Customer Data Processing Agreement

This Data Processing Addendum ("**DPA**") forms part of the Services Agreement ("**Agreement**") between Kenshoo Ltd. d/b/a skai, or the applicable skai subsidiary, from which Customer is acquiring (directly or through an authorized distributor or reseller) the Services, (collectively, "**Company**") and the person or entity who acquires the Services under the Agreement ("**Customer**"). This DPA reflects the parties' agreement with regard to the processing of personal data as part of Company's provision of Services under the Agreement and is effective as of Customer's signature date.

All capitalized terms not defined herein will have the meaning ascribed to them in the Agreement, or under Applicable Data Protection Law.

Data Processing Terms

1.1. *Definitions:* In this DPA, the following terms shall have the following meanings:

(a) "**Affiliate**" means any legal entity directly or indirectly controlling, controlled by or under common control with a party to the Agreement, where "control" means the ownership of a majority share of the voting stock, equity, or voting interests of such entity;

(b) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law, US Privacy Laws and the Federal Law No. 13.709/2018 (Brazilian General Law on Data Protection – "**LGPD**");

(c) "**controller**" means the entity which determines the purposes and means of the processing of Personal Data, which includes a "controller" or "business" as defined under Applicable Data Protection Law;

(d) "**Company Information Security Policy"** means the information security documentation applicable to the specific Service purchased by Customer, as updated from time to time;

(e) "**data subject**" means the identified or identifiable person to whom personal data relates, which includes a "data subject" or "consumer" as defined under Applicable Data Protection Law;

(f) "**EEA**" means the European Economic Area;

(g) "**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General

Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**; and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i) or (ii); in each case as may be amended or superseded from time to time;

(h) "**personal data**" means any information relating to an identified or identifiable natural person and includes 'personal data', 'personal information' or 'personally identifiable information' as defined under Applicable Data Protection Law;

(i) "**processing**" shall have the meaning given to it in Applicable Data Protection Law (and the terms "**process**", "**processes**" and "**processed**" will be interpreted accordingly);

(j) "**processor**" means the entity which processes personal data on behalf of the controller, which includes a "processor" or "service provider" as defined under Applicable Data Protection Law.

(k) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

(l) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"); and

(m) **"US Privacy Laws"** means all U.S. state privacy laws applicable to the Data, including where relevant: (i) the California Consumer Privacy Act (the "**CCPA**"), as amended by the California Privacy Rights Act ("**CPRA**"), as well as any regulations that may be issued thereunder; and, where applicable, (ii) the Virginia Consumer Data Protection Act ("**CDPA**"); (iii) the Colorado Privacy Act ("**CPA**") when effective; (iv) the Utah Consumer Privacy Act when effective ("**UCPA**"); (v) the Connecticut Data Privacy Act ("**CTDPA**") when effective; in each case, only to the extent that such law(s) apply to the processing of Data under the Agreement.

1.2. *Relationship of the parties:* Customer (the controller-and if Customer processes the Data on behalf of a third party - a Processor) appoints Company as a processor to process the personal

data described in Annex I (the "**Data**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law.

1.3. *Prohibited data:* Customer shall not disclose (and shall not permit any data subject to disclose) any special categories of Data to Company for processing.

1.4. *Customer obligations:* Customer's instructions to Company will comply with Applicable Data Protection Law. Customer will have sole responsibility for the accuracy, quality and legality of the Data, the means by which Customer acquired the Data, and Customer permissions to process the Data pursuant to this DPA. As required under Applicable Data Protection Law, Customer will provide all necessary notices to data subjects and secure the applicable lawful grounds for processing Data under the DPA, including where applicable, all necessary permissions and consents from them. To the extent required under Applicable Data Protection Law, Customer will receive and document the appropriate consent from the data **subject.**

1.5. *Processing restrictions*: Company will not "sell" or "share" Data (as such terms are defined by US Privacy Laws). Furthermore, Company will not retain, use or disclose Data (i) for any purpose other than for the purpose of performing the Services, or (ii) outside of the business relationship between Customer and Company, except where required by a relevant authority in accordance with the Applicable Data Protection Law. In addition, Company will not combine Data with information received from another source, except where necessary to provide the Services or if required by a relevant authority in accordance with the Applicable Data Protection Law. Company acknowledges and will comply with the restrictions set forth in this Section 1.5. The parties acknowledge and agree that the Data that Customer discloses to Company is provided to Company for a Permitted Purpose (as defined below), and Customer is not "selling" Data to Company in connection with the Agreement, or "sharing" (as such term is defined under the CCPA) Data to Company unless in accordance with the limitations on service providers under the CCPA or other Applicable Data Protection Laws.

1.6. *Company's Obligations under US Privacy Laws:* Company shall notify Customer if it makes a determination that it can no longer meet its obligations under Applicable Data Protection Law. Customer may, upon written notice, and at Customer's expense, take reasonable steps to stop and remediate an unauthorized use of Data in accordance with Applicable Data Protection Law (which may include, for example, assessments, audits and other technical or operational testing) . In addition, Company shall provide the same level of privacy protection for the Data as required by the CCPA in order to give effect to consumer requests made, including informing of any consumer request made and cooperating to ensure the information necessary to comply with the request is provided.

1.7. *Purpose limitation:* Company will process Data on behalf of and in accordance with Customer's instructions. Customer instructs Company to process Data for the following purposes: (i) processing to provide the Services to the Customer in accordance with the Agreement and applicable Order Forms; and (ii) processing to comply with other reasonable instructions provided by Customer in writing where such instructions are consistent with the terms of the Agreement and comply Applicable Data Protection Laws (the "**Permitted Purpose**"). Processing outside the scope of this DPA (if any) will require prior written

agreement between Company and Customer on additional instructions for processing, including agreement on any additional fees Customer will pay to Company for carrying out such instructions. Company will inform Customer immediately, if in Company's opinion an instruction violates any provision under Applicable Data Protection Law and will be under no obligation to follow such instruction, until the matter is resolved in good-faith between the parties.

1.8. *Restricted transfers:* The parties agree that when the transfer of Data from Customer to Company is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

(a) in relation to data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply and Module Three will apply to the extent that Customer is a processor of the Data on behalf of a third party controller;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 1.11 of this Agreement;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I to this Agreement; and

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II to this Agreement;

(b) in relation to Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows:

(i) the EU SCCs, completed as set out above in clause 1.7(a) of this Agreement shall also apply to transfers of such Data, subject to sub-clause (ii) below;

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Agreement.

(c) in the event that any provision of this Agreement contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

(d) To complement and reinforce the safeguards provided by the EU SCCs, Company warrants that, unless required by a valid court order or otherwise prohibited by law, Company will:

(i) not purposefully create 'back-doors' or similar programming that could be used to access the Data;

(ii) not provide the source code or encryption keys to any government agency for the purpose of accessing the Data;

(iii) Upon Customer's written request, provide reasonable available information about the requests of access to Data by government agencies that Company has received in the six (6) months preceding to Customer's request.

1.9. *Onward transfers:* Company shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in compliance with Applicable Data Protection Law (*e.g.*, pursuant to the appropriate Standard Contractual Clauses implemented between the exporter and importer of the Data).

1.10. *Confidentiality of processing:* Company shall ensure that any person that it authorises to process the Data (including Company's staff, agents and subprocessors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. Company shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

1.11. *Security:* Company shall implement appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (a "**Security Incident**"), pursuant to the Company Information Security Policy and pursuant to SOC2 controls and audits. Whilst Company may amend and update the Company Information Security Policy and/or the security measures provided for at Annex II, the Company will not materially decrease the overall security of the Service during the term of the Agreement. Further information on the technical and organisational measures implemented by the Company are set out in Annex II.

1.12. *Subprocessing:* Company shall not subcontract any processing of the Data to a third party subprocessor without the prior written authorisation of Customer. Notwithstanding this, Customer authorises the Company to engage third party subprocessors to process the Data provided that: (i) Company imposes data protection terms on any subprocessor it appoints that protect the Data, in substance, to the same standard provided for by this Clause; and (ii) Company remains fully liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor. Customer hereby provides Company with a general authorisation to engage the subprocessors listed at: https://skai.io/processor-and-service-type/ and Company Affiliates as at the date of this DPA. The Customer shall subscribe to the Company's webpage accessible via https://skai.io/processor-and-service-type/ which provides a mechanism for the Customer to subscribe to notifications of the addition or

replacement of any subprocessors used to process Data. Customer may object to the engagement of a new subprocessor, for reasonable and explained data protection grounds, within 5 business days following Company's notice of the intended change. Where Customer objects on this basis and within this timeframe, Company will make commercially reasonable efforts to provide Customer with the same level of Service without using the new subprocessor. If this is not possible, the parties will work in good faith to find an appropriate solution.

1.13. *Affiliates:* Some or all of Company's obligations under the Agreement may be performed by Company Affiliates.

1.14. *Cooperation and data subjects' rights:* Taking into account the nature of the processing and subject to the applicable retention period(s), Company shall provide all reasonable and timely assistance to Customer to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights, solely to the extent required by the Applicable Data Protection Laws (including its rights of access, correction, objection, erasure, opt out of sale/sharing of personal data and data portability, as and when applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Company, and to the extent it is clear the Customer is the relevant controller, Company shall promptly forward such request to Customer. Customer authorises on its behalf, and on behalf of its controllers when Customer is acting as a processor, Company to respond to any data subject who makes a request to the Company, to confirm that the Company has forwarded the request to the Customer.

1.15. *Data Protection Impact Assessment:* Company shall provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a data protection impact assessment (including a 'risk assessment' or 'privacy impact assessment') in accordance with Applicable Data Protection Law including, if necessary, to assist Customer to consult with its relevant data protection authority or privacy regulator.

1.16. *Security incidents:* Upon becoming aware of a Security Incident, Company shall inform Customer without undue delay and shall provide all such timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Company shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all developments in connection with the Security Incident.

1.17. *Assistance:* Except for negligible costs, Customer will reimburse Company with costs and expenses incurred by Company in connection with the provision of assistance to Customer under this DPA, specifically in relation to Clause 1.14 , 1.15 and 1.65.

1.18. *Deletion of Data:* Within 180 days upon (i) termination or expiry of the Agreement, or (ii) request of the Customer, Company shall destroy all Data (including all copies of the Data) in

its possession or control (including any Data subcontracted to a third party for processing). This requirement shall not apply to the extent that Company is required by any applicable EU (or any EU Member State) or UK law to retain some or all of the Data, in which event Company shall isolate and protect the Data from any further processing except to the extent required by such law until deletion is possible.

1.19. *Audit:* Company will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer, in relation to Company's obligations under this DPA. Company may satisfy the audit obligation under this Clause 1.18 by providing Customer with attestations, certifications or summaries of audit reports conducted by accredited third party auditors. All audits by Customer are subject to the following terms: (i) the audit will be pre-scheduled in writing with Company, at least forty-five (45) days in advance and will be performed not more than once a year (unless the audit is required by a Supervisory Authority); (ii) a third-party auditor will execute a non-disclosure and non-competition undertaking toward Company; (iii) the auditor will not have access to non-Customer data (iv) Customer will make sure that the audit will not interfere with or damage Company's business activities and information and network systems; (v) Customer will bear all costs and expenses related to the audit; and (vi) Customer will receive only the auditor's report, without any Company 'raw data' materials, will keep the audit results in strict confidentiality and will use them solely for the specific purposes of the audit under this DPA; (vii) at the written request of Company, Customer will provide Company with a copy of the auditor's report; and (viii) as soon as the purpose of the audit is completed, Customer will permanently and completely dispose of all copies of the audit report.

1.20. *Term:* This DPA will commence on the later date of its execution or the effective date of the Agreement to which it relates and will continue until the Agreement expires or is terminated.

1.21. *Miscellaneous:* Any alteration or modification of this DPA is not valid unless made in writing and executed by duly authorised personnel of both parties. Invalidation of one or more provisions of this DPA will not affect the remaining provisions. Invalid provisions will be replaced to the extent possible by those valid provisions which achieve essentially the same objectives.

Annex I

Data Processing Description

This Annex I forms part of the Agreement and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): Customer whose name, address and contact details are further set out in the Order Form. The Customer (in its role as a controller) will provide certain personal data in order to receive the Services pursuant to the Agreement.

Processor(s) / Data importer(s): Company whose name, address and contact details are further set out in the Order Form. The Company (in its role as a processor) will process personal data in order to provide the Services pursuant to the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	**Customer's end users interacting with Customers' adds.**
Categories of personal data transferred:	**IP addresses, tracking ID and other performance and attribution data.**
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	**None.**
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	**Continuous.**
Nature of the processing:	**Collection, storage, access, use, alignment or combination, retrieval, consultation, use, disclosure by transmission, erasure or destruction of Data.**
Purpose(s) of the data transfer and further processing:	**As necessary to perform its obligations in accordance with the Agreement and applicable Order Forms.**
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	**As set out in Clause 1.15 of the DPA**
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	**Same as Above**

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	**The competent supervisory authority will be in accordance with clause 13 of the SCCs**

Annex II

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

In the course of Processing Customer Personal Data, Company will implement and maintain commercially reasonable, industry standard technical and organizational measures to protect Customer Personal Data, consistent with applicable laws, that meet or exceed the measures described below, or an equivalent standard of protection appropriate to the risk of Processing Customer Data in the course of providing Company's services, and regularly carry out, test, review, and update all such measures:

Measure	Description
Measures of pseudonymisation and encryption of personal data	**IP addresses are (1) encrypted using AES128 CTR + Hash SHA256 or (2) "Masked" by omitting Last octets**
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Company's system architecture was designed to ensure that no single point of failure exists on any level of the system (network switches, firewalls, load balancers and Proxy servers). Systems are working in active/active and active/passive modes. All data and systems are backed up. Company's backup policy includes: Daily snapshot of every customer's DB with a 3 days retention time. An offsite weekly snapshot AWS's S3 bucket with 3 months retention. Company's RPO and RTO are up to 24 hours. Restores are done and tested on a daily basis.**
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	**Company's business continuity plan (BCP) and disaster recovery plan (DRP) contain the necessary preliminary actions and immediate actions needed for: Natural disasters such as flooding, earthquakes or fire, Men made disaster such as cyber-attacks, malicious acts and human errors.**

	The plans also contain the necessary actions needed to ensure quick and efficient system recovery from failure.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	**Vulnerability scans are done on a monthly basis.** **Penetration tests by 3rd parties are done on an annual basis.** **Vulnerability remediations and patches are done according to the severity. Critical issues are taken care of immediately.**
Measures for user identification and authorisation	**Each Company employee has its own personal username and password.** **All passwords are subject to Company's rules regarding length, rotation, etc.** **Access is based on least privilege principle.** **Access is based on RBAC.** **Access is separated and segmented between environments (Production, Dev, QA).** **Remote access is done via encrypted VPN with 2 Factor Authentication**
Measures for the protection of data during transmission	**All data in transit is encrypted via HTTPS, SFTP and secure API.** **Company uses TLS1.1/1.2.**
Measures for the protection of data during storage	**All data and systems are backed up.** **Company's backup policy includes:** **Daily snapshot of every customer's DB with a 3 days retention time.** **An offsite weekly snapshot AWS's S3 bucket with 3 months retention.** **Backups are encrypted.** **Access to backups is limited and based on least privilege.**
Measures for ensuring physical security of locations at which personal data are processed	**Company's Data center facility hosted in a closed private cage.** **Doors are always locked. Guarded 24/7 by security personnel.** **Company uses Universal Power Supply (UPS).** **Company uses Fire suppression / alert systems**

	Company uses CCTV system for surveillance with motion detection. **Access to the facility is permitted only to authorized support employees using a biometric authentication.** **All visitors are registered at the entrance and identified with an ID card.** **Visitors are escorted during their stay in the facility.**
Measures for ensuring events logging	**Security events logs are kept audited on a regular basis.** **Logs are sent to a SIEM system which monitors network anomalies and user behaviour violations.** **Logs are protected and cannot be changed or deleted.** **All login attempts are logged and audited.** **Logs are stored for at least 12 months.**
Measures for ensuring system configuration, including default configuration	**Configuration changes are done upon approvals.** **Test and QA are done in separated environment prior to implementation in production environment.** **Default users and password are being deleted.** **Default access and ports are being blocked.**
Measures for internal IT and IT security governance and management	Company is ISO27001 and SOC2 certified. IT security governance and management are based on these certifications
Measures for certification/assurance of processes and products	**SDLC process.** **Every fix and patch go through the following SDLS steps:** **Analysis** **Design** **Implementation** **Testing** **Deployment** **Maintenance**
Measures for ensuring data minimisation	**Data collection is limited only to what is required to fulfil the specific purpose.** **Data minimisation is assured during our SDLC process at the HLD, data design, code-review and testing phases.**
Measures for ensuring data quality	**Every customer has its own separated application and DB servers.**

	Customer can login and access only to its servers.
Measures for ensuring limited data retention	**Upon request and pursuant to contractual obligations, Company is able to completely and permanently delete specific or all Customer Personal Data from its systems. The deletion process includes deleting the APP& DB followed by deleting its relevant volumes and data, disabling backup and then delete all backups, including from DR sites.**
Measures for ensuring accountability	**Company has in place internal policies containing formal instructions for data processing procedures;** **Company carefully vets its relevant contractors with regard to data security;** **Company's personnel are being vetted prior to engagement and trained periodically to maintain awareness regarding data protection and security requirements.**
Measures for allowing data portability and ensuring erasure	**Company can import or delete all the Customer's data upon its written request.** **Data shall be verifiably deleted. Where appropriate, company shall wipe, degauss or securely destroy hardware by shredding hardware for electronic devices.**

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

If Customer provides Company with the relevant ID, such a s cookie ID, then Company is able to locate the relevant data subject and assist the Customer with the exercise of is rights (or delete such data itself).