PILOT TERMS AND CONDITIONS
Version January 2025

These Pilot Terms and Conditions ("Agreement") govern the use of the Platform and Services (collectively, "Services") provided by **Bager Technology Inc.,** identification number: 10077360, with its registered office at 166 Geary Street, Ste 1500, San Francisco, CA 94108 US, or any affiliate ("Company", "we", "us", or "our") to you ("Customer", "you", or "your") and your relationship with us. By accessing or using our Services, or by accepting an Order through any electronic means, including payment via Stripe or another designated platform, you agree to be bound by this Agreement:

IF YOU DO NOT AGREE TO THIS AGREEMENT, YOU MUST NOT ACCESS OR USE OUR SERVICES.

We agree to provide access to Services as specified in an Order. This pilot is designed to allow the Customer to assess the Services in a test environment before entering into a full commercial agreement.The Customer agrees to pay the Fees and comply with these Agreement.

1. **Definitions**

For purposes of this Agreement, the following terms are defined as follows:

Company: The entity providing the Services, as defined above, or any of its affiliates associated with the Company.

Customer: The entity accessing and using the Services provided by the Company. The Services are for the Customer's use only. If any Customer´s affiliate wants to use the Services, they must sign a separate agreement with the Company. The Customer may not share or extend access to its affiliates without prior written approval of the Company.

Platform: The online service platform "Kale – AI-powered Contextual Sourcer" provided by the Company, which offers various functionalities as outlined in this Agreement, or any other document specifying the Platform's feature..

Services: All services provided by the Company through the Platform, including any support, maintenance, updates, or new features, as specified in an Order.

Intellectual Property Rights: All patents, copyrights, trademarks, trade secrets, know-how, and any other proprietary rights related to the Services or the Platform.

Order: An applicable order, agreement, or subscription confirmation detailing the specific Services and terms agreed upon between and fully executed by the Company and the Customer. The order's terms and conditions take precedence in case of any conflict with the terms of this Agreement.

Fees: The charges payable by the Customer for using the Services, as specified in an Order.

Trial: A period where the Services are provided free of charge before transitioning to a paid subscription, if applicable.

Force Majeure: Any event beyond the reasonable control of the Company that prevents or delays the performance of its obligations under this Agreement, including but not limited to natural disasters, wars, strikes, labor disputes, civil disturbances, pandemics, governmental actions, network failures.

Confidential Information: All and any non-public, proprietary, sensitive information, financial, payment or personal data, trade secrets, or know-how, disclosed by the other party, whether in written, oral, or electronic form, that is identified as confidential or should reasonably be considered confidential given its nature and the circumstances of disclosure.

2. License

2.1 Subject to your compliance with the terms of this Agreement, the Company grants you, for the duration of this Agreement, a limited, non-exclusive, non-transferable, revocable license to access and use the Services and Platform exclusively for lawful business purposes, by the terms, conditions, and limitations set forth herein. The license granted under this Agreement shall automatically terminate upon the expiration or termination of the Agreement. Upon such termination, you shall immediately cease using the Services and Platform.

2.2 The Services and Platform, including all associated Intellectual Property Rights, remain the exclusive property of the Company or its licensors. You are granted only the limited rights expressly outlined in this Agreement, and no additional rights or interests are granted to you under this Agreement. However, you retain full ownership over any data you upload or process via the Platform.

2.3 Any feedback, suggestions, or recommendations ("Feedback") provided by the Customer regarding the Services, Platform, or Company's performance shall be the exclusive property of the Company. The Customer acknowledges that:

- Feedback is provided voluntarily and without expectation of compensation.
- The Company has the right to use, modify, and incorporate Feedback into its products, services, or operations without restriction.

2.4 Customer grants the Company the right to use the Customer's name, logo, and trademarks for marketing, promotional, and advertising purposes, including but not limited to the Company's website, brochures, and case studies, solely to promote the Company's services. The Company will not use the Customer's branding in a manner that could harm the Customer's reputation.

3. Pilot Phase Services Commitment

3.1 The Company is committed to providing reliable, secure, and compliant service while continuously improving the Services. As the Platform is pilot and remains in its early development stage, the Company will use commercially reasonable efforts, consistent with industry standards, to minimize errors and interruptions. However, in the pilot stage, Customer acknowledges that the Services may experience temporary unavailability due to scheduled or emergency maintenance, system adjustments, unforeseen technical challenges, or other factors beyond the Company's control. The Company may, but is not obligated to, provide advance notice of scheduled disruptions. During the pilot phase, the Company shall:

- Maintain Services availability, with occasional downtime for updates, bug fixes, and improvements. Reasonable efforts will be made to minimize disruptions and notify users of significant maintenance. The Company may modify, update, add, or remove features of the Platform at its discretion during the Pilot phase without prior notice or liability.
- Implement and continuously improve security measures to protect user data in compliance with applicable laws.
- Monitor system performance and address issues as they arise to ensure stability, understanding that fluctuations may occur.
- Investigate and resolve security incidents or service disruptions promptly, prioritizing user data protection and compliance.
- Regularly update the Services based on user feedback, technological advancements, and compliance requirements, with Customer/ users acknowledging that features, functionality, and performance may evolve.
- Provide reasonable support to Customer/ users, with response times subject to resource availability during the early stage of development.
- Update services level commitments as the Platform scales, reflecting enhanced capabilities and reliability.

3.2 The Customer shall use the Services and Platform solely for lawful business purposes, in compliance with all applicable laws, regulations, and industry standards, including those governing intellectual property, privacy, data protection, and non-discrimination. Accordingly, you agree mainly, but not limited to:

- Ensure that all activities conducted through the Services are lawful, ethical, and non-discriminatory. You shall not use the Services to engage in any illegal, fraudulent, defamatory, harassing, or otherwise prohibited conduct.
- Only upload, process, or store content for which you have obtained all necessary rights, licenses, or permissions, ensuring compliance with GDPR, the Data Protection Act, and other applicable data protection laws. Additionally, you are solely responsible for ensuring that all data shared with the Platform is compliant with data protection laws and with EXHIBIT 1.
- Ensure that any data, content, or materials used within the Platform do not infringe upon third-party intellectual property, privacy, or other legal rights.
- Use the Services in a manner that does not disrupt, interfere with, or compromise the security, integrity, or performance of the Platform. You shall not introduce malware, or harmful code, or engage in activities that impose an excessive burden on the system.
- You shall not reverse engineer, decompile, modify, sublicense, resell, transfer, lease, or otherwise grant or facilitate unauthorized access to the Services or Platform. Any sharing, assignment, or provision of access to third parties is prohibited unless expressly authorized in writing by the Company.
- Ensure that your use of the Services remains fair, does not disrupt other users, and does not circumvent any access controls or usage limitations implemented by the Company.

Violation of this provision may result in suspension or termination of access to the Services without the Company's liability.

4. **Term**

4.1 The term of these Agreement shall begin on the date on which both parties sign this Agreement, or the date the Customer first accesses or uses the Services, whichever is earlier (the "Effective date") and shall continue for the period specified in the applicable Order (the "Initial Term"), unless terminated earlier following this Section. If no term is specified, the Initial Term shall be 1 (one) month.

4.2 Unless either Party provides written notice of its intent not to renew the Agreement at three (3) days prior to the expiration of the Initial Term or any renewal Term, this Agreement shall automatically renew for successive periods (each a "Renewal Term"). The Company may adjust the fees for the Services at the time of renewal, provided that any fee increase shall be communicated to the Customer in writing at least three (3) days before the renewal. The Customer may terminate the Agreement within ten (10) days of receiving the renewal fee notice.

5. **Payment terms**

5.1 The Fees for the Services will be as specified in the applicable Order, without VAT in EUR, and are non-refundable unless otherwise stated in this Agreement. The Fees are determined based on the specific Services selected, including any features, functionalities, or number of authorized users outlined in the Order. If no Order is in place, the Services will be billed in full according to the applicable plan selected by the Customer.

5.2 For subscription-based Services, invoices will be issued monthly in advance, unless otherwise agreed in the applicable Order. For one-time Services, invoices will be issued upon completion of the service. All payments are due within thirty (30) days from the invoice date. Subscription fees will be automatically charged at the start of each billing cycle. Full payment is required at the time of purchase for credit card payments. All payments must be fully received within the specified due date.

5.3 Payments may be made via the following methods: Credit/Debit Card, Apple Pay, Google Pay, SEPA, ACH (via Stripe), Bank Transfer / Wire Transfer, SEPA Direct Debit (for EU customers, any other payment method as agreed in the Order.

