

Data Processing Agreement (DPA) pursuant to Article 28 of the GDPR

between the Customer (hereinafter referred to as the “Data Controller” or “Client”) and Pakera AI Packaging Optimization GmbH, Brunnenweg 35, 83666 Waakirchen, Germany (hereinafter referred to as “Pakera,” “Contractor,” or “Data Processor”)

Effective as of August 2026

Preamble

This Data Processing Agreement (DPA) specifies the parties’ data protection obligations in connection with the use of the Pakera SaaS platform in accordance with Pakera’s Terms and Conditions. It applies to all activities in which Pakera processes personal data on behalf of the Data Controller (Art. 4(8), Art. 28 GDPR).

The Data Controller is solely responsible for the lawfulness of the processing and for safeguarding the rights of data subjects (Art. 24 GDPR). Pakera processes personal data exclusively in accordance with documented instructions from the Data Controller, unless there is a legal obligation to process such data.

1. Subject Matter, Nature, and Purpose of the Processing

The subject matter and duration of the processing are set forth in the main contract (Terms and Conditions), the order form (if available), and correspond to the term of the contract. The nature and purpose of the processing, the type of personal data, and the categories of data subjects are described in Appendix 1.

2. Right of the Data Controller to Issue Instructions

2.1 Pakera processes personal data only within the scope of the agreements entered into and in accordance with the documented instructions of the controller, unless Pakera is legally obligated to process such data (in which case Pakera shall notify the controller of these requirements prior to processing, unless the law prohibits this due to an important public interest).

2.2 Instructions shall generally be provided in writing; verbal instructions must be confirmed in writing without delay. The provisions set forth in the main contract and in these General Terms and Conditions shall be deemed the initial instructions.

2.3 Pakera shall inform the controller immediately if it believes that an instruction violates the GDPR or other data protection regulations. Pakera is entitled to suspend the execution of the instruction in question until it is confirmed or amended.

3. Obligations of Pakera (Processor)

Pakera undertakes, in particular, to

- process personal data exclusively in accordance with Section 2;
- ensure that persons authorized to process data are bound by confidentiality obligations or are subject to an appropriate statutory duty of confidentiality (Art. 28(3)(b), Art. 29, Art. 32(4) of the GDPR);
- implement and comply with the technical and organizational measures (TOMs) required under Article 32 of the GDPR, as set forth in Annex 2;
- comply with the conditions for engaging additional processors (subprocessors) in accordance with Section 5;
- assist the controller, to the extent possible, with appropriate technical and organizational measures in fulfilling its obligation to respond to requests for the exercise of data subjects' rights (Chapter III of the GDPR) (Art. 28(3)(e) of the GDPR);
- assist the controller in complying with the obligations under Articles 32 through 36 of the GDPR (data security, notification of data breaches, data protection impact assessment, prior consultation), taking into account the nature of the processing and the information available to the processor (Article 28(3)(f) of the GDPR);
- at the controller's discretion, to delete or return all personal data upon completion of the processing services and to destroy any existing copies, provided there is no statutory retention obligation (Section 8);
- provide the controller with all necessary information to demonstrate compliance with the obligations under Article 28 of the GDPR and to facilitate and cooperate with audits pursuant to Section 7;
- appoint a data protection officer, to the extent required by law;
- maintain a record of all categories of processing activities carried out on behalf of the controller in accordance with Article 30(2) of the GDPR.

4. Technical and Organizational Measures (TOM)

Pakera shall implement the state-of-the-art technical and organizational measures described in **Annex 2**. Pakera is entitled to further develop and adapt these measures, provided that the agreed level of protection is not compromised. Significant changes must be documented.

5. Use of Additional Processors (Subprocessors)

5.1 The Data Controller grants its **general authorization** for the use of additional processors (subprocessors). The subprocessors in use at the time the contract is concluded are listed in **Annex 3** and are deemed to be authorized.

5.2 Pakera shall inform the Data Controller of any intended change regarding the engagement or replacement of subprocessors at least fourteen (14) days in advance

and shall give the Data Controller the opportunity to object to the change (Art. 28(2) GDPR). This information may also be provided via an up-to-date list of subprocessors in the Trust Center.

