Personal Data Processing in Freebike s.r.o.

LAST UPDATED: January 29, 2024

I. Document Purpose

Freebike s.r.o., a limited liability company, established and existing under the laws of the Czech Republic, having its registered seat at Křižíkova 237/36a, Karlín, 186 00 Prague 8, Identification No.: 27143503, registered in the Commercial Register maintained by the Municipal Court in Prague under registration number C 99560 ("**FREEBIKE**" or "company" "we", "us", "our") collects and processes personal data as a controller and in specific cases as a processor in the sense of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the „**GDPR**") and the Act No. 110/2019 Coll., on personal data processing, as amended.
The purpose of this document is to present and to inform the Data Subjects of what personal data FREEBIKE processes, for what purpose and what control measures are in place to protect them.

II. General Rules

1. FREEBIKE is processing personal data only where it is necessary for performance of the contract between us and the Client / Supplier, or where there is a legitimate interest of a controller which overrides the privacy interests of the data subject.
2. In cases when explicit consent of the data subject is required, such consent can be revoked at any time.
3. Personal data is processed only for such a period of time where there is a valid purpose for their processing, if the legal requirements do not override such period.
4. We will collect and process only such personal data that match the specified scope and purpose.
5. We will process only accurate and true personal data.
6. We have implemented appropriate technical and organizational security measures against personal data being accidentally or illegally destroyed, lost, changed or damaged, as well as against unauthorized access or misuse as required under Article 32 of the GDPR.

III. Controller and processors

For the purposes of the processing defined below in this document, the following persons are the personal data controller and processors:

personal data controller	FREEBIKE DPO: Ing. David Zahradnický e-mail: zahradnicky@pro-cert.cz phone number: +420721077806
processors involved in processing of personal data	KITE Systems s.r.o. Pekařská 695/10 155 00 Praha

In addition to the above listed third parties, FREEBIKE is entitled to share your personal data with the following entities:

- any competent authority or legal entity based on legal or regulatory requests, court orders, court or legal process, if necessary to comply with applicable laws;
- any acquirer, if the personal data is transferred in the course of the sale or other transfer of part or all of our assets to another company;
- providers of audit, insurance and legal and other advisory services and courts in the recovery of claims and/or defence of the interests of the controller.

IV. Electronic systems used for personal data processing

Personal data is stored and processed (even temporarily) in the following systems:

system	system supplier	Is a subprocessor
OnePass	Freebike s.r.o.	NO
Backend system TKHS	KITE Systems s.r.o.	YES
Payment gateways	PayU/Nets	YES

V. Scope and purpose of personal data processing

This chapter documents the specifics of personal data processing in FREEBIKE - what, why, who, where, how long.

1. Processing of personal data

Types of personal data processed by FREEBIKE, the purpose, legal basis and the way of processing.

i. Personal data processed pre-contract

- **Purpose of personal data processing:** Seeking new business partners, promotion of the company.
- **Scope of personal data processed:**
  - cookies data processed by the FREEBIKE website;
  - contact data of a potential clients' representatives: first name, surname, business e-mail, (business phone number), position in the company;
  - business correspondence with a potential clients' representatives.
- **Legal basis for personal data processing:** Legitimate interest of the controller pursuant to Article 6 (1) (f) GDPR verified by a balancing test (contact data of a potential clients' representatives, business correspondence) or explicit consent of the data subject pursuant to Article 6 (1) (a) GDPR (cookies).
- Data is stored in the following electronic system: MS Outlook
- Retention is limited by the duration of the business negotiations (contact data of a potential clients' representatives, business correspondence) or the data is being stored for the duration of your session (short-term cookies), but no longer then for the period of time you have set in your browser (long-term cookies).

ii. Business Contacts (general)

- **Purpose of personal data processing:** Fulfilling and realisation of contracts concluded with customers (provision of services, handling of defect incidents, processing payments for services, etc.)
- **Scope of personal data processed:**
  - data of clients' authorized personnel: first name, surname, business e-mail, business phone number, language preference, position in the company, the main area of responsibility towards FREEBIKE, business correspondence;
  - clients' accounting data.
- **Legal basis for personal data processing:** Performance of a contract pursuant to Article 6 (1) (b) GDPR.
- Data is stored in the following electronic system: MS Outlook

