DPA · ART. 28 GDPR

Data Processing Agreement

This agreement governs the processing of personal data pursuant to Art. 28 GDPR between Paldra as the processor and the respective customer as the controller.

Parties

Data Processing Agreement (DPA) pursuant to Art. 28 General Data Protection Regulation (GDPR) between

PROCESSOR

Paldra Technologies
Owner: Asmir Kuljancic
Vordere Karlstr. 74
73033 Göppingen
Germany
Email: datenschutz@paldra.com
VAT ID: DE458199320

CONTROLLER

The respective customer / user of the services

collectively also referred to as the "Parties".

Section 1 Subject Matter and Duration of Processing

This agreement governs the processing of personal data by the Processor on behalf of the Controller pursuant to Art. 28 GDPR.

The Processor provides a software platform through which digital software services can be operated, in particular:

- AI-powered chatbots
- Automated communication systems
- API-based applications
- Analytics and automation features

Processing is carried out exclusively for the purpose of providing the services used by the Controller.

The term of this agreement is aligned with the duration of the Controller's use of the Processor's services.

Section 2 Nature and Purpose of Processing

The processing of personal data is carried out for the following purposes:

- Provision and operation of the software platform
- Processing of user inquiries
- Automated generation of responses through AI systems
- Communication with end users
- Ensuring system security

- Error analysis and system improvement

Processing is carried out exclusively on the basis of documented instructions from the Controller.

The services may not be used to process unlawful content or to process personal data in violation of applicable data protection law.

Section 3 Types of Personal Data

The following types of data may be processed in connection with the use of the services:

- Name
- Email address
- Communication data
- Profile details from connected channels (e.g. username and profile picture on Instagram)
- Text inputs from users
- Support inquiries
- Order data from connected store systems (e.g. order number, status, date, items, tracking number, payment link of unpaid orders)
- Usage data
- Technical metadata (e.g. IP address, timestamps)

The Controller undertakes not to transmit special categories of personal data pursuant to Art. 9 GDPR (e.g. health data, biometric data, political opinions, religious beliefs) through the services, unless expressly agreed in writing.

Section 4 Categories of Data Subjects

- Website visitors
- Customers of the Controller
- Prospects
- Users of digital services
- Employees of the Controller

Section 5 Controller's Right of Instruction

The Processor shall process personal data exclusively in accordance with the documented instructions of the Controller.

Instructions may be issued in particular through:

- This agreement
- The terms of service
- Technical settings within the platform
- Written or electronic instructions

If the Processor believes that an instruction violates applicable data protection law, it shall inform the Controller without delay.

The Processor shall process personal data exclusively within the scope of this agreement and in accordance with applicable data protection regulations.

Section 6 Confidentiality

The Processor shall ensure that all persons entrusted with the processing of personal data are bound by confidentiality obligations.

This obligation shall continue to apply after the termination of the activity.

Section 7 Technical and Organizational Measures (TOMs)

The Processor shall implement appropriate technical and organizational measures pursuant to Art. 32 GDPR.

These include in particular:

- Encryption of stored access credentials (IMAP/SMTP credentials and OAuth tokens are stored encrypted, "at rest")
- Tenant isolation: logical separation of data per customer based on a unique tenant identifier (shop_id)
- EU hosting of the production systems in Germany
- Access control and session management
- Role-based access systems
- Authentication systems
- Multi-factor authentication for administrative access
- Encrypted data transmission (TLS transport encryption / HTTPS)
- Secure server infrastructure
- Firewall systems
- System monitoring
- Logging and monitoring
- Regular, encrypted backups (off-host within the EU)
- Recovery mechanisms

The measures are reviewed regularly and adjusted as necessary.

Section 8 Assistance to the Controller

The Processor shall assist the Controller in complying with its legal obligations under the GDPR.

This includes in particular assistance with:

- Exercising data subject rights
- Data protection impact assessments
- Security measures
- Notification of data breaches

Section 9 Notification of Data Breaches

The Processor shall inform the Controller without delay of any data breach involving personal data.

