

Terms of Use and Data Processing Agreement for the WordPress Plugin

“WriteUp” B2B

This agreement governs the provision of the WordPress plugin “WriteUp” as well as the associated processing of personal data in accordance with the legal requirements of the GDPR and the German Civil Code (BGB) for merchants, legal entities under public law, or special funds under public law.

For consumers, the provisions of the User Agreement **for the WordPress plugin “WriteUp” (B2C)** apply!

I. User Agreement (SaaS and License Terms)

1. Subject Matter of the Agreement and Parties

The subject matter of this Agreement is the provision of the functionalities of the WordPress plugin “WriteUp” (hereinafter “Plugin”). The Plugin is intended to provide technical support for text processing within the user’s WordPress environment.

This agreement is intended exclusively for **business entities as defined in § 14 of the German Civil Code (BGB)**.

Role	Contracting Party	Description
Provider	Meta-Level Software AG, Lyonerring 1, 66121 Saarbrücken	Owner of all copyrights and intellectual property rights; technical provider of the software infrastructure.
Reseller	Digistore24 GmbH, St.- Godehard-Straße 32, 31139 Hildesheim	Legal seller (Merchant of Record); the user’s contractual partner for commercial purchases.
User	The business customer	The business owner (Section 14 of the German Civil Code (BGB)) who licenses the plugin for their business activities.

2. Reseller Model (Digistore24)

Commercial transactions are handled by the reseller Digistore24. The user enters into the purchase agreement for the license directly with Digistore24 GmbH.

- **Payment and Billing:** All payment processing and invoicing are handled exclusively by Digistore24.
- **Provision:** Meta-Level Software AG is responsible for the technical provision and maintenance of the plugin, without becoming a party to the purchase agreement concluded between the reseller and the user.

3. Rights of Use and IP Ownership

All copyrights, trademark rights, and other intellectual property rights in the plugin, as well as in the underlying algorithms and cloud infrastructure, remain exclusively with **Meta-Level Software AG**.

- For the duration of the contract, the user is granted a non-exclusive, non-transferable, and non-sublicensable right to use the plugin for commercial purposes on their own WordPress instances in accordance with its intended use.
- Any form of decompilation, reverse engineering, or reproduction beyond the intended use is prohibited, unless required by mandatory statutory provisions.

4. Scope of Services and “Best-Effort” Principle

The plugin and cloud components are provided on a **“best-effort” basis**.

- The Provider does not guarantee availability; Service Level Agreements (SLAs) are not part of this contract.
- The user must accept maintenance windows, necessary updates, or brief interruptions in cloud connectivity. The Provider will endeavor to minimize any disruptions as much as possible.

5. Exclusion of B2C Rights (Right of Withdrawal)

Due to the purely commercial nature of this contract (B2B), the distance selling law for consumers does not apply. There is no statutory right of withdrawal. The provisions of Sections 312g in conjunction with 355 of the German Civil Code (BGB) expressly do not apply.

6. Limitation of Liability and Inbound Transfer Disclaimer

Special Limitation of Liability for Use by Foreign Users:

1. Territorial Scope of Application

Unless expressly agreed otherwise in the service description, the application was developed exclusively with regard to the legal requirements applicable in Germany. The provider is under no obligation to verify or warrant that the application complies with the legal requirements of other countries.

The user is responsible for verifying, prior to using the application outside of Germany or for business activities related to other legal systems, whether its selection, configuration, and specific use are permissible under the applicable regulations.

This does not apply to the extent that the Provider has expressly committed to compliance with certain foreign legal provisions as a contractual obligation. The Provider’s mandatory legal obligations and liability under the general liability provisions of this Agreement remain unaffected.

2. Unless expressly agreed, the Provider is under no obligation to verify or warrant the Application's compliance with foreign legal provisions.
3. German law and the GDPR apply.
4. All server locations and data processing operations are physically located in Germany or the EU.

7. Restrictions

The user agrees not to submit any user content to the WriteUp service that

- infringe the intellectual property rights or other rights of third parties,
- violates any laws or regulations,
- is dangerous, harmful, fraudulent, threatening, harassing, defamatory, or obscene.

Prohibited Use

WriteUp may not be used to generate content that promises or purports to provide legal, medical, financial, or other professional advice without review by a qualified professional.

The Provider reserves the right to restrict or deny access to "WriteUp" if the user violates these Terms and Conditions.

8. Termination

(1) Ordinary Termination:

The contract, including the subscription, may be terminated by either party up to fourteen (14) days prior to the renewal of the subscription, unless otherwise agreed in writing.

