Data Processing Agreement for Self Service Customers

This Data Processing Agreement ("DPA"), including its appendices and the Sub-processor List incorporated under section 6, governs the Processing of Personal Data in Klang's self-service services. It is entered into electronically between:

1. the legal entity or individual acting in a business or professional capacity identified as the customer in the relevant Klang account, subscription or purchase record ("Customer" or "Data Controller"); and
2. Klang AI AB, org. no. 559378-4571, ("**Data Processor**") with an address at Sundstorget 3, 252 21 Helsingborg, Sweden

(each a "Party" and collectively the "Parties").

The person accepting this DPA confirms that they have authority to bind the Customer. The Customer shall keep its legal identity, business address and contact details accurate in its account or provide them to Klang in writing.

1. Background

The Customer obtains Klang's self-service services through an online account or subscription ("Services"). The agreement governing those Services, including any Terms and Conditions validly accepted by the Customer and the applicable subscription or purchase details, is the "Main Agreement". No separately signed SaaS agreement or order form is required for this DPA. This DPA takes effect when the Customer affirmatively accepts it electronically, either directly or by accepting terms that expressly incorporate this DPA and make it available before acceptance ("Effective Date"). Klang offers to be bound by this DPA upon that acceptance; no separate countersignature is required. Payment, use of the Services or downloading this DPA alone does not constitute acceptance under this clause. For an existing customer, the Effective Date is the date of that acceptance, not the date of an earlier purchase. This DPA also operates as a standalone processing agreement if accepted separately from the Main Agreement.

2. Definitions

2.1 The following definitions are used in the Data Processing Agreement:

Applicable Data Protection Legislation	The GDPR (Regulation (EU) 2016/679), the Swedish Act (2018:218) supplementing the GDPR, and other laws applicable to Processing under this DPA, as interpreted by competent courts.
Sub-processor	Another processor engaged by Klang to Process Personal Data on the Customer's behalf.

2.2 "Personal Data" means personal data Processed by Klang on the Customer's behalf in providing the Services, including personal data in Customer content and generated outputs. "Process", "Processing", "Data Subject", "controller", "processor" and "Personal Data Breach" have the meanings given in the GDPR. The Customer acts as controller and Klang as processor. Where the Customer acts as processor for another controller, Klang acts as its sub-processor and the Customer confirms that it has the authority and instructions needed to appoint Klang and instruct the Processing. References to the Data Controller include the Customer acting in that capacity. This DPA does not govern Processing for which

Klang independently determines the purposes and means, such as its own billing and business contact administration; that Processing is described in Klang's Privacy Notice. Customer content is not excluded from this DPA merely because Klang has access to it.

3. Processing of Personal Data

3.1 The Data Processor is responsible for ensuring that all Processing is carried out in accordance with the terms of the Data Processing Agreement and Applicable Data Protection Legislation.

3.2 The Data Processor shall only Process Personal Data in accordance with documented instructions from the Data Controller, including the instructions set out in Appendix 1, including when it comes to transfers of Personal Data to a third country or an international organization, unless the Data Processor is obligated under EU legislation (including the laws of its member states) to Process certain Personal Data. In such cases, the Data Processor shall inform the Data Controller of the legal requirement before the Processing begins, to the extent permitted by applicable law.

3.3 Appendix 1 sets out the types of Personal Data, categories of Data Subjects, and nature and purpose of Processing. This DPA, the Customer's use of the Services and its selected settings constitute documented instructions. Additional instructions must be provided in writing, including by email or through the Services. Klang shall confirm whether an instruction outside the agreed Services can be implemented. The Parties shall agree any resulting change to the Services in writing before implementation. Nothing in this clause permits Klang to refuse assistance or compliance required by Applicable Data Protection Legislation. The Customer is responsible for the lawfulness of its instructions, the Personal Data it provides, and the required legal bases, notices and permissions for recording and Processing.

3.4 The Data Processor shall immediately inform the Data Controller if it considers an instruction to infringe Applicable Data Protection Legislation, explaining its reasons and any changes needed. It shall suspend the affected instruction until the Parties have resolved the issue lawfully. A confirmation from the Data Controller does not require the Data Processor to carry out an unlawful instruction.

