

KOMBO DATA PROCESSING AGREEMENT

Effective Date: As defined in the Agreement

This DPA is entered into between:

This Global Data Processing Agreement ("**DPA**") is incorporated into and forms part of the Agreement between Kombo Technologies GmbH and Customer ("**you**," "**your**," or "**Customer**") as defined in the Terms of Service.

"**Kombo**," "**we**," "**us**," or "**our**" means Kombo Technologies GmbH, a German limited liability company registered at HRB 244447 B, Amtsgericht Charlottenburg, with offices at Rosenthaler Str. 72A, 10119 Berlin, Germany.

This DPA governs the processing of Covered Personal Information in connection with the Kombo Services and addresses requirements under applicable Privacy Laws, including the GDPR, UK GDPR, revFADP, BDSG, and other applicable regulations.

For additional security and compliance information, please visit our Security Portal at <https://security.kombo.dev>.

1. DEFINITIONS

1.1 General Definitions. Capitalized terms not defined in this DPA have the meanings given in the Agreement.

"**Agreement**" means the Master Service Agreement or other written agreement between Customer and Kombo Technologies GmbH governing Customer's use of the Kombo Services. "**Kombo**" means Kombo Technologies GmbH, as defined above. This DPA supplements and is incorporated into Section 6.4 of the Agreement. In the event of conflict between this DPA and Section 6.4, this DPA controls with respect to Covered Personal Information.

1.2 "Covered Personal Information" means personal data or personal information that is Customer Data and has been or will be provided or uploaded by Customer to the Kombo Services, processed by Kombo on behalf of Customer while using the Kombo Services, or otherwise made available to Kombo pursuant to the Agreement while using the Kombo Services. For avoidance of doubt, Covered Personal Information does not include Usage Data or any information that does not constitute "personal data" or "personal information" under applicable Privacy Laws.

1.3 "Data Subject" means an identified or identifiable natural person to whom Covered Personal Information relates.

1.4 "Privacy Laws" means applicable statutes, regulations or other laws pertaining to privacy or data protection, processing of personal information, and/or information security, including, but not limited to: the EU General Data Protection Regulation 2016/679 ("**GDPR**"); United Kingdom General Data Protection Regulation ("**UK GDPR**"); the revised Swiss Federal Act on Data Protection ("**revFADP**"); the **German Federal Data Protection Act ("BDSG")**; and any other applicable

federal, state, provincial, or local laws or regulations regarding information privacy that are in effect or will come into effect during the term of the Agreement.

1.5 "**Processing**" means any operation or set of operations performed on Covered Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.6 "**Sensitive Personal Information**" means, to the extent treated distinctly as a special category of personal information under Privacy Laws: (a) personal information that is genetic data, biometric data, data concerning health, a natural person's sex life or sexual orientation; (b) data about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; or (c) precise geolocation data.

1.7 "**Subprocessor**" means any third party appointed by or on behalf of Kombo to process Covered Personal Information.

1.8 **Jurisdictional Applicability.** The jurisdiction-specific provisions in Section 13 apply only to the extent Customer's use of the Services involves processing activities subject to the laws of that jurisdiction. Customer is responsible for determining which jurisdictions' laws apply to its processing activities.

2. DATA PROCESSING RELATIONSHIP

2.1 Roles and Responsibilities. Customer may either be controller or the processor in respect of its End Customers' personal data and Kombo Technologies GmbH is the processor ("*Auftragsverarbeiter*" under GDPR/BDSG) of Covered Personal Information under applicable Privacy Laws. Customer retains control of the Covered Personal Information and remains responsible for its compliance obligations under applicable Privacy Laws, including providing any required notices and obtaining any required consents.

Where Customer acts as a data processor (*Auftragsverarbeiter*) in respect of personal data of Data Subjects processed via the Kombo Services, Kombo Technologies GmbH acts as a sub-processor (*Unterauftragsverarbeiter*) within the meaning of Art. 28(4) GDPR. In such cases, Customer's processing instructions to Kombo are passed on from Customer's upstream data controllers (i.e., Customer's own clients). Kombo acknowledges this structure and agrees to process Covered Personal Information solely in accordance with such instructions. Where Customer acts as a data controller in its own right in respect of any Covered Personal Information, Kombo Technologies GmbH acts as a processor (*Auftragsverarbeiter*). The applicable role shall be determined by the nature of the processing activity as documented in Exhibit A.

2.2 Processing Instructions. Kombo processes Covered Personal Information only in accordance with Customer's documented instructions as set forth in this DPA and the Agreement, unless required to process such information by applicable law. If Kombo believes any instruction violates applicable Privacy Laws, Kombo will promptly notify Customer and may suspend execution of the instruction until Customer confirms or modifies it.

2.3 Upstream Controller Instructions. Where Customer acts as a data processor in respect of Covered Personal Information, Customer may issue supplementary processing instructions to

Kombo that reflect instructions received from Customer's upstream data controllers. Such supplementary instructions shall be treated as documented instructions for the purposes of Section 2.2 and Art. 28(3)(a) GDPR. Kombo shall comply with any such supplementary instructions within five (5) business days of receipt, or such shorter period as is required to enable Customer to comply with its own obligations to the upstream data controller, including obligations arising from data subject rights requests under Chapter III GDPR. Kombo shall promptly notify Customer if it considers that any supplementary instruction infringes applicable Privacy Laws

2.4 Processing Scope. The details of processing, including subject matter, duration, nature, purpose, categories of Covered Personal Information, and categories of Data Subjects, are set forth in Exhibit A attached hereto.

2.5 Sensitive Personal Information. If Customer intends to process Sensitive Personal Information via the Kombo Services, Customer must provide written notice to Kombo and ensure such processing complies with applicable Privacy Laws. Customer is solely responsible for providing specific processing instructions for such data.

2.6 Customer Processing Controls. Customer may configure certain processing parameters through the Kombo Services interface, including:

- Data retention periods (within applicable limits)
- Integration scope and field-level data mapping
- Access controls and user permissions
- Export and deletion requests

2.7 AI Apply Addendum. Where Customer elects to use Kombo's AI Apply feature, the processing of Covered Personal Information by the Subprocessors engaged for that feature is governed by the AI Apply Addendum, which supplements this DPA. The AI Apply Addendum is optional and applies only upon Customer's activation of the AI Apply feature. Customer's activation of AI Apply constitutes a documented instruction to engage the applicable AI Apply Subprocessors identified in the AI Apply Addendum as Subprocessors for the processing of Covered Personal Information. The AI Apply Addendum prevails over this DPA in respect of the processing of Covered Personal Information through AI Apply, including as regards the processing locations and transfer safeguards applicable to that feature.

3. DATA PROCESSING RESTRICTIONS

3.1 Processing Limitations. Kombo will not:

- (a) sell or share Covered Personal Information;
- (b) retain, use, or disclose Covered Personal Information for any purpose other than the limited purposes specified in the Agreement and this DPA; or
- (c) retain, use, or disclose Covered Personal Information for any purpose other than as specified in the Agreement and this DPA.

3.2 Confidentiality. Kombo will maintain the confidentiality of all Covered Personal Information and will not disclose it to third parties unless Customer or this DPA specifically authorizes the disclosure, or as required by law. If required by law to disclose Covered Personal Information, Kombo will first

inform Customer of the legal requirement and give Customer an opportunity to object or challenge the requirement, unless prohibited by law.

3.3 Employee Obligations. Kombo ensures that employees processing Covered Personal Information are informed of applicable Privacy Laws and bound by appropriate confidentiality obligations during and after their employment.

4. SUBPROCESSORS

4.1 General Authorization. Customer hereby provides general authorization for Kombo to engage Subprocessors to process Covered Personal Information. The following Subprocessors are engaged by Kombo Technologies GmbH as of the Effective Date and are deemed approved by Customer upon execution of the Agreement:

Provider	Purpose	Region ¹	Scope
End Customer Data			
Google Cloud Platform	Cloud Provider	Netherlands	End Customer and Customer Data
Hetzner	Cloud Provider (only used in select cases for serving static IPs when making requests to APIs)	Germany	End Customer and Customer Data
Customer Data²			
Pylon	Customer support ticketing (does not process data of end-customer except when they create tickets directly with Kombo, which is very rarely the case and can be disabled)	USA	Customer Data; no End Customer Data
Frontegg	Authentication of Kombo users towards the Kombo Dashboard	Ireland / us-east / Canada	Customer Data; no End Customer Data
Stripe	Payment information. PII is only limited to the billing email, in case it's a personal email and not a generic email such as billing@company.com	USA	Customer Data; no End Customer Data

¹ The region depends on the Customer's location and decision. Kombo can offer those regions identified in this Section.

² "Customer Data" in this Section refers to data that Kombo collects and processes in connection with the customer relationship (e.g., Customer's business contact name and email address for account management, support, authentication, and billing purposes). These Subprocessors do not process End Customer Data (i.e., data originating from Customer's end users that is processed through the Tool). Customer Data processed by these Subprocessors does not constitute Covered Personal Information under this DPA.

An updated list of Subprocessors is maintained in Kombo's Security Portal at <https://security.kombo.dev>.

Where Customer activates AI Apply, the Subprocessors identified in the AI Apply Addendum are engaged in addition to those listed above for the purposes of that feature. Kombo maintains the current list of those Subprocessors, together with their processing locations, in the Security Portal.

4.2 Subprocessor Changes. Kombo will provide at least thirty (30) days' prior written notice of any intended changes concerning the addition or replacement of Subprocessors by updating the Security Portal and providing email notification to Customer's designated contact. Where reasonably practicable, Kombo will endeavour to provide such notice earlier than thirty (30) days in advance. Such notice constitutes Kombo's fulfillment of its notification obligation, and no additional consent or approval from Customer is required unless Customer exercises its objection rights under Section 4.3.

4.3 Objection Rights. Customer may object in writing to any new or replacement Subprocessor on reasonable data protection grounds within thirty (30) days of receiving notice. The objection must specify the data protection concerns that form the basis of the objection. If Customer timely objects on reasonable grounds, Kombo will use commercially reasonable efforts to: (a) make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid processing of Covered Personal Information by the objected-to Subprocessor; or (b) provide an alternative solution. If Kombo is unable to provide an alternative within sixty (60) days of Customer's objection, Customer may terminate the affected Services by providing written notice to Kombo, and Customer will receive a pro-rata refund of any prepaid fees for the terminated Services covering the remainder of the then-current term.

4.4 Subprocessor Obligations. Kombo ensures all Subprocessors are bound by written agreements requiring them to provide at least the same level of data protection as required under this DPA and applicable Privacy Laws. Kombo remains fully liable to Customer for the performance of any Subprocessor's obligations under this DPA.

5. SECURITY MEASURES

5.1 Technical and Organizational Measures. Kombo implements and maintains appropriate technical and organizational measures to ensure processing complies with Privacy Laws and protects Data Subject rights. These measures ensure appropriate security of processing, including confidentiality, integrity, availability, and resilience of systems processing Covered Personal Information. Such measures meet or exceed applicable industry standards, as evidenced by Kombo's ISO/IEC 27001 certification and SOC 2 Type II report.

5.2 Security Standards. Kombo maintains information security practices and controls as detailed in Exhibit B and the Security Portal at <https://security.kombo.dev> including but not limited to:

- Encryption of data at rest using AES-256 or equivalent
- Encryption of data in transit using TLS 1.2 or higher
- Role-based access control with principle of least privilege
- Multi-factor authentication for all system access
- Regular penetration testing by qualified third parties

- Centralized vulnerability management and patch procedures
- Regular automated backups (3-2-1 backups)
- Security monitoring and incident response capabilities

5.3 Security Certifications. Kombo maintains SOC 2 Type II and ISO 27001:2013 certifications applicable to Kombo Technologies GmbH operations. Current certification documentation is available through the Security Portal.

5.4 Security Updates. Technical and organizational measures may be updated to reflect technological developments and evolving security threats, provided the updated measures maintain at least the same level of security. Material changes will be documented and communicated to Customer.

6. DATA SUBJECT RIGHTS

6.1 Data Subject Requests. Kombo will promptly notify Customer within forty-eight (48) hours if it receives any request from a Data Subject to exercise rights under Privacy Laws regarding their Covered Personal Information. Kombo will provide Customer with all relevant documentation and correspondence related to such requests and will not respond directly to the Data Subject without Customer's prior written authorization.

6.2 Assistance with Rights. Taking into account the nature of processing, Kombo will assist Customer by implementing appropriate technical and organizational measures, insofar as reasonably practicable, to help Customer fulfill its obligations to respond to Data Subject requests under Privacy Laws, including requests for:

- Access to personal information
- Correction or rectification of inaccurate data
- Deletion or erasure of personal information
- Restriction of processing
- Data portability
- Objection to processing

6.3 Data Protection Impact Assessments. Upon Customer's reasonable request, Kombo will provide assistance and information reasonably necessary to enable Customer to conduct data protection impact assessments and consultations with supervisory authorities as required by applicable Privacy Laws.

6.4 Data Retention. Kombo retains Covered Personal Information only for as long as necessary to fulfill the purposes outlined in this DPA and the Agreement, or as required by applicable law. Specific retention periods are:

- Active customer data: Duration of Agreement
- Backup data: Fifteen (15) days after deletion from production systems
- Log data:
 - Audit logs: Twelve (12) months
 - Debug logs: Up to one (1) month
- Audit trails: As required by applicable law, or seven (7) years, whichever is longer

7. SECURITY INCIDENTS AND BREACH NOTIFICATION

7.1 Incident Notification. Kombo will notify Customer without undue delay upon becoming aware of any confirmed unauthorized access, destruction, use, modification, or disclosure of Covered Personal Information (a "**Security Incident**").

7.2 Incident Response Timeline. Following discovery of a Security Incident, Kombo will:

- Initial notification: Within 72 hours of discovery
- Preliminary assessment: Within 72 hours, including affected data categories and estimated number of Data Subjects
- Root cause investigation report: Within 10 business days
- Preliminary remediation plan: Within 15 business days, including measures to prevent recurrence

7.3 Incident Information. Kombo will provide Customer with information and cooperation reasonably requested regarding Security Incidents, including:

- Description of the nature of the Security Incident
- Categories and approximate number of Data Subjects affected
- Categories and approximate number of Covered Personal Information records affected
- Likely consequences of the Security Incident
- Measures taken or proposed to address the Security Incident and mitigate potential adverse effects

7.4 Third-Party Notification. Kombo will not inform any third party of Security Incidents involving Covered Personal Information without Customer's prior written consent, except as required by law. Customer has the sole right to determine whether to notify Data Subjects, supervisory authorities, or other parties as required by law.

8. CROSS-BORDER DATA TRANSFERS

8.1 Data Processing Location.

Covered Personal Information is processed and stored in the European Union using Google Cloud infrastructure located in the EU (Germany/Ireland).

By using the Kombo Services and entering into this DPA, Customer authorizes processing and storage in the European Union.

8.2 Limited Cross-Border Transfers. Notwithstanding Section 8.1, Covered Personal Information may be accessed or processed outside the primary storage location in limited circumstances, including:

- (a) Technical support and incident response by Kombo personnel located in Germany;
- (b) Use of Subprocessors as listed in Section 4.1 and the Security Portal;
- (c) Backup and disaster recovery operations; or
- (d) As necessary to provide the Kombo Services or comply with legal obligations.

8.3 Safeguards for International Transfers.

(a) Transfers within adequate jurisdictions: Where transfers occur between jurisdictions recognized as providing adequate data protection (e.g., within the EEA, or pursuant to adequacy decisions), no additional safeguards are required beyond those set forth in this DPA.

(b) Transfers to Subprocessors in third countries: Where Kombo transfers Covered Personal Information to a Subprocessor established in a country that is not the subject of an adequacy decision, such transfer is governed by the Standard Contractual Clauses (Module Three, processor to processor) concluded between Kombo and that Subprocessor, with Kombo as data exporter and the Subprocessor as data importer, together with any supplementary measures identified in Kombo's transfer impact assessment.

(c) Other international transfers: For any other cross-border transfers, Kombo implements appropriate safeguards as required by applicable Privacy Laws.

8.4 Standard Contractual Clauses. For the purposes of this Section 8, "Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to third countries pursuant to European Commission Implementing Decision (EU) 2021/914, as amended or replaced. Where the Standard Contractual Clauses apply: Module Three (processor to processor) applies where Kombo transfers Covered Personal Information to a Subprocessor; the optional docking clause (Clause 7) does not apply. The optional clause for advance notice of Subprocessor changes (Clause 9(a), Option 2) applies with a thirty (30) day notice period; the governing law is the law of Germany and the competent courts are the courts of Berlin, Germany. For transfers from the United Kingdom, the UK International Data Transfer Addendum to the Standard Contractual Clauses applies. For transfers from Switzerland, the Standard Contractual Clauses apply with references to the GDPR read as references to the revFADP and with the Swiss Federal Data Protection and Information Commissioner as competent supervisory authority.

8.5 Transfer Impact Assessment. Kombo documents an assessment of the transfers described in this Section 8 and makes it available to Customer on request. Kombo will not transfer Covered Personal Information to a Subprocessor established in a third country unless a valid transfer mechanism under Chapter V GDPR is in force for that transfer.

9. AUDIT AND COMPLIANCE

9.1 Audit Rights. Customer has the right to audit or appoint an independent third-party auditor to audit Kombo's compliance with this DPA, provided such audits:

- (a) do not unreasonably interfere with Kombo's business operations;
- (b) are conducted during normal business hours with at least thirty (30) days' prior written notice;
- (c) are limited to once per twelve (12) month period, unless (i) required by applicable law, (ii) requested by Customer's regulatory authority, or (iii) following a Security Incident affecting Customer's Covered Personal Information; and
- (d) are subject to reasonable confidentiality obligations.

Customer will in the first instance exercise its audit rights by reviewing Kombo's SOC 2 Type II report, ISO 27001 certification and the further documentation made available through the Security

Portal, which Kombo will update and make available at least annually. An on-site or bespoke audit may be requested only where that documentation is insufficient to address a specific compliance concern that Customer has identified in writing, or where an audit is required by applicable law, requested by a competent supervisory authority, or follows a Security Incident affecting Customer's Covered Personal Information. Audits are conducted remotely wherever the audit objective can reasonably be achieved remotely, at Customer's cost, and do not extend to the data of other Kombo customers, to Kombo's confidential information, or to information whose disclosure would compromise the security of the Kombo Services.

9.2 Compliance Documentation. Upon reasonable request, Kombo will make available information necessary to demonstrate compliance with this DPA and applicable Privacy Laws. Kombo maintains SOC 2 Type II and ISO 27001:2013 certifications, which are available through Kombo's Security Portal at <https://security.kombo.dev>. Customer may review these certifications and compliance reports in lieu of conducting on-site audits, unless required by applicable law or following a Security Incident.

9.3 Data Protection Officer. Kombo's data protection contact information is provided in Exhibit A. For data protection inquiries, contact security@kombo.dev.

10. REGULATORY INQUIRIES

10.1 Regulatory Cooperation. If Kombo receives any regulatory inquiry, investigation, or request from a supervisory authority regarding Covered Personal Information, Kombo will, to the extent not prohibited by law:

- Promptly notify Customer of the inquiry within forty-eight (48) hours
- Provide Customer with copies of relevant documents and correspondence
- Not disclose Customer's confidential information without prior written consent
- Take necessary measures to respond appropriately and timely
- Cooperate with Customer's legal counsel in formulating responses

10.2 Customer Regulatory Obligations. Customer acknowledges that it remains responsible for compliance with all applicable Privacy Laws and regulatory requirements. Kombo's cooperation under this Section does not transfer any regulatory obligations from Customer to Kombo.

11. TERM AND DATA RETURN

11.1 Term. This DPA remains in effect for the duration of the Agreement and terminates automatically upon termination of the Agreement, except for provisions that expressly survive termination.

11.2 Data Return and Deletion. Upon termination of the Agreement, Kombo will, at Customer's choice, return or delete all Covered Personal Information, including copies, unless applicable law requires continued storage. Customer must make this election in writing within thirty (30) days of termination. If no election is made, Kombo will delete all Covered Personal Information without undue delay after termination.

11.3 Certification of Deletion. Upon Customer's written request, Kombo will provide written certification that all Covered Personal Information has been returned or deleted in accordance with this Section, except where retention is required by applicable law. Such certification will identify any data retained and the legal basis for retention.

11.4 Subprocessor Data Handling. Kombo will ensure that all Subprocessors return or delete Covered Personal Information in accordance with the same requirements applicable to Kombo under this Section.

11.5 Post-Termination Assistance. For a period of thirty (30) days following termination, Kombo will provide reasonable assistance to Customer in retrieving Covered Personal Information at no additional charge. Assistance beyond thirty (30) days or requiring significant custom development may be subject to Kombo's then-current professional services rates.

12. LIABILITY AND INDEMNIFICATION

12.1 Incorporation of Agreement Terms. All liability, indemnification, limitation of liability, and related provisions in the Agreement apply to this DPA and any claims arising under or related to this DPA.

12.2 Allocation of Responsibility. (a) Kombo's Responsibility: Kombo is responsible for compliance with its obligations as a processor under this DPA, including implementing appropriate security measures and processing data only as instructed. (b) Customer's Responsibility: Customer is solely responsible for: ensuring it has a lawful basis to provide Covered Personal Information to Kombo; providing required notices and obtaining required consents from Data Subjects; and Customer's own compliance with Privacy Laws as a controller. (c) No Liability for Customer Actions: Kombo has no liability for violations arising from Customer's instructions, Customer's configurations, Customer's failure to obtain required consents, or Customer's failure to comply with its obligations under this DPA or Privacy Laws.

12.3 Regulatory Fines. Each party is responsible for regulatory fines and penalties imposed directly on that party by a supervisory authority. The Agreement's liability limitations apply to all other claims, including claims for damages, third-party claims, and consequential damages.

13. JURISDICTION-SPECIFIC REQUIREMENTS

13.1 General Applicability. The provisions of Sections 1-12 of this DPA establish a comprehensive global framework for data protection that applies to all Customers regardless of jurisdiction. This Section 13 provides additional jurisdiction-specific requirements, clarifications, and modifications. Where this Section conflicts with earlier provisions, this Section controls for the specified jurisdiction. Customers should review the subsection(s) applicable to their jurisdiction and may disregard non-applicable provisions.

13.2 EUROPEAN ECONOMIC AREA, UNITED KINGDOM, AND SWITZERLAND

13.2.1 Applicability. This Section applies to Customers contracting with Kombo Technologies GmbH who are established in the European Economic Area, United Kingdom, or Switzerland, or who process personal data of data subjects in these jurisdictions.

13.2.2 Applicable Laws. The following laws apply in addition to the general provisions of this DPA:

- EU/EEA: General Data Protection Regulation (GDPR) 2016/679
- Germany: GDPR and German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG)
- United Kingdom: UK GDPR and Data Protection Act 2018
- Switzerland: Revised Swiss Federal Act on Data Protection (revFADP), effective September 1, 2023

13.2.3 Terminology. Under these laws:

- Customer is the "controller" (Verantwortlicher / responsable du traitement)
- Kombo Technologies GmbH is the "processor" (Auftragsverarbeiter / sous-traitant)
- Processing is conducted as specified in Section 2 of this DPA

13.2.4 Supervisory Authorities. The competent supervisory authorities are:

- EU/EEA: Data protection authority of Customer's establishment or Data Subject's habitual residence under GDPR Article 56
- Germany: Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI) or relevant state data protection authority
- United Kingdom: Information Commissioner's Office (ICO)
- Switzerland: Swiss Federal Data Protection and Information Commissioner (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter / Préposé fédéral à la protection des données et à la transparence - FDPIC)

13.2.5 Cross-Border Data Transfers. International data transfers are governed by Section 8 of this DPA, with the following jurisdiction-specific mechanisms:

- EU/EEA to non-adequate countries: Appropriate safeguards as required by applicable law
- UK to non-adequate countries: UK International Data Transfer Agreement (IDTA) or other UK-recognized transfer mechanisms
- Switzerland to non-adequate countries: Appropriate transfer mechanisms as required by the revFADP

13.2.6 German-Specific Requirements. For processing activities conducted by Kombo Technologies GmbH in Germany:

(a) Employee Data Protection: Processing of employee data of German residents is subject to BDSG § 26, which requires:

- Legitimate interests assessment for employee data processing
- Enhanced employee rights and transparency
- Works council consultation where applicable (Customer's responsibility to confirm compliance before providing employee data)

(b) Documentation: Additional documentation requirements under BDSG apply to records of processing activities maintained by Kombo Technologies GmbH.

(c) Language: Upon request, Kombo will provide German-language translations of this DPA and related documentation for German supervisory authorities or data subjects.

13.2.7 UK-Specific Requirements. For processing activities involving UK personal data:

(a) Post-Brexit Framework: Kombo acknowledges that UK data protection law has diverged from EU GDPR following Brexit and monitors UK regulatory developments.

(b) ICO Guidance: Kombo has regard to ICO statutory codes of practice and guidance where applicable to the Services, including guidance on AI and data protection.

(c) UK Transfer Mechanisms: Transfers from the UK are governed by UK-recognized mechanisms, including the UK IDTA or other appropriate safeguards.

13.2.8 Swiss-Specific Requirements. For processing activities involving Swiss personal data:

(a) Stricter Consent Standards: Where consent is the legal basis for processing, Kombo processes data only in accordance with valid consent meeting revFADP standards (explicit, informed, freely given, and specific).

(b) Automated Individual Decision-Making: Kombo does not carry out automated individual decision-making or profiling within the meaning of Article 21 revFADP. Where Customer uses the Kombo Services as an input to its own automated decision-making, Kombo will provide the information reasonably necessary for Customer to meet its disclosure obligations.

(c) High-Risk Breach Notification: For Security Incidents creating high risk to personality or fundamental rights of Swiss data subjects, Kombo provides information necessary for Customer to notify FDPIC as soon as possible.

(d) Language: Upon request, Kombo will provide French, German, or Italian translations of this DPA for Swiss supervisory authorities or data subjects.

14. ASSIGNMENT AND NOVATION

14.1 Assignment by Customer. Customer may, without Kombo's prior consent, assign or novate this DPA (together with the Agreement) to any entity that is a direct or indirect parent, subsidiary, or affiliate of Customer (a 'Group Company'), provided that: (a) Customer provides Kombo with written notice of the assignment or novation at least thirty (30) days in advance; (b) the assignee Group Company assumes in writing all of Customer's obligations under this DPA and the Agreement with effect from the date of assignment or novation; and (c) the assignment or novation does not result in Covered Personal Information being transferred to a jurisdiction that would require additional safeguards not already in place under this DPA. Upon completion of a valid assignment or novation under this Section, Customer is released from its obligations under this DPA and the Agreement to the extent assumed by the assignee Group Company.

14.2 Continuity of Data Protection Obligations. Any assignment or novation under this Section shall not affect the data protection obligations set out in this DPA, which shall continue in full force and effect and shall be binding on the assignee as if it were the original party.

15. MISCELLANEOUS

15.1 Conflict. In case of conflict between this DPA and the Agreement, this DPA prevails with respect to the processing of Covered Personal Information.

15.2 Amendments. This DPA may only be amended by written agreement signed by both parties, except that Kombo may update this DPA to comply with applicable Privacy Laws by providing thirty (30) days' prior notice to Customer. Material changes require Customer's affirmative acceptance; non-material changes (e.g., updated subprocessor list, corrected typos, clarifications) may be implemented with notice only.

15.3 Severability. If any provision of this DPA is held invalid or unenforceable, the remainder of this DPA remains in full force and effect, and the invalid provision will be replaced with a valid provision that most closely reflects the original intent of the parties.

14.4 Governing Law.

This DPA is governed by the laws of Germany, without regard to conflicts of law principles.

15.5 Survival. The following sections survive termination of this DPA: Section 7 (Security Incidents), Section 11 (Data Return), Section 12 (Liability and Indemnification), and Section 15 (Miscellaneous).

15.6 Entire Agreement. This DPA, together with the Agreement and its incorporated documents, constitutes the entire agreement between the parties regarding the processing of Covered Personal Information and supersedes all prior agreements, understandings, and communications regarding such subject matter.

15.7 Notices. All notices under this DPA must be in writing and delivered in accordance with the notice provisions in the Agreement. Notices regarding Security Incidents or regulatory inquiries may be provided by email to Customer's designated contact and will be deemed effective upon transmission.

15.8 No Third-Party Beneficiaries. This DPA is solely for the benefit of the parties and does not create any third-party beneficiary rights, except that Data Subjects may enforce certain provisions as third-party beneficiaries to the extent required by applicable Privacy Laws.

EXHIBIT A

PROCESSING DETAILS

PART 1: ENTITY-SPECIFIC INFORMATION

The following information applies to Kombo Technologies GmbH:

KOMBO TECHNOLOGIES GMBH

Applicable Regions: European Union, United Kingdom, Switzerland, Asia-Pacific

Kombo Entity Information:

- **Legal Name:** Kombo Technologies GmbH
- **Jurisdiction:** Germany
- **Registration:** HRB 244447 B, Amtsgericht Charlottenburg, Berlin
- **Address:** Rosenthaler Str. 72A, 10119 Berlin, Germany
- **Role:** Processor (Auftragsverarbeiter under GDPR/BDSG)

Primary Data Processing Location:

- **Country:** Germany
- **Infrastructure:** Google Cloud - Germany and EU regions
- **Secondary Locations** (optional): Customer's country/region where technically feasible
- **Access Points:** Germany (primary operations)
- **Backup Locations:** AWS regions within primary and secondary processing locations

Governing Law and Jurisdiction:

- **Governing Law:** Laws of Germany
- **Jurisdiction:** Courts of Berlin, Germany
-

Competent Supervisory Authority:

- Determined by Customer's location and applicable Privacy Laws:
 - **Germany:** Berliner Beauftragte für Datenschutz und Informationsfreiheit or relevant state data protection authority
 - **EU/EEA:** Data protection authority of Customer's establishment or Data Subject's habitual residence under GDPR Article 56
 - **United Kingdom:** Information Commissioner's Office (ICO)
 - **Switzerland:** Swiss Federal Data Protection and Information Commissioner (FDPIC)
 - **Other jurisdictions:** As determined by Customer's location and applicable Privacy Laws

PART 2: COMMON PROCESSING INFORMATION

The following applies to all Customers regardless of contracting entity:

Subject Matter: Processing of Covered Personal Information in connection with the provision of Kombo Services as described in the Agreement, including the facilitation of seamless data

synchronization, standardization, and transfer between the Customer's applications and various third-party IT systems.

Duration: For the term of the Agreement and as necessary to fulfill post-termination obligations, including data return, deletion, and regulatory retention requirements.

Nature and Purpose of Processing:

- Facilitating the seamless transfer and synchronization of data between Customer's applications and various IT systems.
- Converting disparate data formats from various third-party providers into a standardized schema for Customer use.
- Providing automated notifications and data updates regarding changes in connected third-party systems.
- Enabling the setup, authentication, and maintenance of API connections (links) between End Customers and the Kombo platform (Tool).
- Customer support and technical assistance provided by personnel in Germany
- Technical support by Kombo personnel
- Service improvement, optimization, and product development
- Compliance with legal obligations and regulatory requirements
- Security monitoring and incident response
- Internal administrative purposes (consolidated reporting, group-wide security monitoring)
- Backup and disaster recovery operations

Categories of Data Subjects:

- End Customer's employees, applicants and customers (end users), End Customers and Customers
- Individuals whose data is processed through Customer's use of the Kombo Services
- Customer's employees and Authorized Users (for account management and system access)

Categories of Covered Personal Information:

Identity Data:

- Full name, date of birth, government-issued identification numbers
- Social Security Numbers, Tax Identification Numbers, or other national identifiers (e.g., National Insurance Number in UK, Sozialversicherungsnummer in Germany)
- Addresses (residential, business, mailing, historical addresses)
- Contact information (email addresses, phone numbers, mobile numbers)
- Photographs and identity verification documents
- Digital identity verification data (biometric templates where permitted)

HR Data:

- Payroll information
- Employment status
- CVs, employment history, reference letters
- Salary, bonuses, equity grants, and currency.
- Manager IDs, department names, and team structures.
- Leave requests, holiday balances, and work schedules.

- Health insurance plans or retirement contribution details.

Demographic Data:

- Age, gender, marital status, family composition
- Geographic location and residency status
- Employment status, occupation, and employer information
- Education level and professional qualifications
- Household composition and dependent information

Behavioral Data:

- Usage patterns and service interactions
- Preferences, settings, and configuration choices
- Communication history with Customer
- Synchronisation and integration records relating to a Data Subject's record (e.g. sync status, error and reconciliation logs)

Technical Data:

- IP addresses and device identifiers
- Browser type, version, and operating system
- Log data, session information, and timestamps
- Cookies and tracking identifiers (where permitted)
- Geolocation data (where permitted and necessary to provide or secure the Services)
- API usage data and system performance metrics

Sensitive Personal Information: Only processed if specifically authorized by Customer in writing and in compliance with applicable Privacy Laws. Customer must provide explicit notice and obtain appropriate legal basis before submitting any Sensitive Personal Information to the Kombo Services. Processing of special categories of data under GDPR Article 9 or equivalent categories under other applicable Privacy Laws requires Customer's express written authorization and appropriate legal basis.