5.4 By providing payment details, the Customer authorizes the Company to automatically charge applicable fees via the selected payment method at the beginning of each billing cycle. The Customer is responsible for maintaining valid payment details.

5.5 The Customer shall be solely responsible for all taxes, duties, levies, and other governmental charges (including VAT, sales tax, and withholding tax) related to the Services, excluding taxes based on the Company's income. The Customer agrees to pay any such taxes or reimburse the Company for any amounts the Company is required to pay on the Customer's behalf. The Customer agrees to bear responsibility for any bank charges, transaction fees, or additional costs resulting from payment issues

5.6 Unpaid amounts may incur a finance charge of 1.5% per month (or the maximum rate permitted by law, if lower), in addition to all costs of collection, including late interest, and reasonable attorney's fees. You must notify us in writing of

any fee disputes within thirty (30) days of receiving the first invoice in question. If no dispute is raised within this period, the charges will be deemed accepted and final. We may, at our sole discretion, consider disputes raised outside of this period.

5.7 The Customer may not withhold, offset, or deduct any payments due under this Agreement, except where required by law.

6. **Termination**

6.1 Either Party may terminate this Agreement immediately upon written notice if the other Party (i) materially breaches this Agreement and fails to remedy the breach within 15 (fifteen) days of written notice, (ii) fails to provide the agreed-upon Services or functionality (for the Company) or fails to make required payments (for the Customer) within 15 (fifteen) days of notice, or (iii) becomes insolvent, files for bankruptcy, or has a receiver/trustee appointed over its assets. Either Party may also terminate this Agreement if a Force Majeure event prevents performance for more than 30 (thirty) days. In such cases, neither Party is liable for damages, but outstanding obligations remain due. In addition, the Company may also terminate the Agreement at any time by giving Customer notice of termination.

6.2 The Company reserves the right to suspend the Customer's access to the Services at any time if the Customer fails to make any payment when due, or if the Customer breaches any material provision of this Agreement. Suspension will remain in effect until the breach or payment issue is remedied to the Company's satisfaction. The Company may also suspend the Services immediately if it determines, in its sole discretion, that the Customer's use of the Services poses a security risk to the Company's network, systems, or other customers, or if the Customer engages in activities that may harm the Company's reputation, operations, or services.

6.3 Upon termination of this Agreement for any reason, the Customer agrees to immediately cease using the Services, at the Company's discretion, either return or destroy any copies of the software, documentation, and any other materials related to the Services that are in its possession or control. The Customer shall pay the Company any fees due and owing under this Agreement for Services rendered up to the termination date. All outstanding amounts shall become immediately due and payable upon termination.

6.4 For any Services or engagements that extend beyond the scope of the pilot phase, a formal written commercial agreement shall be executed between the Customer and Company. Such a commercial agreement will outline the specific terms, scope, deliverables, payment terms, and any other applicable conditions related to the additional services.

6.5 **Post-Termination Obligations**

The Customer's obligations under this Agreement, including payment obligations, license and confidentiality provisions, shall survive the termination of this Agreement. If the Customer terminates this Agreement for any reason other than a material breach by the Company, the Customer shall not be entitled to any refund of fees already paid.

7. Warranties, Limitation of Liability and Indemnifications

7.1 The Customer acknowledges that the Platform and Services are provided on a limited, pilot/trial basis for evaluation purposes only. Notwithstanding the foregoing, the Platform and Services are provided on an "as is" and "as available" basis, without any warranties of any kind. To the maximum extent permitted by law, the Company, including its affiliates, licensors, and subcontractors, expressly disclaims all warranties, whether express, implied, statutory, or otherwise, including, but not limited to:

(i) Implied warranties of merchantability, fitness for a particular purpose, non-infringement, and title,

(ii) Any warranties related to availability, uptime, accuracy, security, or error-free operation.

(iii) Any warranties arising from the course of dealing, usage, or trade practice.

The Company does not warrant that the Platform or Services will meet Customer's specific requirements, operate without interruption, or be free from security vulnerabilities, cyber threats, or unauthorized access. The Company is not responsible for any loss, corruption, or alteration of data transmitted through or stored within the Platform.