3.5 The Data Processor may update the technical and organizational operation of the Services without individual customer approval, provided the update remains within the documented instructions, complies with this DPA and does not materially reduce the overall level of security or protection of Personal Data. Klang shall notify the Data Controller in writing at least thirty (30) days before a planned material change affecting the protection of Personal Data. Where an earlier change is necessary to address an urgent security risk or comply with law, Klang shall notify the Data Controller as soon as reasonably possible. Changes to Sub-processors are governed by section 6; changes to this DPA by section 12. This clause does not authorize a new purpose or a prohibited international transfer.

3.6 Access to Personal Data within the Data Processor's organization shall be limited to those who need access to the Personal Data to fulfill section 1 and Appendix 1 of the Data Processing Agreement.

3.7 The Data Processor shall ensure that all individuals for whom the Data Processor is responsible and who Process Personal Data under the Data Processing Agreement have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.

3.8 The Data Processor undertakes to ensure at all times that relevant personnel within its organization comply with the Data Processing Agreement and the instructions provided by the Data Controller, as well as to keep the relevant personnel informed about the provisions of the Applicable Data Protection Legislation.

3.9 Taking into account the nature of the Processing, the Data Processor shall assist the Data Controller through appropriate technical and organizational measures, insofar as possible, in responding to Data Subjects' requests under Applicable Data Protection Legislation. If Klang receives such a request concerning Personal Data directly, it shall promptly refer it to the Customer and shall not respond on the Customer's behalf unless instructed or required by law.

3.10 Taking into account the nature of the Processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller in ensuring that the obligations under Applicable Data Protection Legislation are fulfilled, including (if applicable) the Data Controller's obligation to (i) implement appropriate technical and organizational measures, (ii) notify the supervisory authority of Personal Data breaches, (iii) inform Data Subjects about Personal Data breaches, (iv) conduct data protection impact assessments, and (v) consult with the competent supervisory authority before Processing.

3.11 The Data Processor shall, without undue delay and unless prohibited by law, inform the Data Controller of contacts with a competent supervisory authority concerning Processing under this DPA. The Data Processor is not authorized to represent the Data Controller or act on its behalf before a supervisory authority.

3.12 The Data Processor shall maintain the records of Processing required by the GDPR and provide relevant information to the Data Controller on request, subject to protecting confidential information relating to other customers.

3.13 The Data Processor shall, at the Data Controller's choice, return or delete Personal Data during the term or following termination of the Services and delete existing copies, unless Union or Member State law requires retention. The Data Controller may use available export and deletion controls or send a written request to Klang. On termination, the Customer may request return within thirty (30) days; if it does not, the Customer instructs Klang to delete the Personal Data after that period. Klang shall complete return or deletion from active systems without undue delay after the request or expiry of that period. Backup copies shall be deleted as set out in Appendix 1 and remain protected and isolated from ordinary use until then. Any legally retained data shall be restricted to the legally required purpose and deleted when that requirement ends. Klang shall confirm completion in writing on request.

4. Security in Connection with Processing

4.1 The Data Processor shall implement appropriate technical and organizational security measures in accordance with Applicable Data Protection Legislation to ensure a level of security appropriate to the risk, including the security measures outlined in Appendix 2.

4.2 The Data Processor shall implement technical and organizational security measures that ensure that any suspicions can be investigated regarding whether someone working for the Data Controller, the Data Processor, or any of its Sub-processors has had unauthorized access to the Personal Data.

4.3 The Data Processor shall comply with any decisions from supervisory authorities regarding measures required to meet legal security requirements.

4.4 Klang shall notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting the Customer's Personal Data, in accordance with Article 33(2) GDPR. Notice shall be sent to the Customer's designated privacy or security contact or, if none is designated, its account administrator's email address. Klang shall provide a contact point and the information reasonably required to assist the Customer with its obligations under Articles 33 and 34 GDPR, including, to the extent then available:

(a) a description of the nature of the Personal Data Breach, and, if possible, the categories and approximate number of Data Subjects and Personal Data concerned;

(b) a description of the likely consequences of the Personal Data Breach; and

(c) a description of the measures taken or proposed to address the Personal Data Breach or mitigate its adverse effects. Information may be provided in phases without undue further delay as it becomes available. Klang shall take appropriate measures to address the breach and provide assistance as required by Applicable Data Protection Legislation. General service-status information may be published at https://status.klang.ai. Such publication does not replace notification to an affected Customer under this clause.

