, mother's maiden name, date of birth, place of birth, marital status, identity card serial number, Turkish ID number)
- Contact (such as address no, e-mail address, contact address, registered electronic mail address (KEP), telephone no)
- Location (location information of where it is located)
- Personnel (such as payroll information, disciplinary investigation, employment records, property declaration information, CV information, performance evaluation reports)
- Legal Action (such as information in correspondence with judicial authorities, information in the case file)
- Customer Transaction (such as call center records, invoice, promissory note, check details, information on desk receipts, order information, request information)
- Physical Space Security (such as employees' and visitors' entry and exit records, camera records)
- Transaction Security (such as IP address information, website login and log out information, password information)
- Professional Experience (such as diploma information, courses attended, vocational training information, certificates, transcript information)
- Marketing (shopping history information, surveys, cookie records, information obtained through campaigns)
- Appearance (information on appearance)
- Health Information (such as information on disability status, blood type information, personal health information, device and prosthesis information)
- Criminal Conviction and Security Measures (such as information on criminal conviction, information on security measures)

iii. Methods of Collecting Your Personal Data

Your personal data are collected through the member registration form, registration/application forms filled out over the internet, receipt and expenditure documents, video and audio recording devices used in events, security camera recordings and the official e-mail address of the COMPANY,info@runkara.com.tr or any e-mail address of the Company.

Personal data is also collected by physically sending documents, physically filling out a document provided by the Company or calling other extension numbers of the Company.

Your personal data is also collected automatically through cookies used on https://runkara.com.tr/ and its extensions. These cookies are only necessary for the visitor to

use the site with full efficiency and are used to remember the visitor's preferences and do not provide any other personal data. You can access our cookie policy at https://runkara.com.tr/.

iii. ***Legal Reasons for Personal Data Processing***

- If the data subject has explicit consent,
- If it is explicitly stipulated in the laws,
- If it is compulsory for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid,
- If it is necessary to process personal data of the parties to the contract, provided that it is directly related to the conclusion or performance of a contract,
- If it is mandatory for the data officer to fulfill his/her legal obligation,
- If it is made public by the data subject himself/herself,
- If data processing is compulsory for the establishment, exercise or protection of a right,
- If it is necessary to process data for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data owner.

The basic processing condition for **private personal data** is explicit consent and the Company basically does not aim to process private personal data. However, your private personal data that we need to process due to our activities or that you have approved with your explicit consent are also processed in a restrained manner within the scope of the legislation.

The conditions listed in the LPPD for the processing of private personal data are as follows;

- If the data subject has explicit consent,
- If it is explicitly stipulated in the laws for private personal data other than health and sexual life,

Personal data relating to health and sexual life can only be processed for the purpose of;

- Protection of public health,
- Preventive medicine,
- Medical diagnosis,
- Carrying out treatment and care services,
- Planning and management of health services and financing,
- by persons under the obligation to keep secrets or authorized institutions and organizations without seeking the explicit consent of the person concerned.

6. TRANSFER OF PERSONAL DATA

Your personal data is shared with authorized public institutions and organizations, judicial authorities, enforcement authorities, law enforcement authorities, law enforcement units and suppliers, business partners and shareholders from whom contracted products and or services are purchased for the purposes and by the means shown in this Policy. The table below shows the parties with whom the information is shared:

Persons to whom Data can be Transferred	Description	Purpose
Shareholders	Shareholders who are authorized to design the strategies and audit activities regarding the company's commercial activities in accordance with the provisions of the relevant legislation	Sharing of personal data limited to the design of strategies regarding the Company's commercial activities and for audit purposes
Legally Authorized Private Law Persons	Private law persons legally authorized to obtain information and documents from the company	Sharing data limited to the purpose requested by the relevant private law persons within their legal authority
Legally Authorized Public Institutions and Organizations	Public institutions and organizations legally authorized to obtain information and documents from the company	Sharing personal data limited to the purpose of requesting information by the relevant public institutions and organizations
Suppliers	Suppliers from which the company receives services	Sharing personal data with the suppliers it works with in order to ensure the continuity of the company's activities.

7. RIGHTS OF DATA SUBJECT

Within the scope of the LPPD, you are entitled to;

- Learn whether your personal data is processed,
- Request information on your Personal Data if it has been processed,
- Learn the purpose of processing your Personal Data and whether they are used appropriately for this purpose,
- Know the third parties to whom your Personal Data is transferred, at home or abroad,
- Request correction of your Personal Data if it is incomplete or improperly processed,
- Request your Personal Data to be deleted or destroyed within the framework of the provisions of the LPPD legislation,
- Request notification of the transactions regarding the destruction or correction of your Personal Data to third parties to whom the data is transferred,
- Object to the appearance of a result against yourself by analyzing the processed data exclusively through automated systems,
- Request the compensation of damages in case of loss due to the illegal processing of your Personal Data.

How Can You Exercise Your Rights?

Data owners can exercise their rights listed above with the application they will send via info@runkara.com.tr at https://runkara.com.tr/.

