

PERSONAL DATA PROCESSING AGREEMENT
ANNEX 1 TO THE SMARTSUPP TERMS OF SERVICE

(hereinafter referred to as the "**Processing Agreement**") concluded between:

A. You, who have chosen to use Smartsupp;
("Controller" or "you")

and

B. Smartsupp.com, s.r.o., ID No.: 036 68 681, with its registered office at Šumavská 31, 602 00 Brno, represented by Vladimír Šandera, Managing Director, registered in the Commercial Register maintained by the Regional Court in Brno, file No. C 86206 , (hereinafter referred to as "**Processor**" or "**we**")

(The Processor and the Controller are hereinafter collectively referred to as the "**Parties**" and individually as a "**Party**").

If you use the Smartsupp service (the "**Service**"), then Smartsupp will be the processor of the personal data you entrust to it. The Service is provided subject to the Smartsupp [Terms of Service](#) ("**Terms**"). By agreeing to the Terms and entering into an agreement between us, you confirm that you have read and agree to the Processing Agreement and it is legally binding on you. This Processing Agreement applies to all users who access or use the Service.

Please read this Processing Agreement carefully, as it sets out the terms and conditions of the processing of personal data under which the Service is provided.

You may contact us at any time at dpo@smartsupp.com if you have any questions regarding the processing of personal data. You can also contact our Data Protection Officer, Mgr. Petra Stupková.

The Parties shall process personal data in connection with the contract concluded pursuant to the Terms in accordance with the law, in particular in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter referred to as "**GDPR**"). Under the GDPR, the Parties must regulate the processing rules in writing, which they do in this Processing Agreement.

1. INTRODUCTION AND BRIEF OVERVIEW OF THE TERMS AND CONDITIONS

- 1.1. **Summary.** If you want to use the Service and complete the registration, we automatically obtain personal data from you, which we process for you as a Processor. We maintain confidentiality and ensure the security of personal data.
- 1.2. **Subject and purpose of the Processing Agreement.** By entering into this Processing Agreement, you, as the Controller, authorise the Processor to process personal data for you in connection with the performance of the Service. The aim is to ensure the protection of personal data to the extent required by law. A more detailed description of the nature, scope, purpose and duration of the processing of Personal Data is set out in **Annex A** of this Processing Agreement.

- 1.3. **Smartsupp Service.** The primary functionality of the service is to provide real-time communication with your website visitors. The Smartsupp service is further defined in the [Terms](#).
- 1.4. **What the position of processor and controller means.** When using the Service, you, as a Controller, transmit personal data to Smartsupp, which then processes it as a Processor on your instructions and to the extent you choose. Therefore, you are in the position of a Data Controller for the processing pursuant to Article 4(7) GDPR, while Smartsupp is in the position of a Processor pursuant to Article 4(8) GDPR.
- 1.5. **Written form.** Pursuant to Article 28 of the GDPR, the Parties must set out the processing rules in writing, which is done in this Processing Agreement.
- 1.6. **Definitions.** The definitions of terms in the Terms shall be adopted in the same sense in this Processing Agreement.
- 1.7. **Duration of the Contract.** This Processing Contract is concluded for the duration of the provision of the Service in accordance with the Terms.
- 1.8. **The time of conclusion and termination of the Processing Agreement.** The Processing Agreement is concluded at the moment of completion of registration for the purpose of using the Service. Termination of the Processing Agreement is possible under the same conditions as in the case of termination of the contract as described in the Terms.
- 1.9. **Effects of termination.** Termination of this Processing Agreement shall also result in the termination of the contractual relationship in the areas covered by this Processing Agreement, unless the Parties agree otherwise. The termination of the contractual relationship governed by the Terms shall also terminate this Processing Agreement. However, the termination of this Processing Agreement shall not affect the obligations of the Processor to transfer (return) Personal Data to the Controller or to dispose of the Personal Data and to maintain the confidentiality of the information.