7.2 **Limitation of Liability**

To the maximum extent permitted by law, neither the Company nor its affiliates, officers, employees, licensors, service companies, or subcontractors, shall be liable for (i) any indirect, incidental, consequential, punitive, or special damages; (ii) any loss of profits, revenue, business, goodwill, or anticipated savings; (iii) any data loss, corruption, breach, or security failures; (iv) any downtime, service failures, or business interruptions; (v) or any other damages arising from the Customer's use of, or inability to use, the Platform or Services; whether based in Agreement, tort (including negligence), strict liability, or otherwise—even if the Company has been advised of the possibility of such damages.

7.3 In no event shall the total aggregate liability of the Company, including its affiliates, licensors, and subcontractors, exceed the total fees paid by the Customer for the Services in the 1 (one) month preceding the event giving rise to the claim, or EUR 100 (one hundred) (or its equivalent in local currency), whichever is lower.

7.4 To the fullest extent permitted by law, the Company and its affiliates shall not be liable for any claims, fines, or damages arising from Customer's failure to comply with this Agreement, laws, data protection regulations, or intellectual property rights.

7.5 **Indemnification**

The Customer agrees to indemnify, defend, and hold harmless the Company, its affiliates, officers, employees, licensors, subcontractors, and agents from and against any and all claims, demands, liabilities, losses, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or related to: (i) Customer's breach of this Agreement or any applicable laws or regulations; (ii) Customer's misuse or unauthorized use of the Platform or Services; (iii) Customer's violation of any third-party rights, including intellectual property, privacy, or data protection rights; (iv) Any negligent, fraudulent, or wrongful acts by the Customer, its employees, contractors, or agents; or (v) any third party claims related to intellectual property infringement and data breaches caused by Customer's use of the Platform.

7.6 The Company reserves the right to assume exclusive control over the defense of any matter subject to indemnification, at the Customer's expense, and the Customer agrees to cooperate fully in such defense.

8. **Miscellaneous**

8.1 **Personal Data Processing**

To the extent the provision of Services involves the processing of Personal Data, the Data Processing Addendum ("DPA") attached as Exhibit 1 to this Agreement shall apply to such processing and shall form an inseparable part of this Agreement.

8.2 **Governing Law**

This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic, without regard to its conflict of laws principles. Any disputes arising out of or in connection with this Agreement shall be subject to the exclusive jurisdiction of the courts located in Bratislava, Slovak Republic, and the Customer hereby consents to such jurisdiction and waives any objections thereto.

8.3 **Amendments, Policies, and Conflicting Terms**

The Company reserves the right to amend, modify, or update this Agreement, along with any related policies or guidelines, at its sole discretion, without prior notice to the Customer, except where required by law. Any such amendments will be effective immediately upon posting on the Company's website or through the Platform. Continued use of the Services after the posting of revised Agreement constitutes the Customer's acceptance of the updated terms.

The Customer acknowledges that any policies, guidelines, instructions, or rules issued by the Company from time to time are an integral part of this Agreement and shall be binding upon the Customer. The Company may issue such policies or modifications as it deems necessary, and the Customer is responsible for reviewing and complying with them.

In the event of any conflict between the terms of this Agreement and any other document or communication provided by the Customer, including but not limited to purchase orders, invoices, or other correspondence, the terms of this Agreement shall prevail, unless expressly agreed to in writing by an authorized representative of the Company. Any modifications, additions, or terms proposed by the Customer shall be deemed null and void unless specifically accepted by the Company in writing. The execution or fulfilment of any order or agreement by the Company shall not be construed as acceptance of such conflicting terms.

8.4 **Confidentiality**

Each party agrees to maintain the confidentiality of Confidential Information. The receiving party shall not disclose, use, or permit access to Confidential Information except as necessary to fulfil its obligations under this Agreement and shall take reasonable measures to protect it from unauthorized use or disclosure, at least to the same extent it protects its own confidential information. Confidential Information does not include information that was lawfully in the receiving party's possession before disclosure, becomes publicly available through no fault of the receiving party, is lawfully obtained from a third party without confidentiality obligations, or is independently developed without the use of the disclosed information. If disclosure is required by law, regulation, or court order, the receiving party shall provide prior notice to the disclosing party (where legally permitted) and disclose only the minimum necessary. These confidentiality obligations shall survive for five (5) years after termination of this Agreement or for as long as the information remains confidential. The Customer agrees that, during the term of this Agreement and for five (5) years, or the maximum period allowed by law after its termination, it will not develop, use, or assist in developing any product or service that competes with the Company's Services based on the Company's Confidential Information or Intellectual Property Rights. The Customer shall not reverse-engineer, copy, or use any of the Company's technology or methods for competitive purposes. This does not apply to products or services independently developed without using the Company's Confidential Information or Intellectual Property Rights.

