atwork

DATA PROCESSING ADDENDUM

DATA PROCESSING ADDENDUM

atwork Corporate AG, c/o TBO Treuhand AG, Steinstrasse 21, 8003 Zürich, Switzerland (“atwork”), and the customer (the “Customer”) (each a “Party” and together the “Parties”), hereby agree as follows:

This data processing addendum (the “DPA”) applies exclusively to the processing of personal data (the “Customer Personal Data”) by atwork on behalf of the Customer where such processing is subject to European Union (EU) or Swiss data privacy law. This Addendum, including its annexes, forms part of, and is subject to, the provisions of the agreement between the parties (the “Main Contract”) in respect of the performance of services (the “Services”) by atwork to the Customer that include the processing of such Customer Personal Data.

atwork acts as the Processor, while the Customer acts as the Controller of Customer Personal Data, in line with these roles defined in the General Data Protection Regulation of the EU (GDP) or Swiss Federal Act for Data Protection (FDPA). The Controller intends to commission the Processor with the services outlined in § 2 of this DPA. The implementation of the DPA also includes the processing of personal data. The General Data Protection Regulation (GDPR) and the Swiss federal Act for Data protection (FDPA), particularly Article 28 GDPR and Article 9 FDPA, demand certain requirements on processing of personal data carried out on behalf of a controller. To comply with these requirements, the Parties hereby enter into the following DPA. The costs for the implementation of the DPA are covered by the price paid by the Controller under the Main Contract, unless explicitly stated otherwise. This DPA covers data processing governed either by the EU GDPR or by the Swiss FDPA. It does not aim to specify or establish which regulation is applicable, nor does it constitute an engagement by the Parties to abide to or comply with the GDPR in cases where the FDPA is applicable, or vice-versa.

Parts of this DPA which only pertain to either regulation shall be deemed nonexistent when the data processing occurring under this DPA is governed by the other regulation.

§ 1

DEFINITIONS

Terms used in this DPA which are defined by the GDPR and/or the FDPA shall have the same meaning as those established by the relevant GDPR or FDPA provision.

§ 2

CONTRACTUAL OBJECT

(1) On behalf of the Controller and based on the Main Contract, the Processor shall carry out services in the following sectors for the Controller: Provision of software for measuring and improving HR metrics and employee experience. In doing so, the Processor shall gain access to personal data and shall process said personal data exclusively on behalf of and according to the instructions issued by the Controller, unless otherwise required by applicable laws to the Processor. The scope and purpose of the Processor's data processing result from the Main Contract, the corresponding service description, and **Annex 1** to this DPA. The Controller shall be the responsible for the lawfulness of the processing done by the Processor within the scope of this DPA.

(2) The Parties have agreed to conclude this DPA in order to specify their mutual rights and obligations under data protection law. In cases of doubt, the provisions of this DPA shall supersede the provisions of the Main Contract.

(3) The provisions laid out in this DPA shall apply to all activities which are performed in connection with the Main Contract by the Processor, its employees or agents and which imply contact with personal data originating from, collected for or otherwise processed on behalf of the Controller.

(4) This DPA shall become effective upon signature by both Parties. Its duration shall be the same as the duration of the Main Contract, unless the following provisions stipulate further obligations.

§ 3

NATURE OF THE DATA PROCESSED, GROUP OF DATA SUBJECTS

With respect to the execution of the Main Contract, the Processor will receive access to the personal data specified in **Annex 1**, belonging to the group(s) of data subjects also specified in **Annex 1**. This data includes special categories of personal data as specified in **Annex 1**.

§ 4

CONTROLLER’S RIGHT TO INSTRUCT

(1) The Processor processes personal data within the scope of the Main Contract and according to the Controller’s documented instructions; this is particularly applicable with regard to transfer of personal data to a third country. If the Processor must carry out further processing due to applicable laws to the Processor, the Processor shall notify the Controller of these legal requirements before any such processing takes place.

(2) The Controller’s instructions shall be initially determined by this DPA (“Individual Instruction”). The Controller shall have the right to issue instructions in a written format at any time, including inter alia instructions regarding the rectification, erasure and blocking of data. The persons authorised to issue respectively receive instructions may be specified by the Parties from time to time. In case of a change or long-term hindrance of the designated persons, the successor or substitute shall be made known to the other Party within 10 days of the change or the beginning of the long-term hindrance. This notification must be given in writing and duly signed by authorized representatives.

(3) The Controller and Processor shall document all issued/received instructions and keep such documentation for the duration of the instruction’s validity, and for three full calendar years thereafter. Instructions going beyond the service as agreed-upon by the Main Contract shall be deemed a Change Request. Arrangements regarding a possible compensation of additional expenses resulting from supplementary instructions given to the Processor by the Controller shall remain unaffected.

(4) Should the Processor suspect that an instruction issued by the Controller violates legal data protection requirements; the Processor shall notify the Controller accordingly without undue delay, in writing or by any means allowing for proof by text. The Processor is entitled to suspend the execution of the instruction in question until the Controller confirms or changes it. The Processor is entitled to refuse the execution of an instruction that infringes applicable laws.

(5) Notwithstanding paragraph 4 above, the Controller remains responsible for verifying the legal and regulatory compliance of its instructions to the Processor. The Processor shall not be held liable for the execution of the Controller’s instructions which would prove unlawful or otherwise illicit, or for failing to identify instructions as such.

§ 5

PROTECTIVE MEASURES ESTABLISHED BY THE PROCESSOR

(1) The Processor shall maintain technical and organisational measures under Article 32 GDPR or Article 8 FDPA; implemented measures are specified in **Annex 2**. Upon the Controller's request, the Processor shall disclose the particulars of how these measures are determined and implemented. The Processor reserves the right to change the implemented security measures, provided that it ensures that these do not fall short of the contractually agreed upon level of protection.

