Data Processing Agreement (DPA)

ALTCHA Cloud Service

Parties

This Data Processing Agreement ("Agreement") is entered into between:
(1) Customer (Data Controller):

Name: _____
Address: _____

(2) Vendor (Data Processor):
Name: BAU Software s.r.o.
Address: Lidická 700/19, 602 00, Brno, Czechia

Together referred to as the "Parties".

1. Purpose of the Agreement

This Agreement governs the processing of personal data by the Vendor on behalf of the Customer in connection with the Vendor's cloud-based protection service (the "Service").

The Customer uses the Service on or in connection with its websites, applications, or other digital services. The Service may process information submitted by or relating to individuals interacting with the Customer's websites or applications in order to provide website protection, anti-abuse, anti-spam, security, or related functionality.

The Parties intend this Agreement to satisfy the requirements of Article 28 of the General Data Protection Regulation (EU) 2016/679 (GDPR), to the extent applicable.

2. Role of the Parties

- The Customer acts as the Data Controller for personal data processed through the Service on the Customer's behalf.
- The Vendor acts as the Data Processor and processes personal data only on the Customer's documented instructions, subject to the terms of this Agreement and the applicable service agreement.
- The Customer remains responsible for determining the purposes and means of processing and for ensuring that its use of the Service has an appropriate legal basis and complies with applicable data protection laws.
- The Vendor will not process personal data for its own independent purposes, except where processing is required by applicable law or is necessary to secure, maintain, and operate the Service as described in this Agreement.

3. Scope and Nature of Processing

The Service is designed to provide protection functionality while minimizing the processing and retention of end-user data.

Depending on the Customer's configuration and use of the Service, the Vendor may process:

- Data submitted to the Service as part of a protection or verification request
- Technical information necessary to receive, process, secure, and respond to requests
- Information necessary to detect abuse, attacks, fraud, or attempts to compromise the Service
- Limited technical logs and operational data where necessary to maintain security, availability, reliability, and performance
- The categories of data subjects may include individuals interacting with the Customer's websites or applications, including website visitors, users, customers, and other individuals whose information is submitted to the Service.

The categories of personal data processed may include identifiers, online identifiers, technical information, IP addresses, device or browser information, request metadata, and other information contained in or associated with a request, to the extent such data is transmitted to the Service by or on behalf of the Customer.

4. Processing Instructions and Limited Purposes

The Vendor shall process personal data only for the following purposes:

- Providing the Service and its protection functionality
- Receiving, processing, and responding to requests submitted to the Service
- Maintaining the security, availability, integrity, and reliability of the Service
- Detecting and preventing fraud, abuse, malicious activity, and attacks
- Troubleshooting and providing technical support where necessary
- Complying with applicable legal obligations

The Vendor shall not sell Customer Data or use End-User Data for advertising, behavioral advertising, cross-site tracking, or profiling unrelated to providing, securing, and operating the Service.

5. Data Retention and Deletion

The Service is designed to process End-User Data only for as long as necessary to provide the requested protection functionality. The Vendor does not intentionally retain the contents of requests after processing is complete where retention is not necessary for the operation of the Service.

Limited technical information may be temporarily processed or retained where necessary for security, abuse prevention, troubleshooting, service reliability, or other legitimate operational purposes.

Upon termination of the Customer's use of the Service, the Vendor shall delete or return Customer Data processed on behalf of the Customer within a reasonable period, unless continued retention is required by applicable law or is necessary for the establishment, exercise, or defense of legal claims.

6. Security of Processing

The Vendor shall implement appropriate technical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access.

- Encryption of data in transit and, where appropriate, at rest
- Access controls and authentication mechanisms
- Measures designed to maintain the confidentiality, integrity, availability, and resilience of processing systems
- Security monitoring and measures designed to detect and prevent unauthorized or malicious activity
- Processes for regularly testing, assessing, and evaluating the effectiveness of security measures
- Confidentiality obligations applicable to personnel authorized to process personal data

7. Location of Processing and International Transfers

For the Cloud Service, End-User Data processed on behalf of the Customer is hosted and processed exclusively within the European Union. The Vendor shall not transfer End-User Data outside the European Union for hosting or processing.

The Vendor may use service providers for infrastructure, security, monitoring, support, or other operational functions. The Vendor shall ensure that any such provider that processes Customer Data is subject to appropriate data protection obligations and safeguards.

Customer account, billing, and other commercial data may be processed separately from End-User Data and may be processed outside the European Union where necessary to provide the relevant services. Any transfer of personal data outside the European Economic Area shall be carried out in accordance with applicable data protection law and using an appropriate legal transfer mechanism where required.

8. Subprocessors

The Customer generally authorizes the Vendor to engage subprocessors for the provision of hosting, infrastructure, security, monitoring, communications, and other services necessary to operate the Service.

The Vendor shall impose data protection obligations on subprocessors that are no less protective than the obligations applicable to the Vendor under this Agreement, to the extent required by applicable law.

The Vendor remains responsible for the performance of its subprocessors to the extent required by applicable law.

The Vendor shall maintain information about relevant subprocessors and provide the Customer with reasonable information about material changes to subprocessors where required by applicable law.

9. Assistance to the Customer

Taking into account the nature of processing and the information available to the Vendor, the Vendor shall provide reasonable assistance to the Customer in fulfilling its obligations under applicable data protection law, including where reasonably necessary in relation to:

- Data subject requests
- Security of processing
- Personal data breach notifications
- Data protection impact assessments
- Consultation with supervisory authorities

The Customer shall provide the Vendor with reasonable cooperation and information necessary for the Vendor to provide such assistance.

10. Personal Data Breaches

The Vendor shall notify the Customer without undue delay after becoming aware of a personal data breach affecting personal data processed on behalf of the Customer, where required by applicable law.

The Vendor shall provide the Customer with information reasonably available to it concerning the nature of the breach, the categories of data and data subjects affected where known, and measures taken or proposed to address the breach.

11. Audits and Compliance Information

The Vendor shall make available to the Customer information reasonably necessary to demonstrate compliance with the obligations applicable to processors under Article 28 GDPR.

12. Customer Responsibilities

The Customer is responsible for:

- Determining the purposes and means of processing personal data
- Establishing an appropriate legal basis for processing
- Providing any required privacy notices to data subjects
- Ensuring that the Customer's instructions to the Vendor comply with applicable law
- Configuring and using the Service in accordance with applicable laws and the relevant service documentation

- Ensuring that the data submitted to the Service is appropriate and necessary for the intended purpose

13. Term and Termination

This Agreement remains in effect for as long as the Vendor processes personal data on behalf of the Customer.

Upon termination of the Customer's use of the Service, the Vendor shall handle Customer Data in accordance with Section 5 of this Agreement.

14. Liability

The Parties' liability in connection with the processing of personal data shall be governed by applicable law and the applicable commercial agreement between the Parties.

Nothing in this Agreement excludes or limits liability to the extent such exclusion or limitation is prohibited by applicable law.

15. Entire Agreement

This Agreement forms part of the main commercial agreement between the Parties and governs the processing of personal data by the Vendor on behalf of the Customer in connection with the Cloud Service.

In the event of a conflict between this Agreement and another agreement between the Parties concerning the processing of personal data, this Agreement shall prevail to the extent of the conflict, unless the Parties expressly agree otherwise in writing.

Signatures

Vendor	Customer
_____	_____
Name:	Name:
Title:	Title:
Date:	Date: