Version 1.0

Prepared for Zaza Draft

Zaza Draft Data Processing Agreement

This Data Processing Agreement forms part of the agreement between the Customer and Zaza Technologies UG (haftungsbeschraenkt), Gumbertstrasse 150, 40229 Duesseldorf, Germany, as provider of Zaza Draft.

Processor: Zaza Technologies UG (haftungsbeschraenkt), Gumbertstrasse 150, 40229 Duesseldorf, Germany.

Controller: The Customer identified in the main agreement, including any teacher, school, district, or other educational institution using the Service.

This Agreement applies where Zaza Technologies processes personal data on behalf of the Customer in connection with Zaza Draft.

1. Subject Matter and Purpose

This Data Processing Agreement sets out the rights and obligations of the parties under Article 28 GDPR where Zaza Technologies processes personal data on behalf of the Customer through Zaza Draft.

Where Zaza Draft is used by an educational institution, the school or district acts as the Controller of student data. Zaza Draft acts solely as a Processor under the direct control of the school.

All student data and education records remain the sole property of the educational institution or user. Zaza Draft acquires no ownership rights.

2. Nature and Purpose of Processing

Zaza Draft is an AI-powered tool for drafting, reviewing, improving, translating, and structuring school communication.

The Service may process user-submitted text such as parent emails, report comments, behaviour notes, handover notes, pastoral communication, meeting summaries, and similar school communication materials.

Zaza Draft processes personal data solely for the purpose of providing the communication drafting service requested by the user. Data is not used for any unrelated purpose.

The Service is designed to support professional school communication workflows while maintaining institutional control over student-related data.

The Service is designed to support FERPA-aligned data handling for US schools, including institutional control, purpose limitation, and safeguards around student-related data.

3. Categories of Data Subjects

- Teachers, school leaders, support staff, and administrative staff.
- Parents, carers, guardians, and emergency contacts referenced in school communication.
- Students referenced in educational communication or records.
- Customer billing contacts, account owners, and support contacts.

4. Categories of Personal Data

- Account and contact data, such as name, email address, school name, role, and account identifiers.
- User-submitted text and communication content entered into the Service.
- Student-related data included by the Customer in submitted content, such as names, class references, behaviour context, attainment context, attendance context, and support needs where lawfully provided.
- Metadata required to provide the Service, such as timestamps, language choices, usage events, and technical logs.
- Billing and subscription data required for account management.

The service is designed to process only the minimum data necessary. Users are advised not to include unnecessary or highly sensitive personal data.

5. Duration of Processing

Processing continues for the duration of the main agreement and for as long as Zaza Technologies needs the data to provide the Service or comply with applicable law.

The Customer may request deletion of Customer data at any time in accordance with Section 11.

6. Obligations of the Processor

Zaza Technologies shall:

- process personal data only on documented instructions from the Customer, unless otherwise required by applicable law;
- ensure that persons authorised to process personal data are subject to confidentiality obligations;
- implement appropriate technical and organisational measures in accordance with Article 32 GDPR and Schedule 2;
- assist the Customer with requests relating to access, rectification, restriction, objection, portability, and deletion where applicable;
- assist the Customer with security assessments, breach response, and regulatory notifications to the extent required by Article 28 GDPR;
- maintain records of categories of processing activities as required by law;
- make available information reasonably necessary to demonstrate compliance with this Agreement;
- notify the Customer if, in Zaza Technologies' opinion, an instruction infringes applicable data protection law.

Zaza Draft does not use customer data, including student-related data, to train, improve, or develop general AI models.

Zaza Draft will not disclose personal data to third parties except as required to provide the service or as legally required.

Zaza Draft does not access user content except where necessary for security, support, or legal obligations.

7. Sub-processors

The Customer authorises the use of sub-processors listed in Schedule 1.

Zaza Technologies shall ensure that each authorised sub-processor is bound by written terms that provide data protection obligations no less protective than those set out in this Agreement.

Zaza Technologies shall remain responsible for the performance of its sub-processors.

Where Zaza Technologies appoints a new sub-processor that materially affects Customer data processing, it shall provide reasonable notice and an opportunity for the Customer to raise a reasonable data protection objection.

8. International Transfers

Where personal data is transferred outside the United Kingdom or European Economic Area, Zaza Technologies shall ensure that appropriate safeguards are in place, including Standard Contractual Clauses or another lawful transfer mechanism.

Where possible, Zaza Technologies will use EU or UK based processing options for school data. Where a US based provider is used, transfers shall be subject to appropriate safeguards.

