

PRINCIPLES OF PROTECTION OF PERSONAL DATA

We have created these Principles of protection of personal data (Privacy policy) in order to inform you about how we collect, process, use and protect personal data while operating e-shop services at <https://shishaoriginal.com/>. In the matter of protecting your privacy and personal data we strictly adhere to applicable legislation, i.e. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as „the Regulation“) and other applicable legislation.

1. Who is the controller of personal data and what are the categories of subjects of personal data, whose personal data we process?

Controller of personal data:

- company SHISHA ORIGINAL s.r.o., ID no. 05223041, registered seat at Plotní 688/75, Komárov, Brno, ZIP code 602 00, registered at the Commercial register by Regional Court of Brno, file number C 104448.

Categories of data subjects:

- controller's customers or potential customers, i.e. persons who concluded a contract of sale of services or goods with the controller via the website <https://shishaoriginal.com/> or persons who contacted the controller with an intention to do so.
- controller's employees,
- service providers and persons acting for the benefit of the controller under another contractual relationship.

2. Which personal data of data subjects do we process?

The controller processes these data of his customers: name, surname, date of birth, address of permanent residence; in the case that the customer is a natural person doing business according to special legal regulations, we will also process his/her registration number and VAT number. Furthermore, in order to communicate with the customer when delivering goods, we process his contact details, such as telephone number and email address, when processing the order. For payment purposes, we may also process the customer's bank account number.

Concerning other data subjects (employees, service providers), we process these personal data: identification data – personal data that can be used to identify data subject, i.e. name, surname, title, date of birth, address of permanent residence; of suppliers – natural persons doing business we also collect his/her registration number and VAT number. Furthermore, we process contact information – personal data that enable us to contact data subject in order to fulfill contractual obligations (contact address, email address, phone number, eventually payment data – IBAN).

Any other personal data (besides those listed above) we may process data with the consent of the data subject for the purposes of, for example, marketing.

3. What are the sources of personal data that we obtain?

We obtain personal data directly from the data subject, in the relation to concluding a contract or for the provision of services or goods through the <https://shishaoriginal.com/> website and also during negotiations on the conclusion of another contractual relationship (with the employee, when entering into a contract with the supplier, etc.) or from third parties in accordance with the Regulation, especially from public sources, while respecting the purpose of processing personal data.

4. How and for how long do we process personal data?

We process the personal data of the controller's customers in an automated way in electronic information systems where the personal data of the data subjects are recorded and stored only in the information system from the beginning. However, there is no automated decision making (i.e. nonhuman involvement), including profiling, when processing personal data. Personal data is protected at all times against unauthorized interference, loss, destruction or misuse. All persons who come into contact with the data are bound by the obligation of confidentiality, especially our employees and processors. Personal data belonging to other than the controller's customers are also handled manually while adhering to the above stated principles.

In case of storing personal data for the purpose of negotiating a contract we store the data for the time necessary to conclude such a contract but no longer than 2 months and in case of a concluded contract we store personal

data for the duration of the contractual relationship and for the time necessary to guarantee all the rights and obligations arising from the contractual relationship, i.e. for the duration of the possible claims arising from the concluded contract (statutory limitation period) and for the period we are bound to in accordance with generally binding legal regulation.

5. Based on what legal title and for what purpose do we process personal data?

Customers' personal data are processed for the purpose of performance of a contract of sale of goods or services according to article 6 paragraph 1 letter b) of the Regulation.

In the context of negotiations on the conclusion of contracts or the performance of contracts with other data subjects (employees, suppliers), personal data are processed in accordance with article 6 paragraph 1 letter b) of the Regulation, i.e. for the purpose of fulfilling such a contract.

Personal data may be also processed in order to protect the legitimate interests of the controller in accordance with article 6 paragraph 1 letter f) of the Regulation, in particular the recovery of any claims arising from contracts entered into with the data subject. In addition, the personal data of data subjects may be processed to use direct marketing (i.e. to send product offers, new product information), subject to the data subject's consent under article 6 paragraph 1 letter a) of the Regulation.

The data subject has the right to object to the controller in accordance with article 21 of the Regulation in the case of the processing of personal data in order to protect the legitimate interests of the controller pursuant to article 6 paragraph 1) letter f) of the Regulation. In the case of this objection, the controller shall not process personal data further unless he demonstrates serious legitimate reasons for processing that prevail over the interests or rights and freedoms of the data subject or for the determination, exercise or defense of legal claims.

