+90 850 255 8080
Atakum, Samsun, Turkey
getride.tr info@getride.tr

GETRİDE TOURISM AND TRAVEL AGENCIES INC. TRANSFER SERVICES VIA ITS MOBILE APP AND WEBSITE COMPREHENSIVE KVKK INFORMATION NOTICE AND PRIVACY POLICY

1. Identity of the Data Controller and Definitions

In accordance with the Personal Data Protection Law No. 6698 ("KVKK"), GETRİDE TOURISM AND TRAVEL AGENCIES INC. ("We") acts as the data controller.

Data Subject / User: A natural person who uses our mobile application and/or utilizes our transfer services; U-ETDS:

The Transportation Electronic Monitoring and Inspection System;

D2 Certificate: A document certifying that carrier companies with which we have a commercial partnership are authorized to provide non-scheduled and contract-based passenger transportation services in accordance with the Road Transport Regulation.

2.1. Categories of Processed Personal Data

Your personal data collected through our systems is categorized as follows, according to its nature: Identity Data: First name, last name, Turkish ID Number (or Foreign ID/Passport Number), date of birth, gender. Contact Data: Phone number, email address, registered residence/billing address.

Location Data: Real-time location information obtained via GPS, boarding and disembarkation (destination) points, travel routes.

Financial Data: Billing information, payment type, tax office/number (for corporate invoices). Your credit card/debit card information is not stored in our Company's systems but is transmitted directly to the encrypted infrastructure of a contracted BDDK-licensed payment institution (e.g., iyzico, PayTR, etc.).

Customer Transaction and Travel Data: Date and time of reservation creation, travel history, favorite locations, applied discount/promotion codes, cancellation/refund transactions, and records of written correspondence and voice calls made through the call center or in-app support module.

Transaction Security and Digital Trace Data: IP address, device model and operating system (OS) information, device ID, app login/logout logs, cookies, and third-party SDK (Software Development Kit) data.

Physical Premises Security Data: Closed-circuit television (CCTV) recordings from D2-certified vehicles belonging to our independent business partners (Carriers) registered on the platform network, which capture only video footage. *(For the purpose of protecting personal privacy, no audio recordings are made inside these vehicles under any circumstances. Our passengers are also informed via physical camera warning labels placed in visible areas inside the vehicles.)*

Marketing Data: Processed upon provision of explicit consent; shopping habits, campaign usage information, market research, and survey data.

2.2. Processing of Personal Data of Individuals Under 18 (Children) and Parental Consent

In accordance with the Platform's terms of commercial use, individuals must be at least 18 years of age and possess full legal capacity to create an account and make reservations directly. In cases where individuals under the age of 18 ("Children") actually use our transfer services (traveling as a passenger, guest, or escort), the following identification (First Name-Last Name, Turkish ID Number/Passport) and location data required for the fulfillment of the transfer agreement must be declared and provided to the Platform exclusively by the child's legal guardian or a legally authorized adult User (account holder) designated by the parent(s).

Our company acknowledges, within legal limits, the existence of parental/guardian consent and the provision of information regarding the processing of children's personal data; it further acknowledges that parents or adult User account holders, when entering children's data into the Platform, undertake to approve the provisions of this privacy notice on behalf of the child as well. Parents holding parental authority or guardianship may personally exercise all rights related to the deletion, updating, or processing of their children's data on their children's behalf as legal representatives, in accordance with the procedures specified in Article 8.

2.3. Terms of Use for Cookies and Third-Party SDKs

Our Platform (mobile app and website) uses various types of cookies and Third-Party Software Development Kits (SDKs) to improve the user experience, ensure system security, and optimize service quality. The cookies used on the Platform are categorized by function as follows:

Essential (Necessary) Cookies and SDKs: These are essential for the platform to function, to keep user sessions active, to securely complete reservations, and to keep the map infrastructure (Google/Apple Maps) active. Data processed through these cookies is automatically processed based on the legal grounds of the conclusion or performance of a contract (KVKK Article 5/2-c).

Analytics and Performance Cookies: These are used to ensure the stable operation of the mobile app, detect potential system errors (crash logs), and optimize performance (via Firebase and AWS infrastructure). These cookies are processed based on the legal ground of our Company's legitimate interests (KVKK Article 5/2-f).

Marketing and Advertising Cookies: If you provide your explicit consent, these cookies are processed to present campaigns, promotions, and targeted ads tailored to your preferences. These cookies are activated only if the data subject has provided explicit consent (KVKK Article 5/1).