Notification shall be made without undue delay and shall contain all relevant information for assessing the incident.

Section 10 Sub-processors

The Processor is authorized to engage sub-processors.

The Processor shall inform the Controller of any changes or additions to the sub-processors engaged in an appropriate manner, for example via the website or by electronic notification.

The Controller has the right to object to such changes within a reasonable period, provided there are legitimate data protection grounds.

A current list of sub-processors engaged is available at all times on the Processor's website at https://paldra.com/subprocessors.

Possible sub-processors include in particular:

PROVIDER	PURPOSE	LOCATION	BASIS
Always in use			
Hetzner Online GmbH Privacy notice	Hosting / storage / backup (cloud infrastructure)	Germany (EU)	EU
Anthropic, PBC Privacy notice	AI / language model (LLM) for responses, automated checks, image descriptions and evaluations (Claude)	USA	SCC · DPF
OpenAI Privacy notice	AI / language model (LLM) as a fallback and for load balancing	USA	SCC · DPF
Mistral AI Privacy notice	AI / language model (LLM), embeddings, OCR, transcription	France (EU)	EU
Microsoft Ireland Operations Ltd. / Microsoft Corp. Privacy notice	Email sending (Microsoft Graph) and optionally connected Outlook mailbox	Ireland (EU) / USA	SCC · DPF
Stripe, Inc. Privacy notice	Payment processing	USA	SCC · DPF
Cloudflare, Inc. Privacy notice	DNS / CDN / proxy	USA	SCC · DPF
Only if the Controller uses the feature			
Google LLC Privacy notice	Optionally connected Gmail mailbox; account sign-in ("Sign in with Google"); delivery of push notifications to Android/Chrome devices	USA	SCC · DPF
Apple Inc. Privacy notice	Account sign-in ("Sign in with Apple"); delivery of push notifications to Safari/iOS devices	USA	SCC · DPF
Meta Platforms Ireland Ltd. / Meta Platforms, Inc. Privacy notice	Optionally connected Instagram / WhatsApp channels	Ireland (EU) / USA	SCC · DPF

Shopify International Ltd. Privacy notice	Integration activated by the merchant: product, order, customer and return data and the store's legal policies; app billing through Shopify	Ireland (EU) / Canada, USA	SCC · DPF

EU = processing within the EU. SCC · DPF = EU Standard Contractual Clauses and, where the provider is certified, the EU-US Data Privacy Framework (Art. 44 et seq. GDPR).

The Processor ensures that all sub-processors engaged are contractually obligated to comply with data protection requirements pursuant to Art. 28 GDPR.

Section 11 International Data Transfers

A transfer of personal data to countries outside the European Economic Area may occur.

Such transfers shall only be carried out in compliance with the legal requirements pursuant to Art. 44 et seq. GDPR.

The following mechanisms may be used in particular:

- EU Standard Contractual Clauses (SCCs)
- EU-US Data Privacy Framework (DPF), insofar as the respective US sub-processor is certified
- Adequacy decisions of the European Commission
- Or comparable legal safeguards under the GDPR, insofar as this is necessary for the provision of the services

For US sub-processors (in particular Microsoft Corp., Google LLC, Apple Inc., Meta Platforms, Inc., Stripe, Inc. and Cloudflare, Inc.), transfers are carried out on the basis of the EU Standard Contractual Clauses and - insofar as the respective company is certified - the EU-US Data Privacy Framework pursuant to Art. 44 et seq. GDPR.

For the AI sub-processors Anthropic, PBC and OpenAI (USA), transfers are carried out on the basis of the EU Standard Contractual Clauses (their respective Data Processing Addendum) pursuant to Art. 46 GDPR.

Section 12 Deletion and Return of Data

Upon termination of the contract or of the use of the services, personal data shall, pursuant to Art. 28(3)(g) GDPR and at the choice of the Controller, be deleted or returned, unless statutory retention obligations apply.

Chat and conversation data are retained for a regular period of 12 months and deleted thereafter.