(2) Extraordinary Termination:

The right to terminate the contract for cause remains unaffected. Cause exists in particular if:

- a) one of the parties repeatedly or seriously breaches its contractual or statutory obligations,
- b) insolvency proceedings are initiated against the assets of one of the parties or an application is filed to initiate such proceedings, or
- c) the actions or omissions of a party result in compliance with the GDPR or other legal requirements no longer being guaranteed.

(3) Termination of the Subscription:

The subscription also ends upon termination of the contract with the reseller, **Digistore24 GmbH** (St.-Godehard-Straße 32, 31139 Hildesheim, Germany). From that point on, the user is no longer entitled to use the services provided.

Consequences of Termination:

Upon termination of the contractual relationship, the Provider undertakes to delete all personal data collected in the course of processing and use in accordance with data protection requirements, unless there is a legal obligation to retain such data.

9. Discontinuation of the Service

(1) The Provider is entitled to discontinue the Service in its entirety or individual, functionally distinct components of the Service with future effect if

- a) their continued operation becomes unlawful or unreasonable for the Provider due to a change in the legal situation or an enforceable administrative or court order,
- b) the Service or the affected component can no longer be operated at an economically and technically reasonable cost due to significant technical changes, in particular the discontinuation of necessary third-party services,
- c) continued operation is no longer justifiable due to significant security risks, or
- d) the provider permanently discontinues the service for economic reasons, provided that the user's interest in the service's continuation does not outweigh the provider's interest in its discontinuation.

(2) The ongoing technical and functional development of the service—in particular, changes to the user interface, the replacement of individual functions with equivalent functions, and technically necessary adjustments—shall not be considered a discontinuation, provided that the agreed-upon ability to use the service is not materially impaired as a result.

(3) Unless a case under paragraph 4 applies, the Provider shall notify the User of the intended discontinuation in writing at least two months in advance. In the event of only a partial discontinuation, the Provider shall specify in the notice the affected service component and the date of its discontinuation.

(4) Immediate discontinuation or temporary suspension is permitted only to the extent that it is necessary to avert a present and significant threat to the security or integrity of the service, to prevent unlawful use, to comply with an enforceable administrative or judicial order, or due to other circumstances that, upon weighing the interests of both parties, make it unreasonable for the Provider to continue the service until the end of the notice period. The provider shall inform the user immediately of the measure and its reason, provided that no statutory provisions, official orders, or legitimate security interests preclude this.

(5) If the discontinuation of individual components significantly impairs the agreed-upon use of the remaining service, the user is entitled to terminate the affected contract for cause as of the date of discontinuation. The user may give notice of termination within two weeks of receiving the notification.

(6) In the event of complete discontinuation, the contract shall terminate on the notified date of discontinuation. Any usage-based or time-based fees paid in advance for the period following the end of the contract shall be refunded to the user on a pro-rata basis. Any further claims shall be governed by the agreed liability provisions.

(7) The right of both parties to terminate the contract for cause in accordance with the contractual provisions, as well as to terminate the contract extraordinarily for good cause, remains unaffected.

10. Final Provisions and Jurisdiction

- **Place of Jurisdiction:** The exclusive place of jurisdiction for all disputes arising from or in connection with this contract is **Saarbrücken**.
- **Governing Law:** The law of the Federal Republic of Germany shall apply, excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).
- Should individual provisions of this contract be wholly or partially invalid or unenforceable, or become invalid or unenforceable after the conclusion of the contract, the validity of the remaining provisions shall remain unaffected.

II. Data Processing Agreement (DPA) pursuant to Art. 28 of the GDPR

§ 1 General Provisions

(1) The Provider processes personal data on behalf of the User within the meaning of Art. 4(8) and Art. 28 of Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR). This Agreement governs the rights and obligations of the parties in connection with the processing of personal data.

(2) Where the terms "data processing" or "processing" (of data) are used in this agreement, the definition of "processing" as defined in Article 4(2) of the GDPR shall apply.

§ 2 Subject Matter of the Agreement

The subject matter of the processing, the nature and purpose of the processing, the type of personal data, and the categories of data subjects are set forth in Annex 1 to this Agreement.

§ 3 Rights and Obligations of the User

(1) The User is the controller within the meaning of Article 4(7) of the GDPR for the processing of data carried out by the Provider on its behalf. Pursuant to Section 4(5), the Provider has the right to notify the

User if, in its opinion, legally impermissible data processing is the subject of the contract and/or an instruction.

(2) As the data controller, the User is responsible for safeguarding the rights of data subjects. The Provider shall immediately inform the User if data subjects assert their rights against the Provider in connection with this processing of data on behalf of the User.

