

BLITZSUPPORT DATA PROCESSING AGREEMENT

Last updated: February 2026

This Data Processing Agreement (“DPA”) is an addendum to the Terms of Service between the Customer and aiGonomic GmbH (operating the BlitzSupport service) and governs the processing of Customer Personal Data in connection with the BlitzSupport services.

This DPA is intended to meet the requirements of Article 28 GDPR to the extent applicable and to reflect the parties’ obligations under applicable data protection laws for the processing described herein. If there is a conflict, this DPA prevails only with respect to data processing obligations (including Article 28 GDPR terms) relating to Customer Personal Data.

Availability and Execution

This DPA is made available publicly and forms part of the Terms of Service agreement. The Customer accepts this DPA by accepting the BlitzSupport Terms of Service and using the services. If the Customer requires a separately signed copy for its records, the parties will execute a signed version of this DPA upon request.

1. Parties

1.1 Customer (“Customer”, “Controller”): The organization or entity that uses the BlitzSupport services and determines the purposes and means of processing Customer Personal Data.

1.2 Processor: aiGonomic GmbH (“aiGonomic”, “BlitzSupport”, “Processor”)

1.3 Processor Contact:

- Privacy contact email: privacy@aigonomic.com
- Registered address: Ghersburgstraße 41, 83043 Bad Aibling, Germany

2. Definitions

2.1 “Customer Personal Data” means any Personal Data that the Customer (or its end-users) uploads, transmits, stores, or otherwise makes available through the BlitzSupport services and that the Processor processes on the Customer’s behalf.

2.2 “Data Protection Laws” means laws and regulations applicable to the processing of Customer Personal Data under this DPA, including the GDPR where applicable.

2.3 “Subprocessor” means any third-party service provider engaged by the Processor to process Customer Personal Data to support delivery of the services.

3. Subject Matter, Duration, and Processing Details

3.1 The Processor will process Customer Personal Data on behalf of the Customer for the purpose of providing the BlitzSupport services and related technical support, as described in the Terms of Service and further detailed in Annex 1 (Details of Processing).

3.2 Processing will continue for the duration of the Customer’s use of the services and until deletion or return of Customer Personal Data in accordance with Section 11.

4. Roles and Instructions

4.1 Controller and Processor. The Customer is the Controller of Customer Personal Data and determines the purposes and means of processing. The Processor acts as Processor and processes Customer Personal Data only on documented instructions from the Customer and as described in this DPA.

4.2 Customer Responsibilities. The Customer is responsible for (a) having a lawful basis and providing required notices and consents, (b) configuring the services appropriately, and (c) determining whether the services meet its compliance requirements for intended use.

4.3 Instructions. By entering into the Terms of Service and this DPA, the Customer instructs the Processor to process Customer Personal Data to provide the services. The Processor will not process Customer Personal Data outside the services' documented functionality and Customer instructions.

4.4 Unlawful Instructions. If the Processor reasonably believes an instruction violates applicable Data Protection Laws, the Processor will inform the Customer without undue delay and may suspend the relevant processing until the parties resolve the issue.

4.5 Legal Requirements. If the Processor is required by applicable law to process Customer Personal Data other than on Customer instructions, the Processor will inform the Customer unless legally prohibited.

5. Confidentiality of Processing

5.1 The Processor will ensure that persons authorized to process Customer Personal Data are bound by appropriate confidentiality obligations (contractual or statutory).

6. Security Measures

6.1 The Processor will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, as described in Annex 2 (Security Measures).

6.2 The Processor may update its measures over time to address evolving risks, provided the overall level of protection is not materially reduced during the term.

6.3 The Customer remains responsible for using the services securely (for example, protecting credentials, using appropriate access controls, and limiting the submission of sensitive content where not required).

7. Subprocessing

7.1 General Authorization. The Customer authorizes the Processor to engage Subprocessors to process Customer Personal Data as needed to provide and operate the services.

7.2 Subprocessors and Safeguards. The Processor engages reputable Subprocessors that provide appropriate technical and organizational safeguards. Where available, the Processor may rely on independent assurance materials (for example, ISO 27001 certifications or SOC reports) to support vendor due diligence.

7.3 Flow-Down and Responsibility. The Processor will (a) ensure that written data protection terms are in place with each Subprocessor for the relevant processing, and (b) remain responsible for the Subprocessor's processing of Customer Personal Data under this DPA.

7.4 Notification. The Processor maintains a current list of Subprocessors in Annex 3 and will provide reasonable advance notice of any intended addition or replacement of Subprocessors.

7.5 Objection. If the Customer reasonably objects to a new Subprocessor on data protection grounds, the Customer must notify the Processor in writing within 14 days of the notice. The parties will work in good faith to address the objection. If unresolved and the Subprocessor is required to provide the services, the Customer may terminate the affected services as its sole remedy under this Section.