- Retention is limited by the duration of the contract with the business partner (public company data can be stored without any expiration), if the legal requirements do not override such period (accounting data is being stored for 10 years).

iii. Personal data required for claim handling

- **Purpose of personal data processing:** Handling of complaints or other claims, recovery of receivables and other contractual obligations under contracts concluded between us and our clients or other contractual partners.
- **Scope of personal data processed:**
    - data of clients' authorized personnel: first name, surname, business e-mail, business phone number, language preference, position in the company, the main area of responsibility towards FREEBIKE, business correspondence;
    - clients' accounting data.
- **Legal basis for personal data processing:** Legitimate interest of the controller pursuant to Article 6 (1) (f) GDPR verified by a balancing test.
- Data is maintained by the following department: IT department, Development & Business Development department, Accounting department
- Data is stored in the following electronic system: Internal information system, managed by Freebike administrator
- Retention is limited by the existence of the dispute (or a reasonable basis for its anticipation), however, we retain the data for no longer than the statutory limitation periods (generally, the statutory limitation period under the Czech law is 10 years).

iv. Personal data of job applicants

- **Purpose of personal data processing:** Assessment of the suitability of a job applicant during the selection procedure and re-contacting in the event of termination of employment with another selected candidate during the probationary period.
- **Scope of personal data processed:** first name, surname, e-mail, phone number, CV, correspondence.
- **Legal basis for personal data processing:** Legitimate interest of the controller pursuant to Article 6 (1) (f) GDPR verified by a balancing test or explicit consent of the data subject pursuant to 6 (1) (a) GDPR.
- Data is maintained by the following department: HR department, Accounting department
- Data is stored in the following electronic system: Internal storage system
- Retention is limited by the probationary period of the successful applicant for the respective position or by the validity of applicants' consent.

v. Personal data in connection with data subjects' requests handling

- **Purpose of personal data processing:** Handling of data subjects' requests under the GDPR.
- **Scope of personal data processed:** Any and all of the above listed types of data.
- **Legal basis for personal data processing:** Compliance with a legal obligation of the controller pursuant to Article 6 (1) (c) GDPR.
- Data is maintained by the following department: IT department, Development & Business Development department, Accounting department
- Data is stored in the following electronic system: Internal information system, managed by Freebike administrator
- Retention is limited by the time the request is being handled. If there is a reasonable basis for a dispute anticipation, we may store the data for longer on the legal basis of legitimate interest of the controller pursuant to Article 6 (1) (f) GDPR verified by a balancing test, but never for longer than the statutory limitation periods.

vi. Personal data of end users of the bicycles and applications

- **Purpose of personal data processing:** Fulfilling and realisation of DPAs concluded with customer (provision of services, service support, handling of defect incidents, etc.)

- **Scope of personal data processed:** Defined by the respective customer who is a controller of such personal data.
- **Legal basis for personal data processing:** DPA concluded under article 28 of GDPR.
- Data is maintained by the following department: IT department, Development & Business Development department, Accounting department
- Data is stored in the following electronic system: Internal information system, managed by Freebike administrator
- Data can be processed by the subprocessors named in article iii.
- Retention is limited by controller's instructions.

VI. Technical and Organisational Measures

1. Storage, processing and Security of Data

i. Personal data is recorded on the original paper forms like for example the hand-signed versions of the master service agreements and related documents.
   - These documents are stored in the FREEBIKE office premises. The access to the document is restricted using the common measures (controlled physical access to the building and to the office, locked storage containers, cupboards, etc.).

ii. Personal data is processed and stored via computer systems (see section IV)
   - Database and application servers are located in single purpose data centres with strictly limited physical access (locked racks, camera systems, access authorized only for pre-defined persons with personal ID card checks). The data centres are located in ČR and in the countries of EU.
   - Privileged system access is governed by the access management policy and is enabled only to the named administrators. The local and domain administrators are reviewed every year.
   - All servers processing personal data is protected by malware protection, the systems and data is regularly backed-up, regularly patched and scanned against the known vulnerabilities.
   - The databases of electronic systems used for personal data processing are encrypted, i.e. they are readable only for authorized users.
   - If the access from internet is granted, the communication channel is encrypted so that the data cannot be tapped and modified during the transfer.
   - All web systems accessible from internet are checked by independent penetration testing and they are regularly (yearly) tested for vulnerabilities.

