Data Processing Addendum

This Data Processing Addendum ("**DPA**") amends and is part of the Terms and Conditions (the "**Agreement**") between Work Nexus Labs Limited, trading as Zaro, a company incorporated in England and Wales with registered address at 3rd Floor 1 Ashley Road, Altrincham, Cheshire, United Kingdom, WA14 2DT ("**Service Provider**"), and the customer listed on the Order Form ("**Company**"). This DPA prevails over any conflicting terms of the Agreement but does not otherwise modify the Agreement.

1. Definitions

1.1 In this DPA:

(a) "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process**/**Processing**", "**Processor**", and "**Supervisory Authority**" have the meaning given to them in the GDPR;

(b) "**Company Personal Data**" means any Personal Data, the Processing of which is subject to Data Protection Law, for which Company is the Controller, and which is Processed by Service Provider in the context of the Services under the Agreement;

(c) "**Data Protection Law**" means all applicable legislation relating to data protection and privacy, including the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**EU GDPR**"), the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR", and together with the EU GDPR, the "GDPR"), the Data Protection Act 2018, the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) on Privacy and Electronic Communications and the UK Privacy and Electronic Communications (EC Directive) Regulations 2003 and their national implementations in the European Economic Area ("**EEA**"), the United Kingdom ("UK") and any other applicable jurisdiction, together with any successor or implementing legislation, in each case as applicable and as may be amended or replaced from time to time;

(d) "**Data Subject Rights**" means Data Subjects' rights as set out in Data Protection Law;

(e) "**International Data Transfer**" means any transfer of Company Personal Data from the EEA, Switzerland or the UK to an international organization or to a country outside of the EEA, Switzerland and the UK;

(f) "**Services**" means the services provided by Service Provider to Company under the Agreement; and

(g) "**Subprocessor**" means a Processor engaged by Service Provider to Process Company Personal Data.

1.2 Words and expressions used in this DPA shall have the same meaning as is given to them in the Agreement unless the context otherwise expressly requires.

2. Scope and applicability

2.1 This DPA applies to Processing of Company Personal Data by Service Provider to provide the Services.

2.2 The subject matter, nature and purpose of the Processing, the types of Company Personal Data and categories of Data Subjects are as follows:

(a) Categories of Data Subjects: this DPA applies to the Processing of Company Personal Data relating to Employees and contacts of the Company's customers, prospects, suppliers, and business partners whose Personal Data is processed by Service Provider on behalf of Company pursuant to the Agreement.

(b) Types of Company Personal Data: Company Personal Data includes Contact data: name, business email, phone number, job title, employer. Usage and interaction data: activity logs, meeting or call records.

(c) Subject-matter Nature and Purpose of the Processing: the subject-matter, nature and purpose of Processing of Company Personal Data by Service Provider is the provision of the Services to Company that involves the Processing of Company Personal Data, as set out in the Agreement.

(d) Duration of the Processing: Company Personal Data will be Processed for the duration of the Agreement until deletion or return of such data as instructed by Company under this DPA.

7.2 Company is a Controller and appoints Service Provider as a Processor on behalf of Company. Company is responsible for compliance with the requirements of Data Protection Law applicable to Controllers.

7.3 Company acknowledges that Service Provider may Process Personal Data relating to the operation, support, or use of the Services for its own business purposes, such as billing, account management, data analysis, benchmarking, technical support, product development, and compliance with law. Service Provider is the Controller for such Processing and will Process such data in accordance with Data Protection Law.

8. Instructions

3.1 Service Provider will Process Company Personal Data to provide the Services and in accordance with Company's documented instructions.

3.2 The Controller's instructions are documented in this DPA and the Agreement. Company may reasonably issue additional instructions as necessary to comply with Data Protection Law. Service Provider may charge a reasonable fee to comply with any additional instructions.

3.3 Unless prohibited by applicable law, Service Provider will inform Company if Service Provider is subject to a legal obligation that requires Service Provider to Process Company Personal Data in contravention of Company's documented instructions.

4. Personnel

4.1 Service Provider will ensure that all personnel authorized to Process Company Personal Data are subject to an obligation of confidentiality.

5. Security and Personal Data Breaches

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Service Provider will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

5.2 Service Provider will notify Company without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach involving Company Personal Data. If Service Provider's notification is delayed, it will be accompanied by reasons for the delay.

6. Subprocessing

6.1 Company hereby authorises Service Provider to engage Subprocessors. A list of Service Provider's current Subprocessors is available at https://zaro.ai/legal/subprocessors.

6.2 Service Provider will enter into a written agreement with Subprocessors which imposes the same obligations as required by Data Protection Law.

6.3 Service Provider will notify Company prior to any intended change to Subprocessors. Company may object to the addition of a Subprocessor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Service Provider's notification of the intended change. Company and Service Provider will work together in good faith to address Company's objection. If Service Provider chooses to retain the Subprocessor, Service Provider will inform Company at least thirty (30) days before authorizing the Subprocessor to Process Company Personal Data, and Company may immediately discontinue using the relevant parts of the Services, and may terminate the relevant parts of the Services within thirty (30) days.