8.5 This Agreement, together with Order, any addendums, amendments, or policies issued by the Company, constitutes the entire understanding between the Parties and supersedes all prior or contemporaneous agreements, communications, or proposals, whether oral or written.

8.6 If any provision of this Agreement is found to be invalid, illegal, or unenforceable, that provision shall be severed, and the remaining provisions shall continue in full force and effect.

8.7 The Company may assign or transfer its rights and obligations under this Agreement without the Customer's prior consent. The Customer may not assign or transfer its rights or obligations under this Agreement without the prior written consent of the Company.

8.8 Nothing in this Agreement shall be construed as creating a partnership, joint venture, agency, or employment relationship between the parties. The Customer has no authority to bind the Company in any manner.

EXHIBIT A - DATA PROCESSING ADDENDUM

1. Introduction

This Data Processing Addendum ("**DPA**") will be effective from the effective date of the Agreement or from the date the Customer is provided with access to the Services, whichever is sooner, and will apply to any processing of Personal Data by the Company. This DPA applies where Company processes Personal Data as a Processor on behalf of Customer to provide the Services and such Personal Data is subject to Applicable Data Protection Laws.

2. Definitions

For purposes of this DPA, the following terms are defined as follows:

Definitions	
Adequate Country	A country or territory that is recognized under European Data Protection Laws as providing adequate protection for Personal Data.
Applicable Data Protection Laws	All laws and regulations that are applicable to the processing of Personal Data under the Agreement, including European Data Protection Laws and the US Data Protection Laws.
Controller	An entity that determines the purposes and means of the processing of Personal Data, and includes "controller," "business," or analogous term as defined under the Applicable Data Protection Laws.
EU SCCs	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.
European Data Protection Laws	All laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom applicable to the processing of Personal Data under the Agreement (including, where applicable, (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 (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 and the UK Data Protection Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii), (iii), (iv).
Personal Data	Any information relating to an identified or identifiable natural person.
processing, **data subject**, **supervisory authority**	Shall have the meanings ascribed to them in European Data Protection Law.
Processor	Entity which processes Personal Data on behalf of the Controller, including an entity to which another entity discloses a natural individual's personal information for a business purpose pursuant to a written contract that requires the entity receiving the information to only retain, use, or disclose Personal Data information for the purpose of providing the Services, and includes "processor," "service provider," or analogous term defined under the Applicable Data Protection Laws.
Restricted Transfer	(i) where the EU GDPR or Swiss FADP applies, a transfer of Personal Data from the European Economic Area or Switzerland (as applicable) to a country outside of the European Economic Area or Switzerland (as applicable) which is not subject to an adequacy determination by the European Commission or Swiss Federal Data Protection and Information Commissioner (as applicable); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018. For the avoidance of doubt, a transfer of Personal Data to the United States pursuant to the Data Privacy Framework shall not be a Restricted Transfer.
Subprocessor	Any third party engaged by Company to assist in fulfilling its obligations with respect to providing the Services and that processes Personal Data as Processor.
UK Addendum	The International Data Transfer Addendum (Version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK Data Protection Act 2018, as updated or amended from time to time.
US Data Protection Laws	All laws and regulations of the United States applicable to the processing of Personal Data under the Agreement, including (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 - 1798.199, 2022) and its implementing regulations (collectively, the "CCPA"); (ii) any other United States state or federal data protection laws; and (iii) all laws implementing or supplementing the foregoing.

3. Status of the parties

3.1 Each party will comply with and provide the same level of privacy protection regarding the Personal Data as required by the Applicable Data Protection Laws.

3.2 In respect of the parties' rights and obligations under this DPA, the parties acknowledge and agree that the Customer is the Controller and Company is a Processor. To the extent the CCPA is applicable, Customer is the "business" and Company is the "service provider".

4. Customer's instructions

4.1 Customer, as the Controller, will ensure that its instructions to the Processor for processing Personal Data complies with Applicable Data Protection Laws. Any use of the Services, together with the Agreement, shall be deemed as the Controller's instruction to the Processor.