Backups shall be deleted within the regular backup cycles.

Section 13 Audit Rights

The Controller is entitled to verify compliance with this agreement.

The Processor shall provide the Controller with all information necessary to demonstrate compliance with the GDPR.

Such audits must not disproportionately disrupt the Processor's business operations and must be conducted with reasonable prior notice.

The costs of an audit shall generally be borne by the Controller, unless a significant breach of data protection provisions by the Processor is identified.

Section 14 Liability

To the extent permitted by law, the Processor's liability for damages arising from or in connection with this agreement shall be limited to the amount paid by the Controller to the Processor in the twelve (12) months preceding the event giving rise to the damage.

This limitation of liability shall not apply in cases of:

- Intentional misconduct
- Gross negligence
- Injury to life, body or health
- Mandatory statutory liability provisions

Section 15 Final Provisions

Should any provision of this agreement be or become invalid, the validity of the remaining provisions shall remain unaffected.

The law of the Federal Republic of Germany shall apply.

The place of jurisdiction shall be - to the extent permitted by law - the registered office of the Processor.

Section 16 Use of AI Systems

The Processor may use automated systems including artificial intelligence to provide the services.

Data transmitted by the Controller shall be processed exclusively for the purpose of generating responses and providing the services.

The data is not used to train AI models, neither by the processor nor by its sub-processors.

This is distinct from learning from cases: the processor may derive examples (question and answer) from requests that have already been answered and store them in the controller's knowledge base in order to improve future answers for the controller. No AI model is trained or changed in the process. These examples are used exclusively for the controller, are not passed on to third parties and are deleted together with the controller's data. The controller can deactivate this feature at any time in their dashboard.

Likewise, the processor may derive procedures from requests that the controller's staff have resolved (type of request, details needed from the customer, the team's steps, outcome) and store them in the controller's knowledge base ("learned procedures"). Recognisable personal data is removed before processing by AI systems and before storage; what is stored is the procedure without reference to individual customers, the number of cases, the team members involved and, for each case, an irreversible key that is deleted together with the conversation. No AI model is trained or changed in the process. Cases involving special categories of personal data (Art. 9 GDPR) and data from the Gmail API are not used; learning only uses conversations that started after the feature was turned on. The controller can deactivate the feature per channel and view, edit, pause and delete every procedure. If the system classifies a procedure as a rule that the team always applies, or applies under a specific condition, the AI assistant may mention its steps and outcome as long as the controller has turned learning on; without review by the team only if the procedure occurred at least three times and does not contradict the knowledge base. It mentions other procedures only with the controller's permission. The controller's return address named by the team may be stored with the procedure. A procedure that has not occurred again for twelve months is deleted.

If the controller has connected an Outlook or IMAP mailbox and learning from emails is turned on, the processor also uses replies that the controller's staff sent directly from that mailbox (sent items folder), under the same rules and only from the time the feature was turned on; mailboxes connected through Google's Gmail interface

(sign-in with Google) are excluded. If staff change an AI draft before sending it, the processor counts per controller, without any text, which kind of offer was removed or kept, and stops suggesting repeatedly removed offers on its own; information about customers' statutory rights is never suppressed by this. These counts are deleted after twelve months.

At the explicit request of a customer of the controller, the processor may send exactly one requested document per reply: files the controller has released for this purpose in its knowledge base, PDF files publicly available on the controller's website and – after verifying identity as for invoice information – invoices as PDF from the invoicing services the controller has connected. Knowledge base files that have not been released are not sent to customers. Every file sent is stored with the message in the conversation history and deleted together with the conversation.

Content generated by AI systems is produced automatically based on inputs provided by the Controller or its users.

The Processor makes no warranty as to the accuracy, completeness or legal admissibility of content generated by AI systems.

The Controller is responsible for reviewing the outputs of the systems and ensuring their use in compliance with applicable law.

Section 17 Entry into Force

This Data Processing Agreement shall enter into force automatically upon use of the Processor's services or upon execution of a corresponding master agreement between the Parties.