2. JOINT OBLIGATIONS OF THE CONTROLLER AND THE PROCESSOR

- 2.1. **Lawfulness of processing.** The Controller and the Processor undertake to comply with the regulations governing the protection of personal data, including related regulations (for example, Act No. 127/2005 Coll., on electronic communications governing the processing of cookies and other tracking technologies).
- 2.2. **Special Categories of Personal Data.** The Controller undertakes not to disclose any Personal Data that falls within a Special Category of Personal Data within the meaning of Article 9 of the GDPR without the prior written consent of the Processor. Special Categories of Personal Data may only be processed with the express agreement of the Processor. The Controller undertakes not to use the Service primarily in a way that would require or encourage visitors (Data Subjects) to fill in such Personal Data.
- 2.3. **Cooperation.** The Controller and the Processor undertake to assist each other to the extent necessary and reasonable in the performance of their obligations in the

processing of personal data arising from their respective contracts and legal provisions, in particular in connection with responses to the exercise of data subjects' rights, security incidents, as well as the preparation of impact assessments and dealings with supervisory authorities. The Parties undertake to provide the necessary supporting documents for the processing of a request under the Terms to the other Party without undue delay.

- 2.4. **Incident.** A Party shall notify the other Party that it has become aware of a security breach within 48 hours of becoming aware of the security breach. Breach means any breach of security of Personal Data that has the potential to result in the accidental or unlawful destruction, alteration, or unauthorized disclosure or access to Personal Data that is processed under a contract as set out in the Terms.

3. RIGHTS AND OBLIGATIONS OF THE PROCESSOR

- 3.1. **Access Restrictions.** The Processor shall ensure that access to Personal Data is limited to (a) employees who process Personal Data as part of their job description and (b) persons who cooperate with the Processor and may process Personal Data for the Processor as part of that cooperation, in accordance with the terms of this Processing Agreement and for the purpose of providing the Services under the Terms. If these persons are not subject to a legal obligation of confidentiality, the Processor shall ensure their contractual confidentiality.
- 3.2. **Confidentiality of the Processor.** The Processor undertakes to observe the obligation of confidentiality of all personal data transmitted by the Controller and will keep them secret, not disclose them, not make them available to third parties, neither as a whole nor in parts, unless they are to be transmitted on the basis of the Controller's instructions or if so provided by law.
- 3.3. **The commitment of the Processor regarding the measures taken.** The Processor has adopted and undertakes to maintain throughout the duration of this Processing Agreement appropriate technical and organizational measures in accordance with the GDPR Regulation applicable to the Processor. The other processors (sub-processors) under contract with the Processor undertake to comply with the same data protection obligations as set out in the Processing Agreement, in particular, to provide sufficient safeguards to ensure that the processing complies with the requirements under the GDPR. An overview of the measures taken can be found in **Annex C** of this Processing Agreement.
- 3.4. **The processor undertakes:**
- 3.4.1. to comply with all obligations arising for the Data Processor from the relevant legislation when processing Personal Data;
 - 3.4.2. to process Personal Data solely on the basis of the Controller's instructions made pursuant to this Processing Agreement, including in relation to the transfer of Personal Data to a third country or an international organization;
 - 3.4.3. to notify the Controller without undue delay in cases where an inspection or other administrative proceedings are initiated by the Agency for Personal Data Protection or another administrative authority in relation to the processing of Personal Data by the Processor, and to provide the Controller

with all information about the course and results of such inspection or the course and results of such proceedings;