4.2 Customer acknowledges that Company is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Company's provision of the Services meets or will meet the requirements of such laws or regulations.

4.3 Customer warrants that Company's processing in accordance with Customer's instructions will not cause Company to violate any applicable law or regulation, including Applicable Data Protection Law.

4.4 Any additional instructions outside the scope of the Agreement will be agreed to between the parties in writing, including any additional fees that may be payable by Customer to Company for carrying out such additional instructions.

5. Company obligations

5.1 With respect to Personal Data it processes in its role as a Processor, Company shall:

a) only process Personal Data for the limited and specified business purpose of providing the Services and in accordance with: (i) the Customer's written instructions as set out in the Agreement, unless required to do so by applicable Union or Member State law to which Company is subject, and (ii) the requirements of Applicable Data Protection Laws;

b) not use the Personal Data for the purposes of marketing or advertising;

c) implement technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include measures set out in Annex 2 ("**Technical and Organizational Measures**"). Customer acknowledges that the Technical and Organizational Measures are subject to technical progress and development and that Company may update or modify the Technical and Organizational Measures from time to time;

d) without undue delay notify the Customer upon becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed for the purpose of providing the Services to Customer by Company, its Subprocessors, or any other identified or unidentified third party (a "**Personal Data Breach**") and provide the Customer with reasonable cooperation and assistance in respect of that Personal Data Breach;

e) other than to the extent required to comply with applicable law, following termination or expiry of the Agreement, to delete or return Personal Data (including copies thereof) processed pursuant to this DPA at Customer's written request.

5.2 To the extent that Company is processing Personal Data on behalf of the Customer within the scope of the CCPA, Company makes the following additional commitments to Customer: Company will not retain, use, or disclose that Personal Data for any purposes other than the purposes set out in the Agreement and as permitted under the CCPA, including under any "sale" exemption. Company will not "sell" or "share" such Personal Data, as those terms are defined in the CCPA. This clause 5.2 does not limit or reduce any data protection commitments Company makes to Customer in the Agreement.

6. Subprocessing

6.1 Company will disclose Personal Data to Subprocessors only for the specific purpose of providing the Services.

6.2 Company will ensure that any Subprocessor it engages to provide an aspect of the Service on its behalf in connection with this Agreement does so only on the basis of a written contract.

6.3 Customer grants a general written authorization to Company to appoint Subprocessors to process Personal Data on Customer's behalf.

6.4 Company will notify the Customer at least ten (10) days prior to the date on which those Subprocessors commence processing of Personal Data. If Customer objects to any new or replacement Subprocessor on reasonable grounds related to data protection, it shall notify Company of such objections in writing within ten (10) days of the notification and the parties will seek to resolve the matter in good faith.

7. Audit and records

7.1 Company shall, in accordance with Applicable Data Protection Laws, make available to Customer such information in Company's possession or control as Customer may reasonably request with a view to demonstrating Company's compliance with the obligations of Processors under Applicable Data Protection Laws in relation to its processing of Personal Data.

7.2 Company may fulfill Customer's right of audit under Applicable Protection Laws in relation to Personal Data, by providing:

a) an audit report not older than thirteen (13) months, prepared by an independent external auditor demonstrating that Company's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard, if available;

b) additional information in Company's possession or control to a data protection supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by Company under this Agreement.

c) to the extent that Customer's Personal Data is subject to the EU SCCs and the information made available pursuant to this clause 7.2 is insufficient, in Customer's reasonable judgment, to confirm Company's compliance with its obligations under this Agreement or Applicable Data Protection Laws, then Company shall enable Customer to request one onsite audit per annual period during the term of the Agreement to verify Company's compliance with its obligations under this Agreement in accordance with clause 7.3.

7.3 The following additional terms shall apply to audits the Customer requests:

a) Customer must send any requests for review of Company's audit reports to privacy@trykale.com.

b) Audit shall last no longer than the equivalent of 1 working day (8 hours) of Company's representative.

c) Company may charge a fee based on Company's reasonable costs.