5.3 If the Controller objects to the change for an important data protection reason and no mutually agreeable solution can be found, the Controller shall have a special right of termination with respect to the affected service.

5.4 Pakera contractually obligates each subprocessor to comply with essentially the same data protection obligations as those set forth in these General Terms and Conditions (Art. 28(4) GDPR), in particular to provide sufficient guarantees regarding appropriate technical and organizational measures. In the case of subprocessors in third countries, Pakera ensures an adequate level of protection (e.g., adequacy decision or EU Standard Contractual Clauses along with supplementary measures, Art. 46 GDPR).

6. Reporting of Data Breaches

6.1 Pakera shall notify the controller of any personal data breach that has occurred within the scope of responsibility of Pakera or its sub-processors without undue delay after becoming aware of it, generally within 48 hours.

6.2 The notification shall contain at least the information required under Article 33(3) of the GDPR, to the extent known to Pakera. Pakera shall assist the controller in fulfilling its reporting and notification obligations to the supervisory authority (Article 33 of the GDPR) and to data subjects (Article 34 of the GDPR).

7. Inspection and Audit Rights

7.1 The controller has the right to verify compliance with the agreed-upon measures (Art. 28(3)(h) GDPR). Pakera shall provide the necessary information for this purpose and may provide evidence primarily through appropriate certifications, current attestations, or reports from independent bodies.

7.2 If documentation alone is insufficient to provide proof, the Data Controller may, upon timely notice (generally at least 30 days in advance), during normal business hours, without disrupting business operations, and no more than once a year (as well as on an ad hoc basis), conduct an on-site inspection or have it conducted by a third party bound by a confidentiality obligation. Each party shall bear its own costs; Pakera may reasonably invoice the Data Controller for any disproportionate expenses.

8. Deletion and Return Upon Termination of the Contract

8.1 Upon termination of the processing services, Pakera shall, at the Data Controller's discretion, either delete all personal data or return it and destroy any existing copies, provided there is no legal obligation to retain the data.

8.2 In accordance with the main contract, customer data will be irrevocably deleted after the expiration of a 30-day retrieval/return window following the end of the contract; within this window, the data controller may choose between deletion or return in accordance with Section 8.1. Exceptions include support tickets, data that must be retained for legal reasons (e.g., retention periods under commercial and tax law), and backup copies

that are periodically overwritten as part of the regular backup cycle. Until deletion, all data that has not yet been deleted remains subject to restricted processing and the provisions of these General Terms and Conditions.

8.3 Pakera shall provide evidence of the deletion or return in an appropriate form upon request.

9. Final Provisions

9.1 In the event of any conflict between this DPA and the General Terms and Conditions, the provisions of this DPA shall take precedence with regard to data protection regulations.

9.2 German law applies. The place of jurisdiction is Munich, to the extent permitted by law.

9.3 Should any individual provisions be invalid, the validity of the remaining provisions shall remain unaffected.

Attachment 1 – Description of Processing

Type of Processing: Collection, recording, storage, organization, structuring, adaptation, retrieval, consultation, use, disclosure (within the scope of approval processes), erasure, and destruction of personal data in connection with the operation of the Pakera SaaS platform.

Purpose of Processing: Provision and operation of the contractually agreed-upon SaaS services (packaging and logistics optimization), including user and rights management, authentication, creation and approval of packaging results/packing instructions as well as associated comment/approval functions, and support.

Type of personal data:

- User master data: Name, business email address, phone number, address, job title, employer/company name
- Access and authentication data: Login, encrypted password, OTP/token information, role/permission assignment;
- Usage and log data: IP address, device/browser information, log and access data, session data;
- Content-related data that may contain personal information (e.g., personal data inadvertently included in uploaded CAD/Office files, comments, and approval pages);
- Data of external participants in approval processes (e.g., name, email address for sending the approval link, comments).

Categories of data subjects: Employees and authorized users of the controller (Owners, Admins, Classified Users, Users), external participants in approval/commenting processes, and other individuals whose personal data may be contained in the uploaded content.

Note on special categories of data: The processing of special categories of personal data (Art. 9 GDPR) is not intended. The data controller ensures that no special categories of data are uploaded to the platform without a separate agreement.