Where the right to process personal data is based on the granting of consent, such consent may be revoked by the data subject at any time; e. g. in the case of consent given to marketing purposes. However, the withdrawal of this

consent is without prejudice to the lawfulness of processing based on consent prior to its withdrawal.

Personal data are also processed by the controller for the purpose of fulfilling legal obligations in accordance with article 6 paragraph 1) letter c) of the Regulation, such as state bodies (e. g. tax administrators for tax administration, courts, bailiffs, notaries), to fulfill statutory obligations under special legal regulations

6. What are the statutory rights of the data subject regarding personal data processing?

Right to access personal data:

The data subject has the right to obtain a confirmation from the controller that he is processing his or her personal data and, if so, the data subject has the right to access such personal data and the information specified in article 15 of the Regulation.

The right of rectification, erasing and restriction of processing:

The data subject has the right (in the cases specified by the Regulation) to ask the controller to correct or complete incorrect or incomplete personal data, to request erasure of personal data, if there is or is no reason to process it, and to request a restriction of the processing of personal data in connection with the handling of the processing of personal data by the controller.

The right to object:

The data subject has the right, in connection with his or her particular status, at any time, to raise an objection with the controller, as to the processing of personal data processed for the purpose of protecting the legitimate interests of the controller or other persons (pursuant to the Regulation); the legitimate interests under the Regulation may in particular refer to cases of protection of rights of the controller and enforcement of legal claims of the controller.

The right to data portability:

The data subject has the right (under the conditions set out in the Regulation) to obtain his or her personal data from the controller and pass it on to another data controller.

The right to lodge a complaint with a supervisory authority:

The data subject has the right to lodge a complaint with the supervisory authority if he or she suspects that the processing of his or her personal data has violated the Regulation. The supervisory authority is the Czech Office for Personal Data Protection.

Where the right to process personal data is based on the granting of consent, such consent may be revoked by the data subject at any time; e. g. in the case of consent given to marketing purposes. However, the withdrawal of this consent is without prejudice to the lawfulness of processing based on consent prior to its withdrawal.

To exercise all of his or her rights, the data subject may use the contact details listed in paragraph 7 of these Principles below. The controller informs the data subject about the processing of his or her application and the measures taken without delay (the Regulation gives the controller a period of 1 month from receipt of the request). A more detailed description of the data subject's rights is freely available on our website <https://shishaoriginal.com/pricipiles-of-protection.html>

7. Where can the data subject exercise his / her rights or lodge any objections to the processing of personal data?

In order to object to the processing of personal data, to revoke the consent or to change its scope, or to exercise any of their rights, the data subject may use any of the following ways:

- send a letter to address at Plotní 688/75, Komárov, Brno, ZIP code 602 00
- pcall us on number: +420 777 070 838
- send an email to: hello@shishaoriginal.com
-

8. To whom do we provide personal data?

Personal data is processed by controller's employees or by controller's processors under a contract concluded in accordance to article 28 of the Regulation. In all cases, however, the processor keeps all the obligations that the controller and its employees derive from the applicable legislation and when transmitting the data, the controller ensures that the personal data may not be compromised or misused.

The processors or receivers of personal data are especially but not exclusively:

- State authorities and other institutions within the scope of their authority, in particular public authorities, courts, tax administrators, law enforcement authorities, social security authorities, bailiffs, notaries, Czech insurance association, insurance companies;
- a company managing the information systems of the controller and a company providing IT services to the controller;
- third parties, based on a consent obtained prior to data transfer or according to direct order of the data subject.

9. Under what conditions do we transfer personal data to third countries?

Personal data are never transferred to third countries or to any international organization.

10. Do we process personal data by automated means or do we do profiling?

While processing personal data, no automated decision making is involved (e.g. data are not processed without human supervision), that includes no- use of profiling.

11. What does the terms used in these Principles mean?

- Data subject – natural person, whose personal data are processed by a controller;
- Controller – a subject who determines the purposes and means of the processing of personal data and bears responsibility for it – e. i. comp. SHISHA ORIGINAL s.r.o.
- Processor – a subject who in accordance to authority given by law or in accordance to a contract concluded with a controller processes personal data;
- Receiver – a subject to whom personal data are made available to;
- Processing of personal data – any action or sequence of actions that the controller or processor systematically or otherwise carries out with personal data by automated or other means; such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.