- 3.4.4. to assist the Controller in ensuring compliance with the Controller's personal data security obligations under Articles 32 to 36 GDPR, taking into account the nature of the processing to be carried out by the Processor;
 - 3.4.5. to notify the Controller of any Personal Data breach of which it becomes aware without undue delay, and no later than 48 hours after becoming aware of the breach. The minimum scope of such notification is set out in Article 33(3) of the GDPR;
 - 3.4.6. to keep a record of all Personal Data breaches and the corrective measures taken to ensure an adequate level of security of processing. The Processor is obliged to provide the Controller with all necessary cooperation related to the investigation of the breach and the fulfillment of the Controller's obligations under Articles 33 to 34 of the GDPR;
 - 3.4.7. assist the Controller in documenting processes or documents that demonstrate the Controller's compliance with the GDPR.
- 3.5. **Reimbursement.** The parties agree that the Processor shall be entitled to reimbursement from the Controller for its reasonable costs associated with providing assistance.
- 3.6. **Trade secrets.** All information and documents disclosed by the Processor to the Controller in connection with an audit or inspection, form a part of the Processor's trade secrets and, unless otherwise specified, shall be subject to the confidentiality requirements of this Processing Agreement. Such information and documents may only be disclosed to an authorized supervisory authority.
- 3.7. **Lawfulness of processing.** The obligations of the Processor regarding the protection of Personal Data shall be fulfilled by the Processor for the entire term of the agreement as amended by the Terms unless it is clear from the Terms, this Processing Agreement, or applicable law that they are to continue after the termination of the agreement.
- 3.8. **Notification of the involvement of a new processor.** If the Processor will be engaging processors other than those listed in **Annex B** of this Processing Agreement, the Processor shall notify the Controller prior to such change. In the event that the Controller does not agree to the engagement of a new Processor, the Administrator may file an objection no later than five (5) days after receipt of the Processor's notice. The filing of an objection, and thus the failure to involve the new (sub)processor, may result in the prevention of using the Service.
- 3.9. **Obligation of the Processor in case of termination of cooperation.** The Processor undertakes to delete all Personal Data in the event of termination of the provision of the Services and to the Controller's request unless EU or Czech law requires their storage. In this case, they will be returned within five months of the receipt of the Administrator's request via a secure storage facility, which the Controller will specify in its request and provide the Processor with access to. If, after three years from the end of the cooperation, the Controller has not instructed the personal

data to be transferred, the Processor shall notify the Processor of the possibility of returning the data. If the Data Controller does not instruct the Data Controller to transfer the data within one month of the notification, the Personal Data shall be deleted with a view to fulfilling its legal obligations.

4. FINAL PROVISIONS

- 4.1. **Legal order.** For matters not specifically covered by this Processing Agreement, generally binding legal regulations shall apply. The Processing Contract shall be governed by and interpreted in accordance with the laws of the Czech Republic, in particular Act No. 89/2012 Coll., the Civil Code, as amended. The Parties agree that commercial custom shall not prevail over any provisions of law, even those that are not coercive.
- 4.2. **Force majeure.** The Processor shall not be liable for situations in which it is unable to fulfill its obligation under the Processing Agreement due to an event referred to as force majeure (war, riots, terrorism, riots, strikes, fires, epidemics or natural disasters).
- 4.3. **Communication between the Parties.** The Parties agree that their communications regarding the Processing Agreement (including notification of a Security Incident) will be conducted via email addresses:
 - 4.3.1. Controller: the email address used by the Controller to register for the Service;
 - 4.3.2. Processor: dpo@smartsupp.com.
- 4.4. **Prohibition of assignment.** Neither Party may assign or transfer in any manner the rights and obligations under or related to this Processing Agreement without the prior written consent of the other Party.
- 4.5. **Updates and changes.** The Processor reserves the right to modify or update this Processing Agreement. If we make changes that alter the rights and obligations under the Processing Agreement, you will be notified in a timely manner via an email, that we will send to you. If you do not agree to the modifications, please stop using the Service. By using the Service after the new version of the Processing Agreement becomes effective, you agree to be bound by its terms. The current version of the Processing Agreement can be found [here](#).
- 4.6. **Annexes to the Processing Agreement.** The following annexes form an integral part of this Processing Agreement:
 - Annex A: Nature, scope, duration, and purpose of the processing of Personal Data**
 - Annex B: List of processors**
 - Annex C: Technical and organizational measures**