Duration of processing: For the term of the main contract. The following retention periods apply to the project history: Unregistered use: no storage; Free: storage for 30 days, followed by automatic deletion; Pro: storage for 180 days, followed by automatic deletion; Business and Enterprise: permanent archiving of the project history or until the end of the subscription.

Attachment 2 – Technical and Organizational Measures (Art. 32 GDPR)

Confidentiality

- Access control: Hosting of core data in certified data centers in Germany (subprocessor, see Appendix 3) with access security, surveillance, and access logging by the data center operator.
- Access Control: Password-protected access; password storage in accordance with **Bcrypt**; one-time passwords (OTP) and passwords for registration, login, and the approval page; multi-factor authentication (MFA) and single sign-on (SSO).
- Access Control: Role-Based Access Control (RBAC) with the roles Owner, Admin, Classified User, and User; project-specific access restrictions for particularly sensitive/classified data (Enterprise); need-to-know principle for Pakera employees.
- Encryption: Transport encryption according to **TLS 1.3**; encryption of data at rest using **AES-256-GCM**; optional encryption of CAD data with a customer password (Bring Your Own Key)

Integrity

- **Input Control:** Logging of accesses and security-related events (access logs starting with the Business plan); traceability of approvals and their documentation/archiving.
- **Data Sharing Control:** Encrypted transmission; secure sharing links with access protection (OTP) and time limits.

Availability and Resilience

- Multi-redundant infrastructure with an uninterruptible power supply at the hosting subprocessor; target availability of 99.6% on an annual average.
- Regular data backups; protective measures against DDoS attacks via OVHcloud and/or Cloudflare.

Procedures for Regular Review, Assessment, and Evaluation

- Data protection management and review of measures; alignment with ISO/IEC 27001.
- Control of subcontractors through contractual obligations (see Appendix 3) and compliance with instructions.
- Incident response and reporting process in accordance with Section 6.

Attachment 3 – List of Subprocessors

This list includes processors that may process personal data on behalf of the controller in connection with the operation of Pakera. Other services, such as marketing and website services for which Pakera itself is the controller, are listed in the Privacy Policy.

Subprocessor	Purpose / Service	Headquarters / Location of Processing	Transfer Mechanism (for third countries)
OVH GmbH	Hosting, data center, infrastructure, DDoS protection	Germany, processing on servers in Germany	N/A
HubSpot Germany GmbH	CRM, Marketing	Germany, processing on servers in Germany	EU Standard Contractual Clauses + EU-US Data Privacy Framework, if applicable
Hanko GmbH	Authentication, Login, MFA/SSO	Germany, processing on servers in Germany	N/A
Cloudflare, Inc.	Bot/abuse protection, DDoS protection	USA, processing on global servers	EU Standard Contractual Clauses + EU-US Data Privacy Framework, if applicable
Microsoft Ireland Operations Ltd.	Email, website user analytics	USA, processing on servers in the EU	EU Standard Contractual Clauses + EU-US Data Privacy Framework, if applicable
Google Ireland Ltd.	Website user analytics	USA, processing on global servers	EU Standard Contractual Clauses + EU-US Data Privacy Framework, if applicable
PostHog, Inc.	Website user analytics	USA, processing on servers in Germany	EU Standard Contractual Clauses + EU-US Data Privacy Framework, if applicable

Subprocessor	Purpose / Service	Headquarters / Location of Processing	Transfer Mechanism (for third countries)
Brevo GmbH	Sending of transaction/system emails	Germany, processing on servers in Germany	N/A
FooMonk LLC (Instantly)	Email Outreach	U.S., processed on servers in the U.S.	EU Standard Contractual Clauses
Livestorm SAS	Webinars	France, processed on servers in Ireland	N/A
Tella HQ, Inc.	Video streaming	U.S., processed on servers in the U.S.	EU Standard Contractual Clauses
Framer B.V.	Marketing website hosting, analytics	Netherlands, processing on servers in the U.S.	EU-US DPF, if applicable; otherwise EU SCCs

Pakera AI Packaging Optimization GmbH · Brunnenweg 35, 83666 Waakirchen ·
info@pakera.com