7.4 Company may object in writing to an auditor appointed by Customer to conduct any audit under clause 7.2 c) if the auditor is, in Company's reasonable opinion, not suitably qualified or independent, a competitor of Company, or otherwise manifestly unsuitable (i.e., an auditor whose engagement may have a harmful impact on Company's business comparable to the aforementioned aspects). Any such objection by Company will require Customer to appoint another auditor or conduct the audit itself. If the EU SCCs (including as they may be amended in Section 8. below) applies, nothing in this clause 7.3. varies or modifies the EU SCCs nor affects any supervisory authority's or data subject's rights under the EU SCCs.

8. Data transfers

The parties agree that when the transfer of Personal Data protected by European Data Protection Laws from Customer or its Affiliate to Company is a Restricted Transfer, then the appropriate standard contractual clauses and additional safeguards shall apply as follows:

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

(i) Module Two will apply;

(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 6.4. of this DPA;

(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 Slovak law;

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

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA; and

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA.

(b) **UK Transfers:** in relation to Personal Data that is protected by the UK GDPR, the EU SCCs, completed as set out above in clause 6.1(a) of this DPA, shall apply to transfers of such Personal Data, except that:

(i) The EU SCCs shall be deemed amended as specified by the UK Addendum, which shall be deemed executed between the transferring Customer (or affiliate) and Company;

(ii) Any conflict between the terms of the EU SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum;

(iii) For the purposes of the UK Addendum, Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed using the information contained in the Annexes of this DPA; and

(iv) Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party."

9. Limitation of Liability

Except as expressly set forth in Section 10. below, to the maximum extent permitted by law, Company's and its affiliates' aggregate liability towards Customer arising out of or in connection to this DPA (including EU SCCs), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability (including any agreed aggregate financial cap) set forth under the Agreement. For the avoidance of doubt, nothing in this DPA is intended to limit the rights a Data Subject may have against Company arising out of Company's breach of the EU SCCs, where applicable.

10. Indemnity

Notwithstanding anything else to the contrary in the Agreement, the Customer shall fully indemnify and hold the Company harmless from and against all expenses, liabilities, claims, or losses arising from Customer's breach of warranty in clause 4.3.

11. General

11.1 This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

11.2 Except where and to the extent expressly provided in the EU SCCs or required as a matter of Applicable Data Protection Laws, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

11.3 This DPA and any action related thereto shall be governed by and construed in accordance with the laws as specified in the Agreement, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts specified in the Agreement.

11.4 If any provision of this DPA is, for any reason, held to be invalid or unenforceable, the other provisions of the DPA will remain enforceable. Without limiting the generality of the foregoing, Customer agrees that clause 9. (Limitation of Liability) and 10. (Indemnity) will remain in effect notwithstanding the unenforceability of any provision of this DPA.

11.5 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter.

Annex 1

Data Processing Description

This Annex 1 forms part of the DPA and describes the processing that Company will perform on behalf of Customer.

A. LIST OF PARTIES

Data exporter(s):

Name: Customer and any Customer Affiliates described in the Agreement.	As stated in the Agreement or Order.
Address: Addresses of Customer and any Customer Affiliates described in the Agreement (or otherwise notified by Customer to Company)	As stated in the Agreement or Order.
Contact person's name, position and contact details:	As stated in the Agreement or Order.
Activities relevant to the data transferred under this DPA and the EU SCCs:	Use of the Service pursuant to the Agreement.
Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.
Role (controller/processor):	Controller

Data importer(s):

Name:	As stated in the Agreement or Order.
Address:	As stated in the Agreement or Order.
Contact details:	privacy@trykale.com
Activities relevant to the data transferred under this DPA and the EU SCCs:	Processing necessary to provide the Service to Customer pursuant to the Agreement.
Signature and date:	This Annex 1 shall be deemed executed upon execution of the DPA.
Role (controller/processor):	Processor

B. DESCRIPTION OF DATA PROCESSING AND TRANSFER

Categories of data subjects:	● Customers' employees, agents, or contractors who access or use the Services. ● Job candidates, current and former members of staff.
Categories of Personal Data:	● Identification and contact data (name, email address); IT related data (computer ID, user ID, password, IP address, log files). ● Identification and contact data (name, email address); mobile telephone numbers; web address; email address; date of birth and birth place; gender; education, language(s) and special competencies; certification information; probation period and employment duration information; job or position title; business title; job type or code; business site; company, supervisory, cost center and region affiliation; work schedule and status (full-time or part-time, regular or temporary); employment history; work experience information; accomplishment information; award information.
Sensitive data:	Company does not require any special categories of data to provide the Services and does not intentionally collect or process such data in connection with the provision of the Services.
The frequency of the transfer:	Continuous for the duration of the Agreement.
Nature of the processing:	Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and this DPA.