(3) The User shall inform the Provider immediately if it detects any errors or irregularities in connection with the Provider's processing of personal data.

(4) In the event that there is an obligation to inform third parties pursuant to Articles 33 and 34 of the GDPR or any other statutory reporting obligation applicable to the User, the User is responsible for complying with such obligations.

(5) In the event of termination of the contractual relationship, the user agrees to delete, prior to termination, any personal data that the user has stored in the services.

(6) Upon request by the Provider, the User shall designate a contact person for data protection matters.

§ 4 General Obligations of the Provider

(1) The Provider shall process personal data exclusively within the scope of the agreements entered into. These are initially set forth in the main contract and may subsequently be amended by the User in writing through specific instructions. Exceptions to this are statutory provisions that may require the Provider to process data in a different manner. In such a case, the Provider shall notify the User of these legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest. Otherwise, the purpose, nature, and scope of data processing shall be governed exclusively by this contract and/or the User's instructions.

(2) The Provider undertakes to carry out data processing on behalf of the User only in member states of the European Union (EU) or the European Economic Area (EEA). Processing in a third country is excluded.

(3) With regard to processing on behalf of the User, the Provider guarantees the contractual execution of all agreed-upon measures.

(4) The Provider is obligated to organize its operational processes in such a way that the data is secured to the necessary extent and protected against unauthorized access by third parties.

(5) The Provider shall immediately inform the User of any processing operations that violate instructions or are unlawful. The Provider is entitled to suspend the execution of an instruction until it is confirmed or amended by the User.

(6) The Provider shall process the User's data separately from other data sets. Physical separation is not required.

§ 5 Provider's Data Protection Officer

(1) The Provider confirms that it has appointed a Data Protection Officer in accordance with Art. 37 of the GDPR. Contact information is published on the Provider's website.

(2) The obligation to appoint a data protection officer does not apply only if the Provider can demonstrate that it is not legally required to do so and that internal policies ensure compliance with the regulations.

§ 6 Provider's Reporting Obligations

(1) The Provider shall immediately notify the User of any violation of data protection regulations or instructions. The same applies to breaches of personal data protection.

(2) The provider shall immediately inform the user of any activities by supervisory authorities pursuant to Art. 58 of the GDPR, provided that such activities relate to the contract.

§ 7 Audit Rights

(1) The User has the right to monitor the Provider's compliance with the regulations and agreements at any time to the extent necessary.

(2) The Provider is obligated to provide information.

(3) The user may request access to the processed data and systems.

(4) On-site inspections are possible during normal business hours upon notice given with reasonable advance notice.

(5) The Provider shall assist the User in connection with measures taken by the supervisory authority.

(6) The Provider may charge a reasonable fee for such assistance, provided there is no breach on the part of the Provider.

§ 8 Subcontracting

(1) The User grants the Provider general authorization to engage additional subprocessors within the meaning of Article 28 of the GDPR. Existing subprocessors are listed in Appendix 2.

(2) The Provider shall carefully select subprocessors and regularly monitor them for compliance with the technical and organizational measures (TOMs) pursuant to Article 32 of the GDPR.

(3) The Provider shall obtain confirmation from the subprocessor that a data protection officer has been appointed or shall request appropriate evidence of a statutory exemption.

- (4) The Provider ensures that the provisions of this Agreement also apply to the subprocessor.
- (5) A contract in accordance with Article 28 of the GDPR must be concluded with the subprocessor. A copy of this contract must be provided to the user upon request.
- (6) Purely ancillary services (mail, transportation, security) are not considered subcontracting relationships but require appropriate safeguards.

§ 9 Confidentiality Obligation

- (1) The Provider shall maintain the confidentiality of all data it receives in connection with the order.
- (2) The Provider shall require its employees to maintain confidentiality and shall familiarize them with the data protection provisions.
- (3) Proof of these obligations must be provided to the User upon request.
- (4) This obligation shall continue after the termination of the contract.

§ 10 Protection of Data Subjects' Rights

- (1) The User is solely responsible for protecting the rights of data subjects. The Provider shall assist the User with requests pursuant to Articles 12–23 of the GDPR.
- (2) Necessary measures shall be taken in accordance with the User's instructions. The Provider shall support the User with appropriate technical and organizational measures.
- (3) Provisions regarding compensation for additional expenses remain unaffected.
- (4) The Provider may refer data subjects to the controller and provide the controller's contact information.

§ 11 Liability and Damages

- (1) The parties shall assist each other in clarifying claims for damages pursuant to Article 82 of the GDPR.
- (2) The liability provisions agreed upon in the main contract also apply to this agreement.