4.5 The Data Processor shall evaluate the effectiveness of its technical and organizational security measures at least annually and following material changes or incidents where appropriate. It shall make relevant information available to the Data Controller on request and cooperate with the Data Controller's assessment under section 5.

5. Audit

The Data Processor shall make available all information necessary to demonstrate compliance with this DPA and Applicable Data Protection Legislation, and allow and contribute to audits, including inspections, by the Data Controller or its appointed auditor. The Parties shall first use available security documentation and independent audit reports where these provide sufficient assurance. If further verification is reasonably necessary, Klang shall allow an audit or inspection. The Parties shall agree reasonable arrangements for scope, timing, confidentiality and protection of other customers' data. Ordinarily, inspections require thirty (30) days' notice, take place during business hours and occur no more than once per year; these arrangements do not restrict audits required by law or a supervisory authority, or additional or urgent audits reasonably needed following a Personal Data Breach or suspected non-compliance. Each Party bears its own costs, except that Klang shall reimburse the Customer's reasonable audit costs if the audit identifies Klang's non-compliance with this DPA. These arrangements shall not prevent the exercise of statutory audit rights.

6. Sub-processors

6.1 By accepting this DPA, the Customer gives general written authorization for Klang to engage the Sub-processors identified in the list maintained at https://trust.klang.ai ("Sub-processor List"), as updated in accordance with this section. The Sub-processor List forms part of this DPA and is its sole list of Sub-processors. It shall identify each Sub-processor's legal entity, function, relevant Services, categories of Personal Data, and countries of storage and other Processing, including remote access, together with applicable transfer safeguards. Klang shall keep the list accessible before acceptance and throughout the Services and make dated versions or a change history available for the Customer's records. Klang shall give the Customer at least thirty (30) days' prior written notice of a proposed addition or replacement, or a material change to a listed Sub-processor's function, data scope or processing countries. Notice may be sent automatically through the Trust Center to the contact designated under section 13.2. The Customer need not separately subscribe to receive required notices; merely updating the list is not notice. The Customer may object within that period on reasonable data protection grounds. If the Customer does not object within the period, the change is authorized without a further signature or amendment, subject to section 7. If the Customer objects, Klang shall seek a commercially reasonable resolution, such as an alternative provider or configuration. The disputed change shall not apply to the Customer's Personal Data while the objection remains unresolved. If no resolution is available, either Party may terminate the affected Services, or the Main Agreement where the affected Services cannot reasonably be separated, before the disputed Processing begins. Termination under this clause is without penalty and Klang shall refund prepaid fees for the unused period of the terminated Services. Each Sub-processor shall be bound by a written agreement imposing the same data protection obligations as this DPA. Klang remains fully responsible for its Sub-processors' performance. On request, Klang shall provide relevant copies of those agreements, with redactions only as necessary to protect unrelated confidential information. An update to the Sub-processor List does not amend other obligations under this DPA or authorize a new Processing purpose.

7. Processing Locations and International Transfers

7.1 The Processing locations for the relevant Services are specified in the Sub-processor List at https://trust.klang.ai. The Customer authorizes Processing at those locations, subject to this DPA. Changes follow section 6 without a separate signature or amendment. Any data residency commitment expressly agreed for the Customer's Services continues to apply.

7.2 Any transfer of Personal Data subject to Chapter V of the GDPR shall comply with that Chapter. Before the transfer, Klang shall ensure an applicable adequacy decision or appropriate safeguards are in place, including, where used, binding European Commission standard contractual clauses with the applicable module and completed annexes, together with any required assessment and supplementary measures. Klang shall make relevant information available on request. If a transfer mechanism ceases to be valid, Klang shall implement a lawful alternative or suspend the affected transfer.

7.3 Any legally required disclosure of Personal Data remains subject to Applicable Data Protection Legislation and this section. Unless legally prohibited, Klang

shall inform the Customer before legally required Processing outside the Customer's instructions.

8. Confidentiality

The Data Processor shall keep confidential Personal Data and confidential information received in connection with this DPA. Disclosure is permitted only to authorized personnel, approved Sub-processors and professional advisers who need the information and are bound by confidentiality, or as required by applicable law or a binding governmental decision. Such disclosure remains subject to sections 3, 6 and 7. Any applicable confidentiality obligations in the Main Agreement also apply. This section survives termination.

9. Compensation

The Data Processor is not entitled to any specific compensation for the Processing of Personal Data under the Data Processing Agreement. The Data Processor's compensation for the service delivery under the Main Agreement includes compensation for fulfilling the obligations set out in the Data Processing Agreement.

10. Liability

10.1 This DPA creates no separate obligation for Klang to indemnify or defend the Customer, reimburse the Customer's fines or sanctions, or maintain or provide evidence of a particular insurance policy. Klang's liability is governed by this section and applicable law.

10.2 Subject to section 10.4, any limitations and exclusions of liability validly agreed in the Main Agreement also apply to contractual claims under or in connection with this DPA. This DPA does not create a separate or additional liability cap; claims under this DPA and the Main Agreement count towards the same applicable aggregate limit.

10.3 If no limitations of liability have been validly agreed in the Main Agreement, then, subject to section 10.4, Klang's total aggregate contractual liability to the Customer arising out of or in connection with this DPA shall not exceed the fees paid by the Customer to Klang for the Services during the six (6) months immediately preceding the first event giving rise to the claim. In that case, Klang shall not be liable for indirect or consequential loss, or loss of profit or revenue.

10.4 Nothing in this DPA limits the rights of Data Subjects, the powers of supervisory authorities, liability for fraud, wilful misconduct or gross negligence, or any liability or right of recourse that cannot lawfully be excluded or limited, including under Article 82 GDPR. This section does not reduce Klang's obligations to comply with Applicable Data Protection Legislation or perform its Processing obligations under this DPA. Section 10 survives termination.

11. Term of Agreement

This DPA takes effect on the Effective Date defined in section 1. Subject to the continuing obligations below, it terminates automatically on the effective expiry or termination of the Customer's paid subscription for the Services. Giving notice of cancellation does not terminate this DPA before that date. On termination, section 3.13 and the deletion periods in Appendix 1 apply. This DPA continues to govern any Personal Data remaining with Klang or its Sub-processors until deletion is complete, including backup copies. During that

period, Processing is limited to return, deletion, protection of the remaining data and retention required by law, as provided in this DPA. This does not extend the subscription or permit continued use of the Personal Data to provide the Services. Termination does not affect accrued rights or obligations expressly stated to survive.

12. Amendments and Additions

12.1 Amendments to this DPA must be agreed in writing, including through affirmative electronic acceptance. Klang may propose a revised version by written notice specifying the changes and proposed effective date. Posting a revised version or the Customer's silence does not by itself amend the version already accepted. Operational updates within section 3.5 and changes to the Sub-processor List, including processing countries, made in accordance with sections 6 and 7 are authorized under this DPA and do not require a separate amendment or signature. A new Processing purpose, or a change inconsistent with an express data residency commitment, requires express written agreement. Each accepted DPA version and the applicable Sub-processor List history shall remain available to the Customer for its records.

12.2 The Parties shall cooperate without undue delay to agree amendments necessary to comply with Applicable Data Protection Legislation. Pending agreement, Klang shall continue to comply with that legislation and this DPA and shall suspend any affected Processing that cannot lawfully continue.

13. Miscellaneous

13.1 This DPA, its appendices and the Sub-processor List incorporated under section 6 govern its subject matter and take precedence over inconsistent provisions of the Main Agreement relating to Processing, including any general content-use licence, disclaimer or deletion provision. If the Sub-processor List conflicts with another provision of this DPA, that other provision prevails. Mandatory provisions of applicable standard contractual clauses prevail over this DPA. A separately negotiated data processing agreement for the same Services continues to apply unless the Parties expressly agree that this DPA replaces it. Acceptance of this DPA alone does not constitute acceptance of other terms that were not expressly presented for acceptance.

13.2 Assignment of the Data Processor's obligations under this DPA requires the Customer's prior written consent, which may be given electronically. Notices and instructions under this DPA may be sent electronically. The Customer shall maintain a current account administrator email address and may designate a privacy or security contact. Notices to Klang, requests, objections and instructions under this DPA may be sent to support@klang.ai. Klang shall send notices requiring action to the designated contact or, if none, the account administrator; a website update alone does not satisfy a notice requirement.

14. Dispute Resolution and Applicable Law

14.1 The Data Processing Agreement shall be interpreted and applied in accordance with Swedish law, with the exception of such international private law provisions that would result in the application of the law of another jurisdiction.