Purpose(s) of the data transfer and further processing:	Processing necessary to provide the Services to Customer in accordance with the documented instructions provided in the Agreement and this DPA.
The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Until the earliest of (i) expiry/termination of the Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Agreement (to the extent applicable).
Subject matter, nature and duration of the processing:	The subject matter, nature and duration of the processing shall be as specified in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Competent supervisory authority:	● EU SCCs: competent supervisory authority determined in accordance with Clause 13 of the EU SCCs. ● UK Addendum: means the UK Information Commissioner's Office.

Annex 2
Technical and Organizational Measures

1. Measures for User Identification and Authorization

- Allocates privileges based on roles and follows the principle of least privilege access.

2. Measures for System Configuration

- Aligning configuration baselines with industry best practices (e.g., CIS Level 1 benchmarks).
- Implementing strict change control processes with auditing and regular checks.
- Configuring systems with least privilege and default "deny-all" access settings.

3. Measures for Protection of Data During Transmission

- Utilizes transport encryption protocols.
- Employs public-key certification authorities and infrastructure.
- Implements protective measures against attacks, such as firewalls, mutual TLS encryption, and API authentication.
- Uses effective encryption algorithms (e.g., 128-bit symmetric and 2048-bit RSA or 256-bit ECC for asymmetric encryption).
- Ensures proper software implementation and vulnerability management.
- Enforces secure key management practices.
- Audits, logs, and tracks data transmissions.

4. Measures for Protection of Data During Storage

- Utilizes encryption protocols and trustworthy public-key certification authorities.
- Regularly tests systems for vulnerabilities and possible backdoors.
- Employs strong encryption methods (e.g., AES-XTS with 128-bit or longer keys).
- Maintains proper key management and software implementation.
- Identifies and authorizes systems and users accessing data storage.
- Logs and monitors access to storage systems.

5. Measures for Encryption of Personal Data

- encryption protocols designed to provide effective protection against active and passive attacks with resources known to be available to public authorities;
- public-key certification authorities and infrastructure;
- encryption algorithms and parameterization, such as a minimum of 128-bit key lengths for symmetric encryption, and at least 2048-bit RSA or 256-bit ECC key lengths for asymmetric algorithms.

6. Measures for Testing and Evaluating Technical and Organizational Measures

- Conducting internal audits and risk assessments.

7. Measures for Event Logging

- Authenticating authorized personnel with strong multi-factor authentication.
- Maintaining updated lists of system administrators.
- Detecting, assessing, and responding to high-risk anomalies.
- Keeping access logs for twelve months.
- Regularly testing logging configurations, monitoring systems, and incident response processes.

8. Measures for Internal IT and IT Security Governance

- Keeping documentation for audits and ensuring compliance with technical and organizational measures.

9. Measures for Sub-Processor Transfers

- Specific technical and organizational measures are taken by sub-processors to assist the controller (and data exporter for processor-sub-processor transfers).

10. Measures for Physical Security of Locations

- Logs and monitors access to data centers where Personal Data is hosted.
- Secures data centers with alarm systems and other appropriate security measures.

11. Measures for Data Availability and Access Recovery

- disaster-recovery and business continuity plans and procedures;
- geographically-distributed data centers;
- redundant infrastructure, including power supplies and internet connectivity;
- backups stored at alternative sites and available for restore in case of failure of primary systems; and
- incident management procedures that are regularly tested.

13. Measures for Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services

- code review process to increase the security of the code used to provide the Services; and testing code and systems for vulnerabilities before and during use;

- using checks to validate the integrity of encrypted data;
- employing preventative and reactive intrusion detection;
- high-availability systems across geographically-distributed data centers;
- measures to protect and maintain the confidentiality of Personal Data including:
  - an authorization policy for the input, reading, alteration and deletion of data;
  - authenticating authorized personnel using unique authentication credentials (passwords) and hard tokens;
  - automatically signing-out user IDs after a period of inactivity;
  - protecting the input of data, as well as the reading, alteration and deletion of stored data; and
  - requiring that data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked and secure.