9. Data Subject Rights

Taking into account the nature of the processing, Zaza Technologies shall provide reasonable assistance to the Customer for the fulfilment of the Customer's obligation to respond to requests by data subjects.

If Zaza Technologies receives a request directly from a data subject relating to Customer data, it shall promptly notify the Customer unless prohibited by law.

10. Data Breach Notification

Zaza Technologies shall notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer data and, where feasible, within 72 hours.

The notification shall include, to the extent then available:

- the nature of the breach;
- the categories and approximate number of affected data subjects;
- the categories and approximate number of affected personal data records;
- the likely consequences of the breach;
- measures taken or proposed to address and mitigate the breach;
- a contact point for follow-up information.

11. Deletion and Return of Data

The Customer may request deletion of Customer data at any time.

Upon termination of the main agreement, or upon a valid deletion request, Zaza Technologies shall delete or return Customer data unless retention is required by applicable law.

Deletion shall be completed within 30 days of the valid request or termination date unless a shorter or longer period is legally required or technically justified and communicated to the Customer.

Confirmation of deletion shall be provided on request.

12. Audit Rights

Zaza Technologies shall make available to the Customer all information reasonably necessary to demonstrate compliance with this Agreement.

The Customer may, no more than once per year and on reasonable prior notice, conduct an audit or appoint an independent auditor bound by confidentiality to verify compliance, provided that the audit does not unreasonably interfere with Zaza Technologies' operations or compromise the security of other customers.

Zaza Technologies may satisfy audit requests through current third-party audit materials, security summaries, certifications, or documented responses where appropriate.

13. Governing Law

This Agreement shall be governed by the law governing the main agreement between the parties.

If the main agreement does not specify governing law, this Agreement shall be governed by the laws of Germany, excluding conflict of laws rules.

Schedule 1 - Sub-processors

1. Vercel Inc.

- Purpose: Hosting, edge delivery, application runtime, logging, and deployment infrastructure.
- Data involved: account data, submitted content processed through the application runtime, operational logs, and technical metadata.
- Location: EU and US infrastructure as configured by the provider.
- Transfer safeguard: SCCs or another valid transfer mechanism where required.

2. Anthropic PBC

- Purpose: AI text processing for drafting, reviewing, improving, translating, and restructuring school communication.
- Data involved: user-submitted prompts, message drafts, and model responses.
- Location: United States.
- Transfer safeguard: SCCs or another valid transfer mechanism where required.

3. Stripe, Inc. / Stripe Payments Europe, Ltd.

- Purpose: subscription billing, payment processing, fraud prevention, and financial reporting.
- Data involved: billing contact data, subscription identifiers, payment metadata, and transaction records.
- Location: EU and US.
- Transfer safeguard: SCCs or another valid transfer mechanism where required.
- Note: Stripe is not intended to receive routine student content.

4. Brevo SAS

- Purpose: transactional email, support communications, and mailing list management where enabled by the Customer.

- Data involved: contact data, email metadata, and support communication data.
- Location: European Union.
- Transfer safeguard: processing within the EU, with contractual safeguards as applicable.
- Note: Brevo is not intended to receive routine student content.

5. Plausible Insights OUE

- Purpose: privacy-friendly website analytics and usage measurement.
- Data involved: pseudonymous website usage data, page views, device and referral metadata.
- Location: European Union.
- Transfer safeguard: processing within the EU.
- Note: Plausible is not intended to receive routine student content or message drafts.

Schedule 2 - Technical & Organisational Measures

- Encryption in transit using TLS for data transmitted between users, the Service, and authorised sub-processors.
- Encryption at rest using AES-256 or equivalent industry-standard protections provided by infrastructure and storage sub-processors.
- Least privilege access controls for production systems and support tooling.
- Role-based internal access controls and segregation of duties where appropriate.
- Authentication protections for administrative access, including strong credentials and multi-factor authentication where supported.
- Logging and monitoring for service reliability, abuse detection, and incident investigation.
- Procedures for incident response, containment, remediation, and customer communication.
- Vendor management and written data processing terms with relevant sub-processors.
- Data minimisation in product design and operational practice.
- Controls to limit human access to Customer content to security, support, and legal necessity cases.
- Secure software update, patching, and vulnerability management processes.
- Backup and recovery measures appropriate to the Service.
- Deletion workflows to support account closure, Customer deletion requests, and end of contract return or deletion.

Acceptance

This Data Processing Agreement is accepted by execution of the main agreement, use of the Service under that agreement, or signature below.

For the Controller / Customer:

Name:

Title:

Institution:

Date:

Signature:

For the Processor:

Zaza Technologies UG (haftungsbeschraenkt)

Name:

Title:

Date:

Signature: