KOMBO
GLOBAL DATA PROCESSING AGREEMENT

Effective Date: As defined in the Agreement

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

"**Kombo**," "**we**," "**us**," or "**our**" means:

- **Kombo Technologies LLC,** a Delaware limited liability company with its principal place of business at 169 Madison Ave, STE 2182, NY 10016, USA, for Customers located in the United States, or Canada; or
- **Kombo Technologies GmbH**, a German limited liability company registered at HRB 244447 B, Amtsgericht Charlottenburg, with offices in Rosenthaler Str. 72A, 10119 Berlin, Germany, for Customers located in the European Union, United Kingdom, Switzerland, or Asia-Pacific regions.

The applicable Kombo entity is determined by the Agreement executed between the parties.

This DPA governs the processing of Covered Personal Information in connection with the Kombo Services and addresses requirements under applicable Privacy Laws. This DPA is designed to meet the requirements of global privacy laws including GDPR, CCPA/CPRA, LGPD, 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 the applicable Kombo entity governing Customer's use of the Kombo Services. "**Kombo**" means the Kombo entity (Kombo Technologies LLC or Kombo Technologies GmbH) with which Customer has contracted, as specified in the Agreement. 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**"); Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); California Consumer Privacy Act ("**CCPA**"), as amended by the California Privacy Rights Act ("**CPRA**"); the Virginia Consumer Data Protection Act ("**VCDPA**"); the Colorado Privacy Act ("**CPA**"); the Utah Consumer Privacy Act ("**UCPA**"); the Connecticut Act Concerning Personal Data Protection and Online Monitoring ("**PDPOM**"); Montana Consumer Data Privacy Act (Mont. Code Ann. § 30-14-1901 et seq.); Delaware Personal Data Privacy Act (Del. Code Ann. tit. 6, § 12D-101 et seq.); Iowa Consumer Data Protection Act (Iowa Code Ch. 715D); Indiana Consumer Data Protection Act (Ind. Code § 24-15); Nebraska Data Privacy Act (Neb. Rev. Stat. § 87-401 et seq.); New Hampshire Privacy Act (N.H. Rev. Stat. Ann. § 507-H); New Jersey Data Protection Act (N.J. Stat. Ann. § 56:8-166 et seq.); Minnesota Consumer Data Privacy Act (Minn. Stat. § 325O); Texas Data Privacy and Security Act (Tex. Bus. & Com. Code § 541 et seq.); Oregon Consumer Privacy Act (Or. Rev. Stat. § 646A.600 et seq.); Tennessee Information Protection Act (Tenn. Code Ann. § 47-18-3201 et seq.); Kentucky Consumer Data Protection Act (Ky. Rev. Stat. Ann. § 365.851 et seq.); Rhode Island Data Transparency and Privacy Act (R.I. Gen. Laws § 6-48.1 et seq.); **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 "**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 (and any successor clauses).

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

1.9 **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 is the controller (or business) and the applicable Kombo entity is the processor (or service provider, or "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.

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 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.

2.4 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.

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

- Data retention periods (within applicable limits)
- Automated decision-making parameters
- Access controls and user permissions
- Export and deletion requests

2.6 AI Apply Addendum. Where Customer elects to use Kombo's AI Apply feature, the processing of Covered Personal Information by AI model providers (including OpenAI) 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 model provider(s) as Subprocessors for the processing of Covered Personal Information.

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) unless permitted by applicable Privacy Laws, (i) retain, use, or disclose Covered Personal Information outside the direct business relationship with Customer, or (ii) retain, use, or disclose Covered Personal Information for any commercial purpose not specified in the Agreement or 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 both Kombo Technologies LLC and 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 or USA	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 Data[2]			
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	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.

	it's a personal email and not a generic email such as billing@company.com		

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

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. 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 for financial services data processing.

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 both Kombo Technologies LLC and 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 financial services regulations 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.

(a) For Customers contracting with Kombo Technologies LLC (customers in the United States, Canada): Covered Personal Information is processed and stored primarily in the United States using Google Cloud infrastructure located in the United States.

(b) For Customers contracting with Kombo Technologies GmbH (customers in the European Union, United Kingdom, and Asia-Pacific regions): Covered Personal Information is processed and stored primarily in Germany using Google Cloud infrastructure located in Ireland.

By using the Kombo Services and entering into this DPA, Customer authorizes processing and storage in the applicable location based on the contracting entity.

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 the United States or 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 from the EU/UK/Switzerland to the United States: Where Kombo Technologies GmbH transfers Covered Personal Information to Kombo Technologies LLC or US-based personnel for the limited purposes described in Section 8.2, such transfers are governed by the Standard Contractual Clauses set forth in Exhibit D.

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

8.4 Standard Contractual Clauses. Where the Standard Contractual Clauses apply under Section 8.3(b), they are incorporated into this DPA as Exhibit D with the following specifications:

- Module Two (controller-to-processor) applies
- Customer is the data exporter; Kombo Technologies LLC is the data importer
- 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 30-day notice period
- Mediation (Clause 18) and governing law/jurisdiction provisions are as specified in Exhibit A

For transfers from the UK, the UK International Data Transfer Addendum to the Standard Contractual Clauses applies. For transfers from Switzerland, the Standard Contractual Clauses apply with references to "GDPR" interpreted as references to the revFADP and the competent supervisory authority being the Swiss Federal Data Protection and Information Commissioner.

8.5 Intra-Group Transfers. Transfers of Covered Personal Information between Kombo Technologies LLC and Kombo Technologies GmbH for internal administrative purposes (e.g., consolidated reporting, group-wide security monitoring) are governed by intra-group data transfer agreements that incorporate the same protections as this DPA.

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 may satisfy its audit rights by reviewing Kombo's SOC 2 Type II and ISO 27001 reports available through the Security Portal, which Kombo will update and make available at least annually.

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/service provider 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/business. (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: Standard Contractual Clauses per Section 8.4
- UK to non-adequate countries: UK International Data Transfer Agreement (IDTA) or UK Addendum to EU Standard Contractual Clauses
- Switzerland to non-adequate countries: EU Standard Contractual Clauses modified for Swiss law (references to "GDPR" interpreted as revFADP; FDPIC as competent authority)

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, UK Addendum to SCCs, or UK-US Data Bridge (if and when operational).

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) Profiling Disclosure: Where processing involves profiling or automated decision-making, Kombo assists Customer in complying with revFADP Article 21 requirements regarding disclosure of logic, significance, and consequences.

(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.

13.3 UNITED STATES

13.3.1 Applicability. This Section applies to Customers contracting with Kombo Technologies LLC who are subject to US federal or state privacy laws.

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

- California Consumer Privacy Act (CCPA) as amended by California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Connecticut Data Privacy Act (CTDPA)
- Utah Consumer Privacy Act (UCPA)
- Montana, Delaware, Iowa, Indiana, Nebraska, New Hampshire, New Jersey, and Minnesota state privacy laws
- Other applicable state privacy laws as defined in Section 1.4

13.3.3 Service Provider and Processor Status.

(a) Under California Law: Kombo Technologies LLC is a "service provider" as defined under CCPA/CPRA. Kombo certifies that it understands and will comply with the restrictions in California Civil Code § 1798.140(w)(2)(A) and § 1798.140(ag)(2)(A).

(b) Under Other State Laws: Kombo Technologies LLC is a "processor" under Virginia, Colorado, Connecticut, Utah, Montana, Delaware, Iowa, Indiana, Nebraska, New Hampshire, New Jersey, and Minnesota privacy laws.

(c) Processing Restrictions: As specified in Section 3.1, Kombo will not:

- Sell or share Covered Personal Information

- Retain, use, or disclose Covered Personal Information outside the direct business relationship with Customer
- Combine Covered Personal Information with personal information from other sources except as permitted by law

13.3.4 Supervisory Authorities and Enforcement. Enforcement authorities include:

- Federal Trade Commission (FTC)
- California Privacy Protection Agency (CPPA)
- State Attorneys General
- Other state-level enforcement agencies as applicable

13.3.5 Sensitive Personal Information. Where Customer provides Sensitive Personal Information as defined under CPRA and other state laws, Kombo:

(a) Processes such information only to perform the Services or as otherwise permitted without requiring consumer consent under applicable state laws

(b) Does not use or disclose Sensitive Personal Information for inferring characteristics about consumers beyond what is necessary to provide the Services

13.3.6 Consumer Rights Assistance. In addition to the data subject rights assistance provided under Section 6, Kombo will assist Customer with US-specific consumer rights, including:

(a) Authorized Agents: If Kombo receives a request from an authorized agent, Kombo will promptly notify Customer and will not respond without Customer's authorization.

(b) Verification: Customer is responsible for verifying consumer identity; Kombo provides reasonable assistance including information about consumer interactions with the Services.

(c) Opt-Out Rights: Honoring opt-out requests for sale/sharing (though Kombo does not sell or share data).

(d) Right to Limit Use of Sensitive Personal Information: Restricting use of Sensitive Personal Information to permitted purposes under CPRA.

13.3.7 State Breach Notification Laws. In addition to Section 7 requirements, Kombo acknowledges that Customer may be subject to state-specific breach notification laws with varying timelines. Kombo will:

(a) Provide Customer with information necessary to comply with state breach notification laws, including nature and extent of breach, types of information involved, and number of affected consumers by state

(b) Cooperate with Customer's notifications to state attorneys general, consumer reporting agencies, and affected consumers

(c) Not notify consumers, regulators, or third parties without Customer's prior written consent, except as required by law

13.3.8 California-Specific Provisions.

(a) Audit Rights: Customer's audit rights under Section 9.1 satisfy Customer's right to take reasonable steps to ensure Kombo's compliance with CCPA/CPRA obligations.

(b) Subprocessor Notice: The 30-day advance notice in Section 4.2 satisfies Kombo's obligation to inform Customer of Subprocessors under CPRA.

(c) Consumer Request Metrics: Upon reasonable request, Kombo will provide information about consumer rights requests received directly by Kombo to assist Customer with CCPA/CPRA reporting obligations.

13.4 CANADA

13.4.1 Applicability. This Section applies to Customers contracting with Kombo Technologies LLC who are subject to Canadian federal or provincial privacy laws.

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

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Substantially similar provincial legislation (Alberta PIPA, British Columbia PIPA)
- Quebec's Act respecting the protection of personal information in the private sector (as modernized by Law 25)

13.4.3 Roles and Accountability. Under PIPEDA:

- Customer is the "organization" responsible for personal information
- Kombo Technologies LLC is a third-party service provider processing personal information on behalf of Customer
- Customer remains accountable for personal information in Kombo's possession or control under PIPEDA Principle 4.1.3
- Kombo provides comparable protection through this DPA and the measures in Exhibit B

13.4.4 Supervisory Authorities. The competent authorities are:

- Federal: Office of the Privacy Commissioner of Canada (OPC)
- Provincial: Provincial privacy commissioners (e.g., Commission d'accès à l'information du Québec for Quebec)

13.4.5 Consent and Withdrawal. Kombo acknowledges that PIPEDA requires meaningful consent for collection, use, and disclosure of personal information:

(a) Customer is responsible for obtaining appropriate consent from individuals

(b) Kombo processes personal information only for purposes for which Customer has obtained consent or as otherwise permitted by law

(c) Kombo assists Customer in responding to consent withdrawal requests as specified in Section 6.

13.4.6 Cross-Border Transfers and Transparency.

(a) Customer acknowledges that personal information will be transferred to and processed in the United States where it may be accessible to US law enforcement and government agencies under US law, as specified in Section 8.1(a).

(b) Upon request, Kombo will provide Customer with information about US processing to enable Customer to comply with PIPEDA's transparency requirements regarding cross-border transfers.

13.4.7 Breach Notification to OPC. For Security Incidents involving Canadian personal information that pose a "real risk of significant harm" to individuals:

(a) Kombo will provide Customer with information necessary to report the breach to the Privacy Commissioner of Canada as soon as feasible, in accordance with the Breach of Security Safeguards Regulations

(b) Information provided will include circumstances of the breach, date/time period, personal information involved, number of affected individuals, steps taken to reduce risk of harm, and notification to affected individuals

(c) Kombo acknowledges that Customer must report to OPC as soon as feasible after determining a breach poses real risk of significant harm

13.4.8 Quebec-Specific Requirements. For Customers subject to Quebec's modernized privacy law (Law 25):

(a) Kombo acknowledges Quebec's stricter requirements regarding consent, data minimization, and privacy by design

(b) Kombo will assist Customer in complying with Quebec's privacy impact assessment requirements

(c) Kombo will cooperate with the Commission d'accès à l'information du Québec (CAI)

(d) Upon request, Kombo will provide French-language versions of this DPA and related documentation

13.4.9 Retention and Disposal. Kombo retains Canadian personal information only as long as necessary to fulfill collection purposes or as required by law, in accordance with PIPEDA Principle 4.5 and Section 6.4 of this DPA.

13.6 ASIA-PACIFIC REGIONS

13.6.1 Applicability. This Section applies to Customers contracting with Kombo GmbH who are established in Asia-Pacific jurisdictions or who process personal data of data subjects in these regions. As Kombo's Asia-Pacific operations evolve, this Section will be updated to address jurisdiction-specific requirements.

13.6.2 General Framework. For Asia-Pacific Customers, the general provisions of Sections 1-12 apply. Kombo processes data in accordance with applicable local data protection laws and will implement jurisdiction-specific requirements as needed.

13.6.3 Data Localization. Where Asia-Pacific jurisdictions require data localization or impose restrictions on cross-border data transfers, Kombo will work with Customer to implement appropriate technical and contractual measures, which may include:

(a) Processing data within the jurisdiction where technically feasible

(b) Implementing appropriate transfer mechanisms recognized under local law

(c) Obtaining necessary approvals or registrations for cross-border transfers

13.6.4 Future Enhancements. As Kombo expands its Asia-Pacific customer base, this Section will be enhanced to address specific requirements under laws including but not limited to:

- Singapore Personal Data Protection Act (PDPA)
- Australia Privacy Act 1988
- Japan Act on the Protection of Personal Information (APPI)
- Other applicable Asia-Pacific data protection laws

Customers in these jurisdictions should contact Kombo for current compliance information and jurisdiction-specific addenda as applicable.

14. MISCELLANEOUS

14.1 Conflict. In case of conflict between this DPA and the Agreement, this DPA prevails with respect to the processing of Covered Personal Information. In case of conflict between this DPA and Standard Contractual Clauses, the Standard Contractual Clauses prevail to the extent required by applicable law.

14.2 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.

14.3 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 same law as specified in the Agreement.

(a) For Customers contracting with Kombo Technologies LLC: Laws of the State of New York, United States, without regard to conflicts of law principles.

(b) For Customers contracting with Kombo Technologies GmbH: Laws of Germany, without regard to conflicts of law principles.

For Standard Contractual Clauses (where applicable), the governing law and jurisdiction are as specified in Exhibit A.

14.5 Survival. The following sections survive termination of this DPA: Section 7 (Security Incidents), Section 11 (Data Return), Section 12 (Liability and Indemnification), and Section 14 (Miscellaneous).

14.6 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.

14.7 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.

14.8 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 based on which Kombo entity Customer has contracted with:

A. FOR CUSTOMERS CONTRACTING WITH KOMBO TECHNOLOGIES LLC

Applicable Regions: United States, Canada

Kombo Entity Information:

- **Legal Name**: Kombo Technologies LLC
- **Jurisdiction**: Delaware, United States
- **Address**: 169 Madison Avenue, STE 2182, New York, NY 10016, USA
- **Role**: Processor (or Service Provider under applicable US state privacy laws)

Primary Data Processing Location:

- **Country:** United States
- **Infrastructure:** Google Cloud - US regions
- **Secondary Locations** (optional): Customer's country where technically feasible
- **Access Points:** United States (primary operations), Germany (technical support)
- **Backup Locations:** AWS regions within primary and secondary processing locations

Governing Law and Jurisdiction:

- **Governing Law:** Laws of the State of New York, United States
- **Jurisdiction:** State and federal courts located in New York, New York
- **For Standard Contractual Clauses:** Generally not applicable for LLC customers unless Customer is transferring data from EU/UK/Switzerland to Kombo Technologies LLC

Competent Supervisory Authority:

- Determined by Customer's location and applicable Privacy Laws:
    - **United States:** Federal Trade Commission (FTC), California Privacy Protection Agency (CPPA), and applicable state attorneys general
    - **Canada:** Office of the Privacy Commissioner of Canada and provincial commissioners

B. FOR CUSTOMERS CONTRACTING WITH 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
- For Standard Contractual Clauses (where applicable):
    - **Governing Law:** Laws of Customer's EU Member State (for EU customers) or laws of Germany (for non-EU customers requiring SCCs)
    - **Jurisdiction:** Courts of Customer's EU Member State (for EU customers) or courts of Berlin, Germany (for non-EU customers)

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 the United States, Germany
- Cross-entity technical support (Germany personnel supporting Kombo Technologies LLC customers)
- 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
- Decision outcomes and model predictions

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 for fraud prevention)
- 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, sensitive personal information under CCPA/CPRA, or equivalent categories under other Privacy Laws requires Customer's express written authorization and appropriate legal basis.