ANNEX A OF THE PROCESSING AGREEMENT

NATURE, SCOPE, DURATION, AND PURPOSE OF THE PROCESSING OF PERSONAL DATA

1. **Nature of processing.** Personal data is processed automatically by means of the Processor's script, which the Controller inserts on its website. This script loads the Chat box on the Controller's website where the script is embedded. The Chat box is part of the primary Service. Visitors to the Controller's website can fill in their personal data in the Chat box in order to contact the Controller's customer support. Other Personal data may be processed in the background by the script itself. The Controller may import additional personal data for processing through the Processor's application programming interface (API) or through integrations with third-party services as part of the primary Service.
2. **Processing title.** The legal basis for processing Personal data in the context of providing the Service is the performance of the contract (Terms).
3. **Scope of processing.** Depending on how the Controller uses the Primary Service, the following types of personal data may be processed in connection with the provision of the Primary Service:
4. **Contact details:**
 - Name, surname, email address, phone number, or social network account contact.
5. **Details about visiting your website:**
 - URL of the website visited, date and time of the website visit, technical information (screen resolution, device type, browser type, operating system, etc.), IP address, geolocation data (country and city from which the user viewed your website).
6. **Special categories of personal data.** This is Personal data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, or sexual orientation. Genetic and biometric data are also considered to be a special category of data when they are processed for the purpose of uniquely identifying a natural person.
7. **Data subject.** As a rule, it is personal data of the Controller's customers, users of the Controller's website, business partners and their employees or representatives or it may be employees of the Controller.
8. **Processing time.** Personal Data is processed for the period of time that the Parties are bound by the Terms, unless another contract or legal regulation provides for a longer period (including, for example, a period for the deletion of data after the end of the contract or confidentiality).
9. **Purpose.** The purpose of the processing is to enable the Controller to:
 - 9.1. provide and improve customer support for visitors to its website;
 - 9.2. get feedback from visitors about its products and services;
 - 9.3. improve the user experience on its website.
10. **Tools to limit processing.** As part of the primary Service, the Processor offers the Controller the following tools to restrict the processing of personal data and improve the privacy of data subjects. All tools are described in more detail at www.smartsupp.com.

11. **Chat box notifications.** The Processor displays a notification of the processing of personal data for visitors to the Controller's website within the Chat Box and allows the Controller to link this notification to its website, where the Controller defines how it processes visitors' personal data within the primary Service.
12. **Setting the processing time.** The Processor allows the Controller to set the retention period for Personal Data within the primary Service. The Controller can set the period in his Smartsupp account by logging into www.smartsupp.com -> section Settings.
13. **IP address tracking.** The Controller can deactivate the tracking of IP addresses of its visitors. This can be set in the Smartsupp account by logging in to www.smartsupp.com -> section Settings. By default, IP address tracking is disabled in the primary service.

ANNEX B OF THE PROCESSING AGREEMENT

LIST OF PROCESSORS

Other processors. We will not disclose the personal data we obtain under the Processing Agreement to any third party. The exceptions are the processors listed below, with whose engagement the Controller agrees:

- [Amazon Web Services \(AWS\)](#) - Used to provide the data infrastructure for the operation of the Service. Data may be processed in accordance with Section 2 of the Processing Agreement. Data is stored in the EU, specifically in a German data center.
- [Mailgun](#) - Used for the delivery of email messages, which is necessary for the operation of the Service. Email addresses, first and last names, and message content are processed. Data is stored in the EU.
- [OpenAI Ireland Ltd. \(ChatGPT\)](#) - Used to implement artificial intelligence (AI) in the chatbot and other Processor's functions that can use AI. The user will always be alerted to the AI involvement before it is started. The data could be stored outside of the EU, in that case, the level of protection according to the GDPR is maintained through Standard Contractual Clauses (adopted by the EU Commission on June 4, 2021) or an adequacy decision issued by the European Commission under Article 45 GDPR.

ANNEX C OF THE PROCESSING AGREEMENT

TECHNICAL AND ORGANIZATIONAL MEASURES

Technical and organizational measures. Security is very important to us and we are constantly working to ensure that your data is protected. When choosing measures, we take into account the scope of processing, the risks of the processing or the state of our technology.

- We back up data regularly;
- we update antivirus software systems;
- we encrypt data using SSL/TLS ("secure sockets layer / transport layer security") for all data transmission;
- we use secure https protocol;
- our data, including Personal Data on servers, is encrypted;
- access passwords to information systems where Personal data will be processed and access permissions are controlled at the individual level.

Organizational arrangements. We have adopted and commit to maintain the following measures:

- Our employees are bound by confidentiality;
- our employees are properly trained and also regularly trained on GDPR and familiarized with the rules of safe work on work equipment;
- access to all systems, including the information system, is personalized and covered by secure passwords;
- we have appointed a Data Protection Officer, Mgr. Petra Stupková, who can be contacted at dpo@smartsupp.com;
- the information system records logs so that we can control employee access to individual User Personal Data.

AWS. The processor uses Amazon Web Services servers and cloud infrastructure to store personal data. You can learn more about the security of this service at this link: <https://aws.amazon.com/compliance/eu-data-protection/>

- [Amazon Web Services security information](#)
- [About physical security of Amazon Web Services data centers](#)
- [Information about Amazon Web Services' compliance with the GDPR](#)