PART 4: CONTACT INFORMATION

Security and Data Protection Contact:

- Data Protection Officer: Fresh Compliance
 Email: dsb@freshcompliance.de
 Phone: [+49 30 327 657 51](tel:+493032765751)
- Email: security@kombo.dev
- Privacy Policy: <https://www.kombo.dev/privacy-policy>
- Security Portal: <https://security.kombo.dev>

Kombo Technologies GmbH Contact:

- Address: Rosenthaler Str 72A, 10119 Berlin, Germany
- Registration: HRB 244447 B, Amtsgericht Charlottenburg
- Legal Entity: German Limited Liability Company (Gesellschaft mit beschränkter Haftung)
- General Inquiries: contact@kombo.dev

PART 5: COMPLIANCE CERTIFICATIONS

Applicable to Kombo Technologies GmbH:

- SOC 2 Type II - Available through Security Portal
- ISO 27001:2013 - Available through Security Portal
- GDPR Compliance Framework - Kombo Technologies GmbH and applicable cross-border transfers
- Digital Operational Resilience Act (DORA) compliance framework

Certification Access: Current certifications and compliance reports are available through the Security Portal at <https://security.kombo.dev>. Enterprise customers may request additional compliance documentation through their account representative.

Audit Rights: Customer audit rights are governed by Section 9 of this DPA and may be satisfied through review of available certifications and compliance reports.

EXHIBIT B

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

I. Technical and organizational measures

Kombo Technologies GmbH is ISO27001 certified and maintains a SOC 2 Type II report. Detailed information about Technical and Organizational Security Measures are provided under the URL security.kombo.dev. Kombo operates no data centre of its own. All processing of personal data takes place in the data centres of Kombo's infrastructure providers (Google Cloud Platform and Hetzner), which are certified to ISO 27001 and comparable standards. Where the measures below are provided by those providers, this is indicated.

1. Pseudonymisation and Encryption, Art. 32 para 1 point a GDPR

Pseudonymisation contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- Encryption of data at rest: all personal data stored in production databases and object storage, and all backup copies, are encrypted using AES-256 or an equivalent algorithm
- Full-disk encryption on all employee laptops and mobile devices used to access Kombo systems, enforced through device management
- Encryption of data in transit: TLS 1.2 or higher for all connections between clients, Kombo systems and external systems, including internal service-to-service communication
- Key management through the infrastructure provider's key management service, with access to keys restricted to a defined group of administrators
- Pseudonymisation: personal data is referenced through internal identifiers, and identifying fields are masked or removed in application logs and traces
- Separate storage of the additional information required to re-identify pseudonymised data, subject to the access controls set out in Section 2.1

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, Art. 32 para 1 point b GDPR

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorized or unlawful processing and integrity and availability by measures to protect against accidental loss, destruction or damage.

2.1 Confidentiality

2.1.1. Physical access control

Measures that prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- Physical access control systems
- Definition of authorized persons; management and documentation of individual authorizations
- Regulation of visitors and external staff

- Monitoring of all facilities housing IT systems
- Logging of physical access
- Data centre security provided by the infrastructure providers: 24/7 on-site security personnel, video surveillance, intrusion detection and alarm systems, multi-factor physical access control and perimeter protection
- Kombo office premises: electronic access control, visitor registration and accompaniment of external staff
- Regular review of the infrastructure providers' certifications and audit reports covering physical security

2.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorization.

- User Authentication by simple authentication methods (using username/password), including two-factor authentication where adequate
- Secure transmission of credentials (using TLS)
- Automatic account locking
- Suspending inactive sessions
- Guidelines for handling passwords and certificates
- Definition of authorized persons
- Managing means of authentication
- Access control to infrastructure that is hosted by cloud service provider
- In-time revocation of access for people who no longer need access / leave the company
- Unique credentials per user

2.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage.

- Automatic and manual locking
- Access right management including authorization concept, implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.

2.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Network separation
- Segregation of responsibilities and duties
- Documentation of interfaces and of the personal data fields transferred through them
- Document procedures and applications for the separation

2.1.5 Control of instructions (order control)

Measures that ensure that personal data processed on behalf of a controller is processed only in accordance with that controller's documented instructions.

- Training and confidentiality agreements for internal staff and external staff

- Information security assessment for vendors/partners
- Written data processing agreements with all subprocessors, imposing obligations no less protective than those Kombo owes its customers
- Processing only on documented instructions; a documented escalation procedure where an instruction is considered to infringe data protection law
- Maintained subprocessor list with at least thirty (30) days' advance notice of additions or replacements and a customer objection right
- Standard Contractual Clauses and documented transfer impact assessments for subprocessors in third countries
- Records of processing activities maintained under Art. 30 GDPR
- Designated data protection contact and defined responsibilities for handling controller instructions and data subject requests
- Periodic review of subprocessor performance and security posture

2.2. Integrity

2.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- Secure transmission between client and server and to external systems by using industry-standard encryption
- Secure network interconnections ensured by Firewalls, anti-virus programs, routinely patching software etc.
- Logging of transmissions of data from IT system that stores or processes personal data
- Implementation of transport policies governing the transfer and carriage of data media and devices

2.2.2 Data input control

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Logging authentication and monitored logical system access
- Logging of data access including, but not limited to access, modification, entry and deletion of data
- Documentation of data entry rights and partially logging security related entries.