PART 3: STANDARD CONTRACTUAL CLAUSES DETAILS

Applicability: Standard Contractual Clauses apply only where required by applicable law, typically for transfers from EU/EEA/UK/Switzerland to countries without adequacy decisions.

When SCCs Apply:

- **EU/EEA Customers** (Kombo Technologies GmbH): When data is accessed by US personnel or transferred to Kombo Technologies LLC for cross-entity support
- **UK Customers** (Kombo Technologies GmbH): UK International Data Transfer Agreement (IDTA) or UK Addendum to SCCs
- **Swiss Customers** (Kombo Technologies GmbH): SCCs modified for Swiss law requirements
- **Other scenarios:** As required by applicable Privacy Laws

SCC Specifications (where applicable):

- **Module**: Module Two (Controller to Processor)
- **Data Exporter**: Customer
- **Data Importer**: Kombo Technologies LLC (for transfers to US) or Kombo Technologies GmbH (for transfers to Germany/Romania)
- **Docking Clause**: Clause 7 does not apply
- **Subprocessor Changes**: Clause 9(a) Option 2 applies with 30-day notice period
- **Mediation**: Clause 18 mediation is optional at Customer's election
- **Governing Law**:
    - For EU customers: Laws of Customer's EU Member State
    - For UK customers: Laws of England and Wales (or as specified in UK IDTA)
    - For Swiss customers: Laws of Switzerland
- **Jurisdiction**:
    - For EU customers: Courts of Customer's EU Member State

- For UK customers: Courts of England and Wales (or as specified in UK IDTA)
- For Swiss customers: Courts of Switzerland

PART 4: CONTACT INFORMATION

Security and Data Protection Contact (Both Entities):

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

Kombo Technologies LLC Contact:

- Address: 169 Madison Avenue, STE 2182, New York, NY 10016, USA
- Legal Entity: Delaware Limited Liability Company
- General Inquiries: contact@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 Both Entities:

- SOC 2 Type II - Available through Security Portal
- ISO 27001:2013 - Available through Security Portal (only Kombo Technologies GMbH)
- 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

The Kombo cloud infrastructure is hosted in SOC 2 Type II and ISO 27001:2013 certified data centers. Additionally, Kombo maintains comprehensive security controls. Both, the certifications as well as a description of the security controls are detailed in the Security Portal at https://security.kombo.dev.

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

High-Risk Processing Activities:

- Automated decision-making with legal or similarly significant effects (credit decisions, fraud detection)
- Large-scale processing of special categories of data (if authorized by Customer)
- Systematic monitoring of publicly accessible areas (if applicable to Customer's use case)
- Processing of financial and credit data for risk assessment

Processing Characteristics:

- Scale: Platform capable of processing millions of decisions annually
- Automation: Highly automated processing with configurable human oversight
- Data Sensitivity: Financial data, identity data, and potentially special categories
- Data Subjects: Consumers, business representatives, vulnerable populations (depending on Customer's use case)

2. NECESSITY AND PROPORTIONALITY

Legitimate Purposes:

- Performance of contract between Customer and Data Subjects
- Compliance with legal obligations (AML, KYC, credit reporting)
- Legitimate interests in fraud prevention and risk management
- Consent where required by applicable law

Data Minimization:

- Customer controls what data is submitted to the platform
- Processing limited to data necessary for specified decision-making purposes
- Configurable data retention periods
- Automated deletion capabilities

3. RISKS TO DATA SUBJECTS

Identified Risks:

- Unauthorized access to financial and identity data
- Incorrect automated decisions affecting creditworthiness
- Discriminatory outcomes from biased models
- Data breaches exposing sensitive financial information
- Lack of transparency in automated decision-making

Risk Mitigation Measures:

- Comprehensive security controls (see Exhibit B)
- Model governance and bias monitoring
- Explainability features for automated decisions
- Customer control over decision logic and thresholds
- 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:

- Right to human review of automated decisions (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