8. Data Subject Rights and Cooperation

8.1 Taking into account the nature of the processing and the information available to the Processor, the Processor will provide reasonable assistance to the Customer to help the Customer comply with Data Protection Laws (including responding to data subject requests, security, breach notifications, and DPIAs). Assistance beyond standard service functionality may be subject to fees.

8.2 If the Processor receives a request directly from a data subject relating to Customer Personal Data, the Processor will, where permitted: promptly notify the Customer, and not respond directly unless instructed by the Customer or required by law.

9. Personal Data Breach Notification

9.1 The Processor will notify the Customer without undue delay after becoming aware of a Personal Data Breach involving Customer Personal Data.

9.2 To the extent reasonably available, the notification will include information reasonably necessary for the Customer to meet its obligations under applicable Data Protection Laws.

9.3 The Customer remains responsible for determining whether it must notify authorities and/or data subjects.

10. Data Transfers and International Processing

10.1 Customer Personal Data may be processed in regions required to provide the services, depending on Customer configuration and Subprocessors.

10.2 Where applicable Data Protection Laws impose cross-border transfer requirements, the parties will ensure appropriate safeguards are in place. Such safeguards may include Standard Contractual Clauses (SCCs) or other valid transfer mechanisms, as described in Annex 4, to the extent required and applicable.

10.3 Any data residency commitments must be agreed in writing and are subject to technical feasibility.

11. Deletion or Return of Data

11.1 During the term, the services may allow the Customer to delete or export Customer Personal Data, subject to the services' functionality.

11.2 Upon termination or expiration of the main agreement, the Processor will, at the Customer's choice to the extent available in the service: return Customer Personal Data to the Customer, and/or delete Customer Personal Data.

11.3 Unless legally prohibited, the Customer may request export or retrieval of Customer Personal Data for up to thirty (30) days after termination or expiration of the main agreement. The Processor will delete Customer Personal Data from production systems as soon as reasonably practicable and in any event within thirty (30) days after termination or expiration. If the Customer requests export within that period, the Processor will provide the export where reasonably feasible within the same 30-day period, and deletion will still occur within that period unless applicable law requires retention.

11.4 Customer Personal Data in backups will be deleted according to the Processor's backup lifecycle and will be fully purged within 90 days after deletion from production systems, unless legal retention obligations apply.

11.5 If the Processor is required by law to retain certain Customer Personal Data, the Processor will isolate and protect it from further processing except as required and will delete it when the legal requirement expires.

12. Audits and Compliance Demonstration

12.1 The Processor will make available information reasonably necessary to demonstrate compliance with this DPA. Audits will be carried out by documentation review and remote means where reasonably sufficient.

12.2 If an on-site inspection is reasonably necessary, it requires prior written notice and a mutually agreed scope and timing, and will be conducted at a mutually agreed professional location during normal business hours. The Customer bears its audit costs unless otherwise agreed.

13. Liability

13.1 Each party's liability arising out of or in connection with this DPA will be subject to the limitations and exclusions of liability in the Terms of Service, to the extent permitted by applicable law.

13.2 Nothing in this DPA limits a party's liability where such limitation is not permitted under applicable Data Protection Laws.

14. General Provisions

14.1 Order of Precedence. If there is a conflict between this DPA and the Terms of Service, this DPA prevails with respect to processing of Customer Personal Data.

14.2 Governing Law. This DPA is governed by the same law and jurisdiction as the Terms of Service, unless required otherwise by applicable Data Protection Laws. For interpretation of SCCs, EU law applies to the extent the SCCs apply.

14.3 Severability. If any provision is invalid or unenforceable, the remainder remains in effect and the parties will replace the invalid provision with a valid provision that best reflects the parties' intent.

14.4 Updates. The Processor may update Annexes that are expressly stated to be updateable (including the Subprocessor List and security measures), provided such updates do not materially reduce protections. Any other changes to this DPA must be agreed in writing.

14.5 Acceptance and Signature. By using the services and accepting the Terms of Service, the Customer is deemed to have accepted this DPA. If a separately signed copy is required, the parties may execute it upon request.

15. Signatures

For the Controller	For the Processor
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Annex 1: Details of Processing

Subject Matter: Provision of the BlitzSupport platform and related support services to the Customer.

Duration: For the term of the main agreement and until deletion or return in accordance with this DPA.

Nature of Processing: Processing may include collection, storage, organization, retrieval, use, transmission, deletion, and other operations necessary to provide the services.

Purpose of Processing: Delivering and operating the services, including ticket management, communications handling, and service functionality. Where enabled by the Customer, this may include processing necessary to provide AI-assisted features (for example, generating summaries or draft replies from Customer-provided content).

Categories of Data Subjects:

- Customer users (employees, contractors, authorized users)
- Customer end-users submitting support requests
- Other individuals whose Personal Data appears in Customer support communications

Types of Personal Data:

- Identifiers and contact details (name, email address, phone number)
- Ticket and communication content (message text, metadata, thread context)
- Attachments (which may contain Personal Data)
- Account, authentication, and usage data within the services
- Logs and security records related to service operation

Special Categories of Data: The services are not intended to process special categories of Personal Data. The Customer should avoid submitting special categories unless necessary and lawful.