2.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Backup Concept
- Protection of stored backup media

- Data centre infrastructure provided by the infrastructure providers: uninterruptible power supply and redundant power feeds, climate control and temperature monitoring, early fire detection and automatic fire suppression, and water detection
- Redundant deployment across separate availability zones within the selected region
- Continuous availability and capacity monitoring
- Protection against denial-of-service attacks at the infrastructure provider level
- Documented incident response process with defined severity levels and escalation paths

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, Art. 32 para 1 point c GDPR

Organizational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- Continuity planning (Recovery Time Objective)
- Backup concept following the 3-2-1 principle: backups are held on separate systems and in a physically separate location from the production environment, so that no single fire compartment or site holds both
- Backups are encrypted at rest and subject to the same access controls as production data
- Regular restore tests to verify that backups can in fact be restored, with the results documented
- Documented Recovery Time Objective and Recovery Point Objective, and a disaster recovery plan that is reviewed and tested at least annually
- Defined retention periods for backup data, as set out in the Data Processing Agreement

4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing, Art. 32 para 1 point d GDPR

Organizational measures that ensure the regular review and assessment of technical and organizational measures.

- Testing of emergency equipment
- Internal assessments
- Continuous automated vulnerability scanning of infrastructure and application dependencies, with defined remediation deadlines by severity
- Penetration testing by qualified independent third parties at least annually and after significant changes to the architecture
- ISO 27001 certification with annual surveillance audits, and an annual SOC 2 Type II examination by an independent auditor
- Internal audit programme and annual management review of the information security management system
- Centralised patch management with defined timelines
- Review of these technical and organizational measures at least annually and following material changes to the processing

II. Organizational measures and governance

Measures that establish the organizational framework within which the technical measures under Section I operate.

- Information security management system certified to ISO 27001, with documented policies covering access control, cryptography, secure development, change management, supplier management and incident response
- Designated data protection contact reachable at security@kombo.dev, and defined internal responsibilities for data protection
- Confidentiality undertakings for all personnel with access to personal data, surviving the end of employment
- Security and data protection training for all personnel at onboarding and at regular intervals thereafter
- Documented onboarding and offboarding procedures, including timely revocation of access
- Data protection by design and by default considered in the development process, including data minimisation and defined retention periods
- Documented process for handling data subject requests and for notifying security incidents within the timelines set out in the Data Processing Agreement

EXHIBIT C

DATA PROCESSING IMPACT ASSESSMENT SUPPORT

Kombo provides the following information to support Customer's data protection impact assessments (DPIAs) as required by GDPR Article 35 and equivalent provisions under other Privacy Laws:

1. PROCESSING OPERATIONS

Nature of the Processing:

- Transfer and synchronisation of HR, recruiting and employment data between Customer systems and third-party HR systems on Customer's documented instructions
- Large-scale processing of special categories of data (if authorized by Customer)
- Processing of employment-related data on a large scale, depending on Customer's use case

Processing Characteristics:

- Scale: high-volume, continuous synchronisation of records across connected systems
- Automation: automated data transfer and format standardisation. Kombo does not evaluate, score, rank or filter Data Subjects and takes no decisions concerning them
- Data Sensitivity: identity, employment and HR data, and special categories only where submitted by Customer
- Data Subjects: employees, applicants and candidates of Customer and its End Customers, and Customer's authorised users

2. NECESSITY AND PROPORTIONALITY

Legitimate Purposes:

- Performance of contract between Customer and Data Subjects
- Compliance with Customer's legal obligations as employer or recruiter
- Legitimate interests in the administration and integration of HR and recruiting systems
- Consent where required by applicable law

Data Minimization:

- Customer controls what data is submitted to the platform
- Processing limited to the data fields Customer selects for synchronisation
- Configurable data retention periods
- Automated deletion capabilities

3. RISKS TO DATA SUBJECTS

Identified Risks:

- Unauthorized access to identity, employment and HR data
- Incorrect or incomplete synchronisation of a Data Subject's record between connected systems

- Data breaches exposing employment data or special categories of data
- Lack of transparency towards Data Subjects about the systems to which their data is transferred

Risk Mitigation Measures:

- Comprehensive security controls (see Exhibit B)
- Customer control over which systems are connected and which data fields are synchronised
- Incident response and breach notification procedures
- Regular security testing and audits

4. SAFEGUARDS AND MEASURES

Technical Safeguards:

- Encryption, access controls, and monitoring (see Exhibit B)
- Audit trails for all processing activities
- Data segregation between customers
- Secure development practices
- Regular penetration testing and vulnerability assessments

Organizational Safeguards:

- DPA with comprehensive data protection obligations
- Staff training on privacy and security
- Vendor management and Subprocessor oversight
- Incident response procedures
- Regular compliance audits (SOC 2, ISO 27001)

Data Subject Safeguards:

- Correction and re-synchronisation of inaccurate records (Customer-controlled)
- Access, correction, and deletion capabilities
- Transparency through Customer's privacy notices
- Objection and restriction rights
- Complaint mechanisms through supervisory authorities

5. CONSULTATION AND STAKEHOLDER INPUT

Kombo has consulted with:

- External legal counsel specializing in privacy law
- Information security experts and auditors
- Industry associations and standards bodies
- Customers regarding privacy requirements and expectations

6. DPIA CONCLUSION SUPPORT

Kombo's assessment indicates that with the security measures, contractual protections, and technical safeguards in place, the residual risks to Data Subjects are reduced to an acceptable level. However, Customer remains responsible for:

- Conducting its own DPIA based on its specific use case
- Determining whether processing is necessary and proportionate
- Implementing additional safeguards as needed
- Consulting with supervisory authorities if required
- Providing appropriate notices and obtaining consents from Data Subjects