14.2 Disputes under this DPA shall be resolved in accordance with any dispute resolution provisions validly agreed in the Main Agreement. If no such

provisions have been agreed, the courts of Sweden shall have jurisdiction, with Helsingborg District Court as the court of first instance. This does not restrict mandatory rights or jurisdiction under Applicable Data Protection Legislation.

Appendix 1 – Instructions for Personal Data Processing

1. Type of Personal Data

Depending on the Customer's use of the Services, Personal Data may include:

(a) Contact details, such as name, phone number, address, and email address

(b) Date of birth

(c) Employment information

(d) Audio and video recordings, including speakers' voices and images

(e) Transcripts, summaries, notes, prompts, uploaded documents and other content or outputs containing Personal Data

(f) Phone calls and related call metadata, where the relevant feature is used

2. Categories of Data Subjects

Depending on the Customer's use, the Personal Data may concern:

(a) The Customer's employees, contractors and other authorized users

(b) The Customer's customers, clients, suppliers, counterparties and their personnel

(c) Meeting participants, interviewees and other people whose information is included in Customer content

(d) Persons mentioned in recordings, transcripts, uploaded materials or generated outputs

(e) For legal or public-sector uses, court personnel, parties, witnesses and expert witnesses

(f) Other individuals whose Personal Data the Customer lawfully submits to the Services

(g) These categories apply only to the extent the Customer actually uses the Services to Process their Personal Data.

3. Nature and Purpose of the Processing

The subject matter is Processing Customer content to provide the Services selected by the Customer. Operations may include collection, recording, transmission, hosting, storage, transcription, speaker identification, summarization, analysis, search, retrieval, export and deletion, together with support and maintenance necessary to provide those Services. Processing occurs on an ongoing basis during use and for the retention periods below. The Customer determines the content and features used. This DPA does not grant the Customer features or service levels not included in its subscription.

Klang shall Process Personal Data only for those purposes and the Customer's documented instructions. Personal Data shall not be used to train general-purpose AI models for Klang's or a third party's own purposes. Customer content may contain special categories of data under Article 9 GDPR or data about criminal convictions or offences under Article 10 GDPR. The Customer shall submit such data only where lawful, permitted by the Services

and supported by appropriate safeguards, and is responsible for any required additional legal basis. Klang shall apply this DPA's confidentiality, access and security protections to that data.

4. Location of Processing

The Processing locations applicable to the Customer's selected Services are set out in the Sub-processor List at https://trust.klang.ai, incorporated under section 6. Processing at those locations and any changes are governed by sections 6 and 7.

5. Sub-processor List

The Sub-processor List at https://trust.klang.ai is the sole list of Sub-processors and forms part of this DPA under section 6. It identifies each Sub-processor and its relevant Processing details. Authorization covers only Sub-processors used for the Customer's selected Services and Personal Data necessary for their function. Updates follow sections 6 and 7 without reissuing or separately signing this DPA.

6. Deletion of Personal Data

Customer content in the web portal is retained until the Customer deletes it or the return and deletion process in section 3.13 applies following termination. Backup copies are deleted within a maximum of ninety (90) days after deletion from active systems. During that period, copies are protected, excluded from ordinary use and accessed only as necessary for recovery or security; any restored data remains subject to the deletion instruction. For API usage, request data is automatically deleted after the request has been processed. Any retention required by law is subject to section 3.13.

Appendix 2 – Technical and Organizational Security Measures

Technical and Organizational Security Measures to be implemented by the Data Processor

The Data Processor shall:

- prevent unauthorized access to computer equipment used to Process and use Personal Data (equipment access protection),
- prevent unauthorized persons from using data processing systems, and ensure that procedures exist for assigning, changing, and revoking such persons' access authorizations (system access control),
- ensure that persons authorized to use a data processing system only have access to the Personal Data relevant to their access authorization, and that Personal Data cannot be read, copied, modified, or deleted without authorization during Processing (data access control),
- ensure that Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage on data media, and that it is possible to check and determine at which points transmission of Personal Data from data transfer facilities is intended (transfer control),
- ensure that it is possible to check and determine after an event whether and by whom Personal Data has been entered, modified, or deleted from systems that Process Personal Data (input control),
- ensure that Personal Data Processed on behalf of the Data Controller can only be Processed in accordance with the Data Controller's instructions (instruction control),
- ensure that Personal Data is protected against accidental destruction or loss (availability control),
- ensure that Personal Data collected for different purposes can be Processed separately (separation control).