Controlling and Disabling Cookies: Our users can disable marketing and analytics cookies at any time by using the Cookie Preference Panel on our website or through their web browser settings. In mobile apps, you can manage your cookie and tracking preferences via "Privacy > Ad Tracking" in your device settings or through the in-app settings. We would like to inform you in advance that if essential cookies are disabled, some technical functions of the Platform (particularly map matching and location-based vehicle assignment features) may not work partially or entirely.

2.4. Methods and Channels for Collecting Personal Data

Your personal data is collected within the scope of the legal and commercial relationship you have established with our Company; for the purpose of ensuring that our services are provided in an uninterrupted, secure, and legally compliant manner, through the digital and physical channels listed below, using methods that are fully or partially automated, or non-automated methods provided they form part of a data recording system:

Mobile App and Website: Through membership registration forms, profile creation screens, and real-time/scheduled reservation forms that you fill out yourself on the platform,

Software Integrations and APIs: Through digital reservation records transferred to the GetRide.tr infrastructure via corporate travel agencies (Booker), API integration channels, and the systems of our corporate partners,

Call Center and Voice Support Line: Through voice call recordings made with our call center during your support requests, complaint management processes, or reservation changes,

WhatsApp and Live Support Channels: Through information, documents, and correspondence you share with our customer representatives via the in-platform live support module, our official WhatsApp support line, or instant messaging platforms,

Email and Contact Forms: Through any written communication channel you establish via our company's official contact forms or our verified corporate email addressinfo@getride.tr ,

Contracts and Electronic Consent Mechanisms: Through timestamps and log data automatically recorded by the system during the digital approval/signing of the User Agreement, Carrier Agreement, Agency Agreement, and Driver Undertakings,

Device and Infrastructure Sensors: Data is automatically collected through GPS location services running in the background or foreground of your device while using our mobile app, cookies, third-party SDK integrations (Firebase, AWS, Google Maps), and transaction security logging mechanisms.

3. Purposes and Legal Grounds for Processing Personal Data

Your personal data is processed based on the legal grounds specified in Articles 5 and 6 of the KVKK for the following purposes:

Issuance of U-ETDS legal notices: Your identity and location data are processed based on the legal grounds set forth in Articles 5/2-a and 5/2-c of the KVKK.

Reservations, vehicle allocation, and fulfillment of the trip: Your identification, contact, location, and customer transaction data are processed based on the legal basis set forth in Article 5/2-c of the KVKK.

VIP Meet-and-Greet (Airport/Hotel Boarding): Your identification (first and last name) and location data are processed within the scope of the performance of the service contract (Article 5/2-c of the KVKK).

Ensuring passenger and driver safety: Your location and physical environment (in-vehicle camera) data are processed based on the legal basis set forth in Article 5/2-f of the KVKK.

Facilitating communication between the driver and passenger: Your communication data is processed based on the legal grounds of contract performance and legitimate interest (KVKK Article 5/2-c and f) using a masked call infrastructure.

Billing and maintenance of accounting records: Your identity, communication, and financial data are processed for the purpose of fulfilling a legal obligation (Article 5/2-ç of the KVKK).

Resolution of application errors and transaction security: Your transaction security and digital trace data are processed in accordance with the provisions of Law No. 5651 and our company's legitimate interests (KVKK Article 5/2-a and f).

Sending commercial electronic communications (SMS/Email): Your identity, contact, and marketing data are processed for campaign and promotional purposes only if the relevant individual has given explicit consent (KVKK Article 5/1).

Request, Complaint Management, and Quality Standards: Voice call recordings and your correspondence received through the call center and support module are processed in accordance with our company's legitimate interests (KVKK Article 5/2-f) for the purposes of resolving potential service deficiencies, serving as evidence in commercial disputes, and improving service quality.

4. Parties to Whom Personal Data Is Disclosed and Purposes of Disclosure

Your collected data is shared, limited to the "need-to-know basis":

Government Agencies: In accordance with the Road Transport Regulation, the Ministry of Transport and Infrastructure of the Republic of Turkey (real-time data flow via the U-ETDS platform), the General Directorate of Security, judicial authorities, and authorized supervisory bodies;

Our Business Partners and Drivers: To independent carrier companies that will actually perform the transfer service (limited to fulfilling legal U-ETDS reporting obligations; including ID, passport/TCKN, and location data); and to drivers and meet-and-greet staff assigned by these companies (limited to first and last name, pickup/drop-off location, and masked call infrastructure).

Service Providers (Domestic): Payment infrastructure providers, e-invoice/e-archive integrators, independent audit and financial advisory firms, law firms, and call center infrastructure providers;

Transfer of Personal Data Abroad and Technology Providers (Cloud Services): To enable the Platform to perform its core functions, conduct real-time route optimization, ensure the stable operation of the mobile app, send notifications, and maintain uninterrupted operation of the mapping infrastructure; your transaction security, location, and digital trace data are transferred to our global technology providers with servers located abroad (Google Maps API, Apple Maps API, Firebase, AWS) in full compliance with the Standard Contractual Clauses (SCCs) established under Article 9/4 of the Personal Data Protection Law (KVKK). Accordingly, "Controller-to-Processor" data processing agreements (DPAs) are established between our Company and our global cloud and infrastructure providers to define the technical and legal boundaries of data processing.

