

Privacy and Personal Data Protection Policy

This Privacy and Personal Data Protection Policy applies to Fabbri Rides Ltd (hereafter FRLTD]. FRLTD, as consulting service provider, ensure the protection and privacy of your personal data. In the following policy, we will outline how this is made possible, as well as your rights. In case you wish, you may contact us at info@fabbrirides.com.

In general

FRLTD is professional advisor about the design, manufacture and sale of amusement rides.

Definition of Personal Data

Personal data means any information according to which, a natural person can be identified and which, may, be grouped as follows:

- Personal information: fist name, surname, title, photograph, nationality, date of birth, gender, relationship to third persons, position, employer, copy of passport or identity, utility bills, bank statements, Tax Number and VAT Number
- Contact details: telephone and fax number, email and postal/residential address
- Financial information required for anti-money laundering or compliance purposes
- Business information: data identifying the clients in relation to matters on which you instruct us or in which you are involved
- Payment details: payment method, bank account number, account holder name, account security details, invoice records, payment records, SWIFT details, IBAN details, payment amount, payment date, records of cheques
- Information from publicly available sources
- Information in connection with investigations or proceedings: where this is necessary to provide our services to you
- Contact details and other information about you or your company or organization where you provide services to our Company
- Criminal record data: where permitted by national law and appropriate to do so, such as existence of prior criminal offences or convictions
- Any other information relating to you which you may provide to us, if required by us in order to be able to provide legal and other services to you

Collection of Personal Data

We collect personal data in the course of our work, in the following ways:

- Directly from our clients and associates
- From records you have publicized
- From public records and government sources
- When you provide services to our company
- Through your Website
- Through screening providers who assist us on our legal obligations

Use of Personal Data

Your personal data will be used in the following occasions:

- For the best possible provision of services related to consulting / auditing / advisory and other issues to our clients

- For the best possible management of our business relationship and communication with you
- For compliance with the applicable laws and applicable laws and regulations
- For the purpose of online security against unauthorized access
- For purposes of adherence to binding decisions
- For the financial management of our companies
- For purposes of research, while safeguarding your best interests and those of our companies, at every level

Principles of processing Personal Data

When processing personal data, we apply the following principles:

- The Principle of Lawfulness, Fairness and Transparency, according to which personal data shall be processed lawfully, fairly, in a transparent manner and in accordance with the requirements of the applicable laws and regulations
- The Principle of Purpose Limitation, according to which Personal Data are collected for specified, explicit and legitimate purposes and not further, processed in a manner that is incompatible with those purposes
- The Principle of Data Minimization according to which Personal Data shall be limited to what is necessary in relation to the purposes for which they are processed
- The Principle of Accuracy according to which, Personal Data shall be accurate and, where necessary, kept up to date
- The Storage Limitation Principle according to which, Personal Data shall be kept for no longer than is necessary for the purposes for which the personal data are processed and no longer
- The Accountability Principle according to which, the Personal Data Controller and the Personal Data Processor take responsibility for and comply with the other rights and principles of the applicable laws and regulations
- The Principle of Integrity and Confidentiality according to which, the appropriate security measures are in place to protect the personal data against unauthorized data processing as well as against any leakage or destruction
- The Principle of Transfer according to which the transfer of personal data to countries or regions outside the EEA is restricted, unless the specific country or region guarantees an adequate level of protection for your rights and freedoms in relation to the processing of their personal data

Lawful basis for processing Personal Data

The collection, processing and use of your Personal Data is conducted wherever necessary. Such a necessity arises when performing our contractual obligations with you, but also during compliance with our legal obligations, including, but not limited to, when applying anti-money laundering and terrorist financing principles and the tax legislation. Furthermore, we may need to collect and process specific categories of data for a legitimate purpose under the law. Such legitimate interests include, but are not limited to:

- Provision of audit / accounting / advisory services
- Business relations management
- Understanding and responding to our clients' needs
- Improvement of the provided services
- Safeguarding the operations of the company and its IT systems

- Compliance with applicable laws, regulations or professional body requirements in which the companies are members

Retention & Deletion of Personal Data

We keep personal data for as long as it is necessary to carry out the lawful purpose for which it was collected, unless the case falls under one of the exceptions described in the applicable laws and regulations. Data is subsequently erased or destructed within a reasonable period of time depending on the quantity, type and risk. It is understood that the company may retain personal data in the event of defending its legal interests in any court proceedings until it has been fully settled.

Individual Rights

It is imperative to know your rights including to the ones listed below:

- The Right to be Informed
- The Right to be Informed in relation to the purpose for which you provide your personal data and their subsequent use
- The Right to Access your personal data, following an access request
- The Right to Rectification in order to have inaccurate or incomplete personal data rectified, following a request, preferably to be made and submitted by email
- The Right to Erasure for your personal data that is no longer necessary for the purpose, which it was originally collected or processed for, following a request, preferably to be made and submitted by email
- The Right to Restrict Processing in order to suppress or limit the use of your personal data, but without erasing it, following a request, preferably to be made and submitted by email
- The Right to Data Portability in order to receive your personal data in a structured, commonly used and machine readable format for use in various services
- The Right to Object enabling you to stop processing of your data, if it is processed for direct marketing purposes or the Company carrying out a task in the public interest or its legal duty
- The Right to lodge a complaint with the competent supervisory authority, in case you consider that the processing of your personal data violates your rights (www.dataprotection.gov.cy).

Notification of personal data breach

In the case of a breach of your personal data, we will notify the competent supervisory authority, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to your rights and freedoms. At the same time, we will take all necessary steps to prevent and mitigate such breach. If, for any reason, it is not possible to notify the competent supervisory authority within 72 hours, we will adequately explain the reasons for such delay. In the event that the breach may result in a high risk for your rights and freedoms, we will communicate with you, orally or in writing, describing the nature of the breach and provide recommendations for mitigating any adverse consequences.

Sharing data with Third Parties

Your personal data may be shared with third parties and in particular, with:

- The staff of our companies in the course of providing the best possible service to you
- Trusted partners (accountants, auditors, IT consultants, software providers etc.)

- Law enforcement bodies and regulators and any other parties required in connection with legal proceedings
- Competent public and supervisory authorities
- Authorities for keeping public records
- Any other person on the basis of your definite instructions and written consent

Transfer of personal data outside the EEA

FRLTD forward your personal data to third country data processors or controllers, where and when this is deemed necessary, and provided, at the same time, that the conditions laid down by the applicable law apply.

Usage data

We may also collect information how the Service is accessed and used ("Usage Data"). This Usage Data may include information such as your computer's IP address, browser type, browser version, the pages you visit, the time and date of your visit, the browsing time, device identifiers and other diagnostic data.

Tracking & Cookies Data

We use cookies and similar tracking technologies to track the activity on our Service and hold certain information. Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyse our Service. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we use:

- Session Cookies: We use Session Cookies to operate our Service
- Preference Cookies: We use Preference Cookies to remember your preferences and various settings
- Security Cookies: We use Security Cookies for security purposes

Transfer Of Data

Your information, including Personal Data, may be transferred and maintained on computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside Cyprus and choose to provide information to us, please note that we transfer the data, including Personal Data, to Cyprus and process it there. Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

FRLTD will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Links To Other Sites

Our Service may contain links to other sites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the

Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

Minor's Privacy

Our Service does not address anyone under the age of 16 without parent or guardian consent ("Minors").

We do not knowingly collect personally identifiable information from anyone under the age of 16. If you are a parent or guardian and you are aware that your Minors have provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from minors without verification of parental consent, we take steps to remove that information from our servers.