The application must include;

- Name, surname and, if the application is in writing, the signature,
- Turkish ID number for citizens of the Republic of Türkiye, nationality, passport number or ID number, if any, for foreigners,
- Residential or workplace address for notification,
- Electronic mail address, telephone and fax number for notification, if any,
- Subject of the request.

- Information and documents related to the subject shall be attached to the application.
- In written applications, the date on which the document is notified to the data controller or its representative is the date of application.
- For applications made by other methods; the date the application is received by the data controller is the date of application.

The Data Controller may also request additional information and documents in order to answer the application and to confirm the identity of the data subject. If this information is not provided, the data controller may not answer the application.

The “COMPANY” finalizes the requests as soon as possible and within 30 days at the latest. The result of the evaluation is notified to the relevant person in writing or electronically, and if the request is accepted, the necessary action is taken in accordance with the LPPD.

In cases where the applications of the data subjects are rejected, the answer given is insufficient or the application is not responded to in due time, data subject may file a complaint to the Personal Data Protection Board within 30 days from the date of learning the answer in accordance with Article 14 of the LPPD.

9. INFORMATION ON THE PROCESSING OF PERSONAL DATA

9.1. Channels through which Personal Data is Obtained

Personal data is obtained through the following channels as needed.

- Organization, Event, Conference Participant-Invitee
- Employee Personnel File Documents
- Camera Recordings,
- SMS/E-Mail, Telephone
- Website, Applications, Cookies and Similar Tracking Technologies,
- Fax,
- Mail, Cargo or Courier Services,
- Other Physical and Electronic Media.

9.2. Classification of Personal Data

Categorization of personal data is extremely important for compliance with the legislation. Our legislation categorizes personal data under two categories: personal data and private personal data.

- Identity (such as name, surname, mother's and father's name, mother's maiden name, date of birth, place of birth, marital status, identity card serial number, Turkish ID number)
- Contact (such as address no, e-mail address, contact address, registered electronic mail address (KEP), telephone no)
- Location (location information of where it is located)
- Personnel (such as payroll information, disciplinary investigation, employment records, property declaration information, CV information, performance evaluation reports)
- Legal Action (such as information in correspondence with judicial authorities, information in the case file)
- Customer Transaction (such as call center records, invoice, promissory note, check details, information on desk receipts, order information, request information)
- Physical Space Security (such as employees’ and visitors’ entry and exit records, camera records)
- Transaction Security (such as IP address information, website login and log out information, password information)
- Risk Management (such as information processed to manage commercial, technical, administrative risks)
- Finance (such as balance sheet information, financial performance information, credit and risk information, asset information)
- Professional Experience (such as diploma information, courses attended, vocational training information, certificates, transcript information)

- Marketing (shopping history information, surveys, cookie records, information obtained through campaigns)
- Audiovisual Recordings (such as audiovisual recordings)
- Race and Ethnicity (such as race and ethnicity information)
- Political Opinion Information (such as information indicating political opinion, political party membership information)
- Philosophical Beliefs, Religion, Sect and Other Beliefs (such as information on religious affiliation, information on philosophical beliefs, information on sectarian affiliation, information on other beliefs)
- Appearance (information on appearance)
- Association Membership (such as association membership information)

Contact Person Classification

The classification of the “COMPANY” for data subjects is shown in the table below:

- Employee Candidate
- Employee
- Volunteer
- Competitor
- Subject of the news
- Shareholder/Partner
- Potential Product or Service Purchaser
- Intern
- Supplier’s Employees
- Supplier’s Authorized Person
- Product or Service Purchaser
- Parent / Guardian / Representative
- Visitor
- Other

STORAGE AND DESTRUCTION OF PERSONAL DATA

"COMPANY" stores the personal data of the data owners whose personal data it processes by taking the necessary technical and administrative security measures in electronic and physical environments.

The storage period of the “COMPANY” for personal data is calculated by taking into account the periods specified in the relevant legislation.

Personal data will be destroyed by the “COMPANY” in the event that the personal data processing purposes that will eliminate the existence of the personal data processing conditions in the LPPD cease to exist. Such destruction operations are carried out ex officio in **6-month periods** in accordance with the provisions of the relevant legislation or concluded if the requests from the data owners are found to be appropriate. In accordance with the legislation, the “COMPANY” shall fulfill the deletion and/or destruction requests of the data subject within **30 days** at the latest and inform the data subject, unless another period is stipulated in the legislation.

Minutes regarding the destruction of Personal Data shall be kept by the “COMPANY” for **3 years**. The periods stipulated in special legislation are reserved, and in

case the periods herein change due to changes in the LPPD and the relevant legislation, the current periods in question shall be applied.

CLARIFICATION OBLIGATION

Pursuant to Article 10 of the LPPD, the “COMPANY” shall fulfill the clarification obligation mentioned in the LPPD by providing the following information to the relevant data subjects during the acquisition of personal data:

- Identity of the data controller and its representative, if any,
- The purpose for which personal data will be processed,
- To whom and for what purpose the processed personal data may be transferred,
- The method and legal reasons for collecting personal data,
- Other rights listed in Article 11.