Processing Locations: Primary processing takes place in the European Union, specifically in Germany using Microsoft Azure (Germany West Central) for production systems and backups. Additional processing locations depend on Customer configuration and Subprocessors used to deliver the services.

Annex 2: Technical and Organizational Security Measures

The Processor maintains measures designed to protect Customer Personal Data, including:

- Encryption in transit: TLS/HTTPS for data transmitted between Customer systems and the service.
- Encryption at rest: Azure SQL Transparent Data Encryption (TDE) for database storage; Azure Storage server-side encryption for stored objects (including logs and backups).
- Access control: Role-based access control and least-privilege access for internal personnel.
- Administrative safeguards: Authentication controls for privileged access. Multi-factor authentication (MFA) is not yet enforced for all administrative access and is planned to be implemented as part of ongoing security hardening.
- Logging and monitoring: Operational and security logging for service reliability and security events. Logs are stored in Azure Blob Storage.
- Vulnerability management and patching: Regular updates and patching of infrastructure and dependencies, commensurate with risk and environment.
- Backup and recovery: Backup and recovery procedures designed to support service continuity and restoration.

The Processor may update these measures over time provided the overall level of protection is not materially reduced during the term.

Annex 3: Authorized Subprocessors

Last updated: February 2026

This Annex 3 lists the Subprocessors that aiGonomic GmbH engages to process Customer Personal Data strictly as necessary to operate and deliver the BlitzSupport platform. It excludes providers used only for website operation, marketing, analytics, or customer acquisition.

aiGonomic maintains a current Subprocessor List for BlitzSupport. This Annex 3 may be updated in accordance with Section 7 (Subprocessing) of this DPA.

Name	Location	Purpose	Data Categories
Microsoft Azure	Germany (Germany West Central)	App hosting, processing, backups, database, logging storage	Contact Data, Usage Data, Support Content, Logs
Mailgun	Europe (EU Region)	Transactional emails (service notifications)	Recipient email/name, communication metadata, message content
OpenAI	See OpenAI DPA & data controls	AI-assisted processing of Customer content, AI agent execution	Support Content, Attachments, Usage Data
WebCrawlerAPI	See provider docs	Web crawling for knowledge base context	Website content as configured by Customer

Notes:

- OpenAI is an authorized Subprocessor for AI-assisted processing of Customer content via the OpenAI API. The applicable data handling, transfer safeguards, and Subprocessor details are described in OpenAI's Data Processing Addendum and data controls documentation.
- The Processor uses the OpenAI API under business terms and does not opt in to share Customer content for model training or improvement. OpenAI states that it does not train its models on API/business inputs and outputs by default unless a customer explicitly opts in.
- OpenAI may retain API data for limited periods for abuse monitoring and compliance purposes, as described in OpenAI's documentation. Where available and required by a Customer (for example, for sensitive workloads), the Processor can review feasibility of additional OpenAI retention or residency controls upon request.
- The Processor will provide notice of any intended addition or replacement of Subprocessors in accordance with Section 7.4.

Annex 4: International Data Transfers (SCCs)

This Annex applies only to the extent Customer Personal Data is subject to a restricted international transfer under applicable Data Protection Laws (a “Restricted Transfer”). Nothing in this Annex expands the scope of processing described in this DPA.

1. Transfers subject to the GDPR (EEA)

For Restricted Transfers subject to the GDPR, the EU Standard Contractual Clauses adopted by the European Commission in Commission Implementing Decision (EU) 2021/914 (Module 2, Controller to Processor) are incorporated by reference and form part of this DPA.

The parties agree the following selections, where applicable:

- Clause 7 (Docking clause): not used
- Clause 9 (Use of Subprocessors): Option 2 (general authorization), subject to Section 7 and Annex 3 of this DPA
- Clause 11 (Redress): optional language omitted
- Annexes I to III of the SCCs: completed by reference to Annex 1 (Details of Processing), Annex 2 (Security Measures), and Annex 3 (Authorized Subprocessors) of this DPA

2. Transfers subject to UK GDPR

For Restricted Transfers subject to UK GDPR, the parties will implement the UK International Data Transfer Addendum to the EU SCCs (or another valid UK transfer mechanism, such as the UK IDTA) before the Restricted Transfer occurs. The relevant Annexes are completed by reference to Annex 1 to Annex 3 of this DPA.

3. Transfers subject to Swiss law

For Restricted Transfers subject to Swiss law, the parties will implement the EU SCCs with the amendments required under Swiss data protection law (or another valid Swiss transfer mechanism) before the Restricted Transfer occurs. The relevant Annexes are completed by reference to Annex 1 to Annex 3 of this DPA.