iii. It is not possible to make unauthorized copies of personal data to mobile media like USB discs or CDs. Such media are enabled only for selected users and the content of the data written to such media is monitored and regularly checked. In case of authorized storage of data, the mobile media is secured by encryption. Storing any documents or data to web storage is restricted, also access to general web mail systems is restricted.

2. Access to personal data

i. Access to personal data in computer systems is possible only with the authorized user ID and password.

ii. All personal data is considered confidential and the access to them is governed by access management policy, i.e. the access is granted in accordance with the need-to- know principle to the roles and users that need such access in order to perform their work tasks.

iii. Users are regularly trained in the areas of information security and personal data protection.

3. Personal data Disposal

Once FREEBIKE stops collecting and processing personal data, or if the retention period is over for the specific data, FREEBIKE will dispose of the data by:

i. Shredding the paper documents;

ii. Deletion or anonymization of personal data in the databases;

iii. FREEBIKE will exclude the relevant data subjects from the further processing.

4. Security Measures

i. Risk Assessment

- Prior to the processing of any personal data a risk assessment has to be conducted to acquire insight in potential threats and security incidents, the risks and consequences thereof and the chance these risks and consequences materializes. A privacy impact assessment (PIA) or, if applicable, a data protection impact assessment (DPIA), is performed, which determines the risks related to the processing of personal data and the measures to address these risks.
- Risks have to be related to the reliability requirements. In general: the higher the risks, the higher the required level of availability, integrity and confidentiality.
- Relevant are the consequences for individuals in case of loss or unauthorized processing of their personal data. Any damages incurred are based on the nature of the personal data, the nature of the processing, the amount of processed personal data and the purposes for processing. Also relevant for the risk level are the state of the art and developments in society.

5. Policies, awareness and training

i. FREEBIKE has adopted this Privacy Policy and an Information Security Policy. In these policies all responsibilities, managerial as well as executive, are clearly defined and assigned.
ii. This FREEBIKE Privacy Policy exists for the protection and nondisclosure of personal data. It is implemented and communicated to all persons involved in the processing of personal data.
iii. Adequate non-disclosure agreements are in place with relevant parties.
iv. All employees, hired personnel and external users have an adequate security awareness, are properly trained and receive on a regular basis training courses to understand the privacy policy, the information security policy and security procedures of the company;

6. Security measures to be implemented for all categories of data

i. Compliance with relevant generally accepted security standards.
ii. IT services and IT equipment are physically protected against access by unauthorized persons, damages and disturbances. The provided level of protection is in line with predetermined risks.
iii. Access procedures only grant authorized users the access to IT systems and IT services and only in so far required for the performance of their duties. Usage rights are cancelled when access is no longer required. Access rights of persons with broad usage rights such as system operators are properly defined.
iv. Logging of all relevant events regarding personal data. Such events include attempts to acquire unauthorized access to personal data and any disturbances which could lead to changes in or loss of personal data.
v. Log files are periodically checked for any indications of unauthorized access or use. All actions required to stop such access or use are implemented.
vi. All applications contain security measures and verify that input, the internal processing and output meet requirements.
vii. All software, including browsers, virus scanners and operating systems, is kept up-to-date and solutions of software suppliers addressing security holes are rolled out timely.
viii. Regarding encryption, all usual precautionary measures have been implemented such as key management and usage of encryption keys in line with the actual state of the art techniques.
ix. Encryption is used if personal data is sent via the internet.
x. Only in exceptional cases (based on a risk analysis) no encryption has to be applied, e.g. in case the personal data exposed just concern the email-addresses of the sender and recipient of email.
xi. All data is (irreversible) removed from equipment with storage capabilities prior to removal or reuse of such equipment.

