Data Processing Agreement (DPA)

BLUUR-Ver.1.3 / English / 18.12.2025

Introduction

This Agreement concerns the "Bluur" service (hereinafter referred to as the "Service"), made available online at https://app.bluur.ai/.

The Parties agree that this Data Processing Agreement (the "Agreement") sets out their obligations concerning the processing and security of data and personal data on behalf of the Controller, in order to process data in compliance with 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 (hereinafter: the "GDPR").

The Agreement forms an integral part of the Terms and Conditions of the Service. Furthermore, the Parties agree that, unless a separate agreement has been concluded, this Agreement governs matters concerning data processing and security.

The Agreement sets out the rules for the operation and use of the Service administered by BTC Spółka z ograniczoną odpowiedzialnością (hereinafter referred to as the "Processor" or "BTC"), with its registered office in Szczecin, Ul. 1 Maja 38, 71-617 Szczecin, entered in the Krajowy Rejestr Sądowy under number 00000129373.

This Agreement is concluded electronically as a result of the Controller accepting its contents during the Service purchase process and enters into force upon such acceptance.

Update restrictions

When the Customer purchases a new Subscription or renews an existing Subscription, the provisions of the Data Processing Agreement (DPA) then in force shall apply and shall not change during the Subscription term.

New features, add-ons or related software

Notwithstanding the update provisions set out above, if new features, add-ons or related software (that were not previously part of the Service) are introduced, BTC may introduce new provisions or update existing provisions of the Agreement that apply to the Customer´s use of those new features, add-ons or related software.
If such provisions materially and adversely amend the Agreement, BTC shall give the Customer a choice regarding the use of the new features, add-ons or related software without losing existing functionality. If the Customer does not install or use the new features, add-ons or related software, the relevant new provisions shall not apply.

Electronic notices

BTC may provide the Customer with information and notices concerning the Service electronically, including by e-mail, through the Service portal or on the designated website. A notice shall be deemed delivered on the date on which BTC makes it available.

Previous versions

These Agreement Terms contain provisions concerning the Service available at a given time. Previous versions of the Agreement can be found at https://bluur.ai/data-protection-addendum-dpa.

Definitions

The following defined terms are used in this Agreement:

- Controller (Customer) - the entity that creates an Account and purchases a Subscription to the Service;
- Account - a physically and/or logically separate instance intended exclusively for a single business entity, in which data and documents are recorded and stored;
- Customer (Controller) - the entity entering into this Agreement;
- Data - any data, including files containing text, sound, software, images and videos, provided to BTC by or on behalf of the Customer as a result of using the Service;
- Personal Data means information relating to an identified or identifiable natural person. An identifiable natural person is a person who can be identified directly or indirectly, in particular

by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

§ 1. Subject Matter of the Agreement

1. The Agreement sets out the rules for entrusting the Processor with the processing of personal data in connection with the Processor providing the Service to the Controller under the Subscription purchased by the Controller.
2. The Controller declares that it is the controller of the personal data entrusted to the Processor under the Agreement.
3. The Processor declares that it provides sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR and protects the rights of data subjects.
4. The Controller entrusts the Processor with the processing of personal data on behalf of the Controller, and the Processor undertakes to process the entrusted personal data lawfully and in accordance with the provisions of the Agreement, including with due care.

§ 2. Processing of Personal Data

1. The Processor shall process the personal data entrusted by the Controller for the purpose of providing the Service. Technical documentation, user documentation, and the terms, conditions and policies are available at: https://bluur.ai/.
2. The scope of personal data processing covers the following categories of personal data in relation to the following categories of persons: employees; data categories: first name, last name, e-mail address, IP address; documents in graphic form that may contain personal data.
3. The Processor may process personal data only within the scope and for the purpose provided for in the Agreement.
4. The Processor shall process personal data only on the documented instructions of the Controller, unless the Processor is required to do so by European Union law or the law of a Member State to which the Processor is subject; in such a case, before commencing processing, the Processor shall inform the Controller of that legal requirement, unless the law prohibits such information on important grounds of public interest. Personal data processing activities commissioned under this Agreement and the Terms and Conditions of the Service shall be deemed documented instructions.
5. Personal data shall be processed during the term of the Subscription to the Service, subject to paragraph 6.
6. The Processor may also process personal data after the provision of the Service has ended (in particular after the Subscription expires, is cancelled or is terminated), solely to the extent that such processing is necessary to pursue the legal interests of the Controller or the Processor, or where necessary for the Controller or the Processor to comply with obligations arising from applicable law.

§ 3. Obligations of the Processor

1. The Processor undertakes to ensure that persons authorised to process personal data keep such data and the methods used to secure it confidential, both while the Service is provided to the Controller and after it has ended.
2. The Processor shall implement all measures required under Article 32 of the GDPR.
3. The Processor undertakes to assist the Controller in complying with the obligations referred to in Articles 32-36 of the GDPR, in particular to:
   a) ensure an adequate level of security for the personal data being processed,
   b) provide the Controller with information about detected personal data breaches without undue delay, but no later than 24 hours after their detection.
4. The Processor undertakes to erase the personal data entrusted to it without undue delay after the purpose of processing has ceased, but no later than 14 days after the provision of the Service to the Controller has ended (in particular after the Subscription expires, is cancelled or is terminated), unless European Union law or the law of a Member State to which the Processor is subject requires the storage of personal data.
5. If no instructions have been provided by the Controller, the Processor may request the Controller to provide guidance on the further handling of the data.
6. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in the Agreement and shall allow audits, including inspections, to be conducted by the Controller or an auditor authorised by the Controller.
7. In connection with the obligation set out in paragraph 5, the Processor shall immediately inform the Controller if, in its

opinion, an instruction given to it infringes the GDPR or other European Union or Member State data-protection law to which the Processor is subject.