§ 12 Confidentiality

- (1) Information must be treated as confidential indefinitely and used solely for the purpose of fulfilling the contract.
- (2) This does not apply to information that is publicly known or has been lawfully obtained from third parties.

§ 13 Prohibition on the Reproduction or Disclosure of Data

(1) Processing of Data:

The data processor is not authorized to copy, reproduce, store, or otherwise process the client's personal data in any manner not expressly covered by this contract or the client's written instructions.

(2) No AI Training with User Data:

The data provided by the Client and processed by the Sally app shall not be used to train AI models. The Data Processor is prohibited from using the data on its own responsibility for its own business purposes. This also applies to non-personal data.

(3) Unauthorized Disclosure:

Any unauthorized disclosure, sale, or use of the data—in particular for the processor's own purposes or those of third parties—is expressly prohibited.

§ 14 Compensation

Remuneration is governed by the main contract (subscription).

§ 15 Technical and Organizational Measures (TOM)

(1) The Provider complies with the measures set forth in Article 32 of the GDPR.

(2) The current status is set forth in Appendix 3. Changes are permitted provided that the level of protection is not reduced.

§ 16 Term of the Agreement

(1) The contract begins upon conclusion of the main contract.

(2) The Provider may amend the agreement in the event of significant legal changes, provided reasonable notice is given (the User's right to object).

(3) In the event of any conflict, this agreement shall take precedence over the main contract.

§ 17 Termination

(1) Upon completion of the services, data shall be returned, anonymized, or deleted at the user's discretion.

(2) Statutory retention obligations remain unaffected.

§ 18 Right of Retention

A right of retention with respect to the data pursuant to § 273 of the German Civil Code (BGB) is excluded.

§ 19 Final Provisions

(1) Any threats to the data posed by third parties (seizure, etc.) must be reported to the user immediately.

(2) Should any provisions of this agreement be invalid, the validity of the remaining provisions shall remain unaffected.

Appendix 1: Scope of the Agreement

Purpose: Provision of cloud-based functions for text optimization and error correction.

Provision of the functionalities of the WordPress plugin “WriteUp” (hereinafter “Plugin”). The Plugin is intended to provide technical support for text processing within the User’s WordPress environment.

Types of personal data:

- Name and email address
- IP address
- Login credentials (hash)
- URL of the WordPress website
- Content of requests (inputs into the AI interface)

Categories of data subjects:

- Users of the WriteUp plugin

Appendix 2: Subcontractors

Subcontractors	Address	Role	Data processing within the EU
Digistore24 GmbH	St.-Godehard-Straße 32, 31139 Hildesheim, DE	Merchant of Record / Reseller & Payment Processing	Yes
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, DE	Hosting and provision of infrastructure for local LLM deployment (server location: Germany)	Yes

Appendix 3: Technical and Organizational Measures (TOMs)

1. Confidentiality

- **Access control:** Smart card access control system for buildings and floors; immediate deactivation upon loss report; security zones; cloud hosting provider in Germany obligated to operate data centers with high security standards (e.g., ISO 27001)
- **Access Control:** Role-based authorization profiles; authentication via username/password or token; encrypted transmission of login credentials; firewall protection.
- **Access control:** Authorization policy managed by administrators; access restricted to the extent necessary for task completion; transmission of all data exclusively via encrypted channels (e.g., HTTPS).
- **Segregation of duties:** Secure client access (Entity Framework); separate storage of user/customer data based on intended use; strict separation of development and production systems.

2. Integrity

- **Input control:** Logging of input, modification, and deletion using unique identifiers to ensure traceability.
- **Disclosure Control:** Data transmission only to the extent functionally necessary; encryption of all data streams; written confidentiality agreements for all employees.

3. Availability and Resilience

- **Backup:** Backup and recovery strategy; regular creation of backup copies.
- **Contingency Plan:** Documented procedures for restoring systems in the event of a crisis.

4. Privacy by Design / Default

- **Data minimization:** Standard limitation of data collection to the functional minimum.
- **Automated Deletion Functions:** Implementation of routines for the automated deletion of request logs after a specified period (30 days).
- **Opt-in solutions:** Optional data collection is disabled by default until explicitly enabled by the user.

5. Procedures for Regular Review

- **Data Protection:** Involvement of the company's Data Protection Officer (DPO) in all data protection-related planning; centralized documentation of procedures

These measures are reviewed regularly and adapted to the state of the art as well as to the client's requirements. Any changes or additions to this appendix shall be agreed upon in writing.