Solely for the purpose of enabling independent Carrier companies, which will actually perform the transfer service, to fulfill their legal U-ETDS notification obligations; Identity (First Name-Last Name, Turkish ID Number/Passport Number, Nationality) and location data are shared with these companies under "Controller-to-Controller" data transfer protocols that comply with the KVKK legislation and define database access limits, data security obligations, and the legal liability limits of the parties. In accordance with the principle of data minimization, only the first and last names and the boarding/alighting locations are transmitted to the drivers and meet-and-greet staff who actually perform the transportation; data transfers are conducted via secure protocols (call masking/masked data) through API and encrypted database integrations, thereby preventing direct visibility of personal contact information.

5. Data Retention Periods

Your personal data is retained for the period required by applicable legislation or as necessary for the purposes for which it is processed:

Identity and Financial (Invoice) Records: 10 years from the end of the contract, in accordance with the Turkish Commercial Code and the Tax Procedure Code.

U-ETDS and Travel Log Records: 5 years, in accordance with relevant

transportation legislation. Traffic (Log) Records (IP addresses, etc.): 2 years, in

accordance with Law No. 5651.

In-Vehicle Camera Recordings: These are retained for a maximum of 30 days for security and public safety purposes; at the end of this period, they are automatically overwritten and deleted. In the event of any legal or administrative case, the relevant recordings are isolated and retained until the legal process is completed.

Marketing Consents: Your data will no longer be used for marketing purposes and will be deleted as of the date you withdraw your consent for commercial communications.

6.1. Data Security: Technical and Administrative Measures Taken

Our company takes high-level measures to prevent the unlawful processing of and unauthorized access to your personal data:

Technical Measures: Network and application security are ensured, and 256-bit SSL encryption is used on servers. Penetration tests are conducted periodically on application databases. Communication between drivers and passengers is facilitated using "Call Masking" technology, minimizing the visibility of your personal phone numbers to drivers to the extent permitted by the integration infrastructure.

Administrative Measures: Company staff and drivers undergo regular training on the Personal Data Protection Law (KVKK), and confidentiality and data security agreements are signed with them. Data access permissions are hierarchically restricted according to the "least privilege" principle.

6.2. Data Breach Notification Procedure:

In the event that the technological infrastructure, databases, or cloud servers managed by our company are subjected to a cyberattack, or if it is determined that processed personal data has been obtained by others through unlawful means (data breach); our company is obligated, in accordance with Article 12/5 of the Personal Data Protection Law (KVKK), to notify the Personal Data Protection Board without delay and no later than 72 hours after becoming aware of the situation.

Furthermore, the affected individuals (Users/Passengers) will be officially notified regarding the scope of the breach, its potential impacts, and the necessary security measures to be taken via our official website (www.getride.tr), in-app system notifications, or the communication channels registered in our systems (email/SMS) in the shortest reasonable time, in accordance with applicable laws.

7. In-App Account and Data Deletion Rights

Our users can delete their accounts at any time by using the [Profile > Settings > Delete My Account] button in the mobile app menu or by filling out the "Data Deletion Request" form on our website. Upon receipt of an account deletion request, all your profile data, location history, and device pairings—excluding data required to be retained by law (invoices, U-ETDS notifications, and transaction security logs subject to retention periods under Law No. 5651)—will be immediately and permanently deleted or anonymized.

8. Rights of the Data Subject Under Article 11 of the KVKK

As the data subject, you have the right to: learn whether your data is being processed; if so, request information about it; learn the purpose of processing and whether it is being used in accordance with that purpose; know the third parties to whom your data has been transferred within or outside the country; request the correction of incomplete or incorrect data, request the erasure or destruction of your data when legal conditions are met, and object if data processed via automated systems (e.g., algorithmic pricing, location assignment) results in a decision that adversely affects you.

Please submit your requests in accordance with the "Communication on the Procedures and Principles for Submitting Requests to the Data Controller" to:

Address: Güzelyalı Mah. 3040 Sk. Pekşen Apartment No. 3, Interior

Door No. 4, Atakum/SAMSUN—either in person with a wet signature or via a notary public;

KEP:getride@hs01.kep.tr —using a secure electronic signature;

Email: You may submit your application toinfo@getride.tr using the email address previously verified in our system.

Your applications will be processed free of charge within 30 (thirty) days at the latest.