The “COMPANY” prepares appropriate clarification texts and presents them to the data subjects in order to fulfill its clarification obligation while carrying out its activities.

PRECAUTIONS FOR THE SECURITY OF PERSONAL DATA

The “COMPANY” shows all reasonable care and attention to ensure the confidentiality and security of the personal data it processes. In addition to the requirements of the relevant legislation, the “COMPANY” takes technical and administrative measures at a reasonable level to ensure data privacy and security within the framework of Article 12 of the LPPD. With the aforementioned administrative and technical security precautions, it is aimed to prevent illegal processing of personal data, to prevent illegal access to personal data, and to keep personal data at an appropriate security level.

In case personal data is illegally seized by third parties, it shall notify the data owners, the Board and other relevant public institutions and organizations in accordance with the provisions of the relevant legislation.

The Personal Data Security Guide (Technical and Administrative Precautions) ad Board resolutions published by the Board are taken into account when taking precautions regarding the security of personal data.

Technical and Administrative Measures

- Network security and application security are ensured.
- Closed system network is used for personal data transfers through the network.
- Key management is implemented.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- Security of personal data stored in the cloud is ensured.
- There are disciplinary regulations that include data security provisions for employees.
- Trainings and awareness raising activities on data security are conducted for employees at regular intervals.
- An authorization matrix has been established for employees.
- Access logs are kept regularly.

- Corporate policies on access, information security, use, storage and destruction have been prepared and implemented.
- Data masking measures are applied when necessary.
- Confidentiality undertakings are made.
- The authorizations of employees whose jobs are changed or who leave their jobs are removed.
- Up-to-date anti-virus systems are used.
- Firewalls are used.
- Signed contracts contain data security provisions.
- Extra security measures are taken for personal data transferred via paper and the relevant document is sent in confidential document format.
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported quickly.
- Personal data security is monitored.
- Necessary security measures are taken for entry and exit to and from physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (fire, flood, etc.).
- Security of environments containing personal data is ensured.
- Personal data is minimized as much as possible.
- Personal data is backed up and the security of backed up personal data is also ensured.
- User account management and authorization control system is implemented and monitored.
- Internal periodic and/or random audits are conducted and have them conducted. Log records are kept without user intervention.
- Existing risks and threats have been identified.
- Protocols and procedures for the security of private personal data have been determined and implemented.
- If private personal data is to be sent via electronic mail, it is sent encrypted and using KEP or corporate mail account.
- Secure encryption / cryptographic keys are used for private personal data and managed by different units.
- Intrusion detection and prevention systems are used.
- Penetration testing is applied.
- Cyber security measures have been taken and their implementation is constantly monitored.
- Encryption is performed.
- Private personal data transferred in portable memory, CD, DVD media are encrypted.
- Data processing service providers are periodically audited on data security.
- Awareness of data processing service providers on data security is ensured.
- Data loss prevention software is used.
- Other

KEEPING RECORDS OF THE INTERNET SERVICE PROVIDED IN THE COMMON AREA

For the purposes of ensuring security by the “COMPANY” and for the purposes specified in this Policy, Internet access can be provided by the “COMPANY” to visitors who request it during their stay at the “COMPANY” premises. In addition, the log records of Internet accesses are registered according to the provisions of the Law No. 5651 and to the superseding provisions of the legislation regulated according to this Law and these records are only processed if required by authorized public institutions or organizations or to fulfill the legal obligations in the audit processes to be carried out within the “COMPANY”.

Company employees who have access to the aforementioned records access these records only for use in requests or audit processes from authorized public institutions and organizations and transfer them to legally authorized persons. The clarification obligation is fulfilled before the relevant processing activity.

PROCESSING OF PERSONAL DATA COLLECTED THROUGH COOKIES

Our Company uses Cookies in order to improve the functioning and use of our websites or mobile applications and as mandatory for our website to perform its activities. Your personal data is processed and transferred through cookies on our digital platforms.

Necessary technical and administrative measures are taken by our Company to ensure the security of personal data collected through cookies in accordance with Article 12 of the LPPD.

IDENTITY OF THE DATA CONTROLLER

Details of the identity of the data controller for all kinds of personal data processing activities covered by this policy are provided below.

Data Controller	***COMPANY*** Daz Spor Aktiviteleri Ve Organizasyonlari Anonim Sirketi
Address	Kizilirmak Mah. Dumlupinar Bul. YDA CENTER NO:9/A KAT:11 NO:355 Cukurambar Cank Ank
Phone	+90 536 590 67 83
Website	https://runkara.com.tr/

17. ENFORCEMENT

This Policy issued by the ***Company*** entered into force on 15.03.2023 and was presented to the public. In case of any conflict between the legislation in force, particularly the Law, and the regulations in this Policy, the provisions of the legislation shall apply.

The ***Company*** reserves the right to make changes in the Policy in parallel with legal regulations. The current version of the Policy is available at (https://runkara.com.tr/).

Date of Last Update: 15.03.2023