7. Information obligation

Data subjects are informed about processing of their personal data through this Privacy policy and, where applicable, in the respective agreements. Data subjects and supervisory authorities are informed about personal data security breaches without undue delay.

8. **Evaluation, assessment of security measures and follow-up**

i. FREEBIKE has to determine periodically that all security measures are implemented, complied with and adequate. In particular, this could mean the following:
   - Verification that security measures are complied with by the personnel.
   - Verification that security measures are implemented in and complied with in the IT systems.
   - Verification that outside working hours no sensitive personal data is available at the workplaces, in meeting rooms, near printers or copiers or in unclosed wastepaper bins.
   - Evaluation that the security levels are in line with the risks related to the processing of personal data and whether the security measures are still adequate or require adjustment in view of e.g. the state of the art and/or latest insights in information security. For software this could mean an inspection of the software (a code review). If the application is maintained by a third party the activities of such party are reviewed to determine for example how fast vulnerabilities or security leaks are solved.
   - Verification of new or changed IT systems that all specified security measures are in place and whether, e.g. via penetration tests, any unforeseen risks or week security spots exits.
   - Verification whether existing security measures are still adequate in case of material changes in the company or the IT systems.
   - Follow-up and take measures to address any issues found in respect of the above.
   - Periodic evaluation of security risks and determining whether measures have to be taken to adequately address these risks.
   - Lessons learned, e.g. from data security incidents, are used to structurally improve security.

9. Data processing by third parties

i. A risk analysis is conducted in respect of the processing by a third party.
ii. A DPA (data processing agreement) is concluded containing adequate arrangements in respect of the security measures to be taken, provided services, applicable reliability requirements, disclosure obligations regarding security and data security incidents, the use of subcontractors, the processing of personal data in countries lacking an adequate level of protection, etc.
iii. It is periodically verified that the DPA is complied with.
iv. Periodic evaluation and adjustment of the DPA.

VII. Automatic decision making/profiling

At the moment there is no automatic decision-making or profiling within FREEBIKE that would have legal (or other) effects for data subjects.

VIII. Your rights in relation to your personal data

1. Based on Articles 15 to 22 of the GDPR and other applicable regulations, data subjects have the following rights:

i. The right to access personal data.
ii. Right to rectification of personal data.
iii. The right to erasure of personal data where the respective legal basis of the processing allows it.
iv. In the cases provided for in Article 18 of the GDPR, the right for the controller to restrict the processing of specific personal data where the respective legal basis of the processing allows it.
v. The right to object to the processing of personal data. We will stop or restrict the processing of personal data on the basis of data subjects' objection where the respective legal basis of the processing allows it.

vi. Right to data portability to another controller - under the terms of Article 20 of the GDPR, including the right to receive from the controller all personal data processed in a commonly used and machine-readable format.
vii. Right to lodge a complaint with the Office for Personal Data Protection, pplk. Sochora 27, 170 00 Prague 7

2. Withdrawal of your consent(s)

i. If your consent is required for the processing of a particular category of personal data, as detailed in section IV.1, you may withdraw your consent(s) at any time without stating a reason.
ii. In such case, we will stop any further processing of the data associated with the respective consent.
iii. Withdrawal of a consent is generally possible via email sent to dpo@freebike.com or (cookies) via web browser settings or cookie banner on our website.

3. Exercising your rights

If you wish to exercise these rights and/or obtain the relevant information, please contact the DPO using the telephone number or email address provided in section III. We will respond to you without undue delay, but no later than within one month of receiving your request.

4. Transfer of personal data in case of change of ownership

FREEBIKE reserves the right to transfer personal data if we are to be involved in the merger, acquisition, winding up or sale of part or whole company. If such transfer requires notice or consent under applicable laws, data subjects will be informed, or their consent will be required.

5. Updating this Privacy Policy

In accordance with the GDPR principles, this Privacy Policy, as well as general organizational and technical measures for the protection of personal data and other internal mechanisms, are regularly updated. Any changes to this Privacy Policy will become effective upon their publication on our website. If we make changes that we consider to be essential and that require consent of data subjects to be granted in accordance with applicable law, we will inform you through the website and e-mail, where applicable, and, if necessary, request your consent.