7. Assistance

7.1 Taking into account the nature of the Processing, and the information available to Service Provider, Service Provider will assist Company, including, as appropriate, by implementing technical and organizational measures, with the fulfilment of Company's own obligations under Data Protection Law to: comply with requests to exercise Data Subject Rights; conduct data protection impact assessments, and prior consultations with Supervisory Authorities and to notify a Personal Data Breach.

7.2 Service Provider may charge a reasonable fee for assistance under this Section 7. If Service Provider is at fault, Service Provider and Company shall each bear their own costs related to assistance.

8. Audit

8.1 Upon reasonable request, Service Provider must make available to Company all information necessary to demonstrate compliance with the obligations of this DPA and allow for and contribute to audits, including inspections, as mandated by a Supervisory Authority or reasonably requested no more than once a year by Company and performed by an independent auditor as agreed upon by Company and Service Provider. The foregoing shall only extend to those documents and facilities relevant and material to the Processing of Company Personal Data, and shall be conducted during normal business hours and in a manner that causes minimal disruption.

8.2 Service Provider will inform Company if Service Provider believes that Company's instruction under Section 8.1 infringes Data Protection Law. Service Provider may suspend the audit or inspection, or withhold requested information until Service Provider has modified or confirmed the lawfulness of the instructions in writing.

8.3 Service Provider and Company each bear their own costs related to an audit. Audits shall not be conducted more than once per year.

9. International Data Transfers

9.1 Company hereby authorizes Service Provider to carry out International Data Transfers with respect to Company Personal Data, provided that each such transfer is subject to an appropriate transfer mechanism required under Data Protection Law. Where required, the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), the UK International Data Transfer Addendum and, for Swiss transfers, the Swiss addendum are incorporated into this DPA by reference, using the module corresponding to the parties' roles, completed using the information in this DPA (including Section 2.2, the Security Annex and Section 6.1) and otherwise as required by Data Protection Law or the Order Form, and are deemed entered into by the parties. Service Provider shall ensure that any Subprocessor outside the EEA, the UK or Switzerland is bound by an equivalent mechanism and maintains measures consistent with this DPA. Service Provider does not warrant the laws or governmental access practices of any destination country, and any Liability under this Section is subject to the limitations of liability in the Agreement.

9. Notifications

10.1 Company will send all notifications, requests and instructions under this DPA to privacy@zaro.ai. Service Provider will send all notifications under this DPA to Company's registered email address.

11. Liability

11.1 Subject to any limitation of liability set out in the Agreement, to the extent permitted by applicable law, where Service Provider has paid damages or fines, Service Provider is entitled to claim back from Company that part of the compensation, damages or fines, corresponding to Company's part of responsibility for the damages or fines.

12. Termination and return or deletion

12.1 This DPA is terminated upon the termination of the Agreement.

12.2 Company may request return of Company Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Service Provider will delete all remaining copies of Company Personal Data within one hundred eighty (180) days after returning Company Personal Data to Company.

13. Modification of this DPA

13.1 This DPA may only be modified by a written amendment agreed in writing and signed by authorised representatives of both Service Provider and Company.

13. Invalidity and severability

14.1 If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

Security Annex

1. Security Measures (Art. 32 GDPR equivalent)

The Processor shall implement and maintain appropriate technical and organisational measures, including:

- TLS 1.2+ encryption for all data in transit
- Encryption at rest across all storage layers (AWS KMS)
- MFA enforced on all internal systems; TOTP available for end users
- SSO (SAML 2.0 / OIDC) supported; SSO-only enforcement configurable
- RBAC with workspace-level data isolation
- Quarterly access reviews
- Background checks for all employees
- Security training completed by all personnel (annual refresh)
- 22 active security policies managed via Drata
- Annual penetration testing
- Cyber liability + Tech E&O insurance (Policy: CHPR5458996XB1)
- Dependabot / automated vulnerability scanning across all repos

2. Data Hosting & Residency

Company Personal Data is hosted in AWS eu-west-2 (London). Certain optional Subprocessors may process data in the EEA or United States. Region-restricted configurations are available on request.

3. Subprocessor Management

Processor shall provide at least 30 days' advance notice of any additions to the Subprocessor list. Company may object to new Subprocessors per the terms of this DPA.

4. Incident Notification

Processor shall notify Company without undue delay, and in any case within 72 hours, of becoming aware of a Personal Data Breach affecting Company Personal Data.

5. Data Deletion on Termination

Upon termination, Processor shall return or delete Company Personal Data in accordance with Section 12 of this DPA. Integration credentials shall be revoked promptly, and deletion instructions shall be issued to Subprocessors within thirty (30) days.

6. No Training on Company Data

Company Personal Data is not used to train Processor's own models or any third-party models.

7. Audit Rights

Company has the right to audit Processor's compliance with this Annex, subject to prior written notice and reasonable cooperation. Processor's SOC 2 Type II report and penetration test report are available under NDA as an alternative audit mechanism.

8. Confidentiality

All Processor personnel with access to Company Personal Data are bound by confidentiality obligations under employment contracts or NDAs. Personnel do not have routine access to Company workspaces.