8. The Processor may use personal data to contact the Controller to the extent necessary to provide the Service and ensure the security of the Service (e.g. service notices, incident notices, technical-change announcements and Service operation reports).
9. The Processor may use personal data to inform the Controller about changes to the Service, new versions of the Service, new options and products. The Controller may opt out of receiving these messages by clicking the unsubscribe link in an e-mail received, following the instructions contained in it, or contacting the Processor. External service providers may be used to manage the sending of marketing e-mails, such as:
   - Mailerlite - Privacy Policy available at: https://www.mailerlite.com/pl/legal/privacy-policy.
10. The Processor may offer paid products and/or services as part of the Service. In such cases, payments are processed through external providers (payment processors). The Processor does not store or collect payment-card data. This information is transmitted directly to external payment processors, whose personal-data-protection rules are set out in their Privacy Policies. The processors apply the PCI-DSS standards managed by the PCI Security Standards Council, a joint initiative of brands such as Visa, Mastercard, American Express and Discover. PCI-DSS requirements ensure the secure processing of payment data. The Processor may use the services of providers such as:
    - Stripe - Privacy Policy available at: https://stripe.com/en-pl/privacy.
11. Except for the entities identified above, the Processor is not authorised to transfer personal data to a third country or an international organisation outside the European Economic Area. The Processor may not use subcontractors that transfer personal data outside the European Economic Area. If, in the course of performing the Agreement or the principal agreement, the Processor intends or is required to transfer personal data outside the European Economic Area, the Processor shall inform the Controller so that the Controller may take the steps necessary to ensure the lawfulness of the processing or terminate the entrustment of processing.

§ 4. Further Entrustment of Personal Data Processing

1. The Controller authorises the Processor to further entrust the processing of personal data within the European Economic Area, subject to paragraphs 2 and 4.
2. The Processor may not assign the entire performance of the Agreement to a subcontractor.
3. Further entrustment of processing shall take place under an agreement concluded by the Processor with a subcontractor, imposing on the subcontractor the same obligations and granting the Controller, in relation to the subcontractor, the same rights as arise under the Agreement, in particular the subcontractor´s obligation to provide sufficient guarantees for the implementation of appropriate technical and organisational measures so that processing meets the requirements of the GDPR, and the Controller´s right to inspect how the subcontractor processes the entrusted personal data.
4. The Processor shall inform the Controller of its intention to further entrust personal data at least 7 days before the further entrustment of processing. The absence of an express objection by the Controller shall constitute consent to the further entrustment of personal data processing.
5. The Processor shall inform the Controller that an agreement under which personal data processing was further entrusted has expired.
6. The Processor provides information about subprocessors at http://bluur.ai.

§ 5. Right of Inspection

1. Subject to § 3(6) of the Agreement, the Controller is entitled to inspect the manner in which the Processor processes the entrusted personal data.
2. The Controller shall inform the Processor of a planned audit at least 7 days before it begins.
3. An audit may be conducted by an authorised employee of the Controller or by an auditor authorised by the Controller.
4. As part of an audit, the Controller has the right to:
   a. inspect documents and information connected with the entrustment of personal data processing,
   b. inspect devices, media and IT or ICT systems used to process the entrusted personal data, provided that such action results from justified doubts on the part of the Controller;
   c. obtain written or oral explanations to the extent necessary to establish the facts.

5. After the audit has been completed, the Controller shall present the audit results to the Processor. The Processor may submit objections to the audit results within 7 days of receiving them.
6. If the audit results are negative, the Controller and the Processor undertake to take joint action to remedy the irregularities and ensure that the Processor continues to process personal data correctly.

§ 6. Liability

1. The Processor shall be liable to the Controller for damage caused by an act or omission in connection with a failure to fulfil obligations imposed directly on the Processor by the GDPR, or where the Processor has acted outside or contrary to the Controller´s lawful instructions.
2. The Processor shall be liable to the Controller for the acts and omissions of a subcontractor as for its own acts and omissions, in particular for a failure to fulfil personal-data-protection obligations.

§ 7. Term of the Agreement

1. The Agreement is concluded for the period during which the Service is provided to the Controller. The Agreement enters into force upon purchase of the Subscription and acceptance of its terms by the Controller. The processing of personal data shall continue until the obligation to return or erase personal data in accordance with § 3(4) has been fulfilled, and the provisions of the Agreement shall apply accordingly until that time.
2. The Parties jointly declare that entrusting the Processor with the processing of the personal data covered by the Agreement is voluntary but necessary for the Processor to properly provide the Service to the Controller. During the Subscription term, the Parties jointly exclude the possibility of terminating or giving notice to terminate the Agreement without simultaneously ending the provision of the Service to the Controller.
3. A breach of the provisions of the Agreement by the Processor constitutes an important reason entitling the Controller to demand the immediate cessation of personal data processing and the termination of the provision of the Service to the Controller (including cancellation of the Subscription), without prejudice to the Controller´s rights under applicable law.

§ 8. Final Provisions

1. In the event of any discrepancy between the provisions of the Agreement and other terms for the provision of the Service (including the Subscription terms), the provisions of the Agreement shall prevail.
2. Matters not regulated by this Agreement shall be governed by the GDPR and Polish law.
3. Disputes arising from the Agreement shall be resolved by the court having jurisdiction over the registered office of the Processor.
4. Any amendments to this Agreement must be made in electronic form, otherwise they shall be null and void.
5. The Agreement is concluded electronically and recorded in the Processor´s ICT system; the Parties acknowledge that acceptance of the Agreement during the account registration and/or Subscription activation process (including ticking a checkbox) is equivalent to making declarations of intent in documentary form.