The Controller acknowledges and accepts that the processing of data under this DPA may occur in private homes (telework or home-office by the Processor's employees).

§ 6

PROCESSOR'S INFORMATION OBLIGATIONS

(1) In case of data breaches the Processor shall inform the Controller accordingly without undue delay. To the extent possible, the notification about a personal data breach should contain the following information:

a. a description of the nature of the personal data breach including, where possible, the categories and number of data subjects potentially affected, and the categories and number of personal data records affected,

b. a description of the likely consequences of the personal data breach, and

c. a description of the measures taken or proposed by the Processor to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

(2) The Processor shall take reasonable measures to assist the Controller in mitigating possible adverse effects suffered by the data subject(s) without undue delay.

(3) If necessary, the Processor shall, in an adequate manner, assist the Controller in ensuring compliance with the Controller's obligations under Articles 33 and 34 GDPR (Article 28 Subsection (3) Sentence 2 lit. f) GDPR) and/or Article 24 FDPA. The Processor shall only execute

notifications on behalf of the Controller according to Articles 33 or 34 GDPR or Article 24 FDPA upon the Controller’s prior instruction as outlined in § 4 of this DPA.

(4) The Processor and, if applicable, its representative, shall maintain a record of all processing activities carried out on behalf of the Controller, containing all specifications required under Article 30 Subsection (2) GDPR or Article 12 FDPA. This record shall be made available to the Controller upon request.

(5) The Processor shall, to an adequate extent and where necessary, assist the Controller in the establishment of its record of processing activities. The Processor shall also assist the Controller with data protection impact assessments the Controller executes in accordance with Article 35 GDPR or Article 22 FDPA and, if applicable, with prior consultations of supervisory authorities in accordance with Article 36 GDPR or Article 23 FDPA. The Processor shall in each case convey the necessary specifications to the Controller in an appropriate manner. The Processor may charge a fee for these services.

§ 7

AUDIT RIGHTS

(1) The Controller may request that the Processor's provide the information necessary to demonstrate the technical and organisational measures taken to ensure compliance with applicable laws and the DPA. The Controller may further have them audited by an expert third party, unless the latter is in a competitive relationship with the Processor; such inspection of documentation will take place during normal business hours. Any such audit or documentation remittance must be coordinated in advance, and its practical modalities must be agreed upon by the Parties; it may start no less than 30 days after the Processor has received written notification from the Controller regarding the Controller’s will to conduct an audit or to inspect the documentation. The Controller shall conduct controls only to the extent necessary so as to not unduly disturb the Processor’s business operations, and such controls shall exclude physical inspection of private residences, sensitive facilities or premises of the Processor, unless required by the applicable law. The Processor may deny audit or documentation remittance requests when such an audit occurred within the last 12 months, unless the Controller validly demonstrates serious and immediate concerns warranting a new audit.

(2) The Controller shall document the control result and communicate it to the Processor in writing. In the case of defects or irregularities detected by the Controller, particularly when assessing order results, the Controller shall inform the Processor accordingly without undue delay. If a control reveals defects or irregularities whose future avoidance requires changes to the process established by the Processor, the Controller shall, without undue delay, notify the Processor of the necessary changes. Findings shall be kept confidential and used solely for verifying compliance with this DPA.

(3) The Controller shall reimburse the Processor for the expenses incurred in the course of an audit.

§ 8

COMMISSIONING OF SUBCONTRACTORS

(1) For the execution of the services contractually agreed-upon the Processor has a general authorisation from the Controller to engage sub-processors. Processor will commission the subcontractors listed in **Annex 3**. Within the scope of its contractual obligations, the Processor may establish further subcontracting relationships. For new sub-processors, the Processor shall notify the Controller at least 30 days in advance. The Controller may object only for reasonable grounds relating to data protection and failure to object within the notice period constitutes approval of a new sub-processor. When commissioning subcontractors, the Processor shall ensure their commitment in line with the provisions of this DPA. If subcontractors from a third country are involved, the Processor shall ensure that an adequate level of data protection is guaranteed by the subcontractor in question. In such cases, Processor may rely on adequacy decisions, standard contractual clauses, or other lawful transfer mechanisms at its discretion. Upon request, the Processor shall demonstrate the conclusion of the aforementioned agreements with its subcontractors.

(2) When the Processor commissions a third party with a purely ancillary service, this shall not constitute a subcontractor relationship within the meaning of these provisions. Such ancillary services include, but are not limited to, postal, transport and shipping services, cleaning services, security services, and telecommunications services without concrete reference to services provided by the Processor for the Controller. Maintenance and testing services constitute subcontractor relationships insofar as they are provided for IT systems also used in connection with the Processor's provision of services on behalf of the Controller.

§ 9

DATA SUBJECT INQUIRIES AND RIGHTS

(1) As far as possible, the Processor shall with appropriate technical and organisational measures assist the Controller in fulfilling the Controller's obligations as established by Articles 12 - 22 GDPR or Articles 25 and 32 FDPA.

(2) If a data subject asserts his/her rights regarding to his/her personal data directly against the Processor, the Processor shall not react independently. Rather, the Processor shall inform the Controller of the request without undue delay and wait for the Controller's instructions on how to proceed.

The Controller shall reimburse the Processor for all reasonable expenses incurred by such assistance activities.

LIABILITY

(1) For data processing governed by GDPR, the Controller and the Processor shall be liable to the data subjects in accordance with the provisions of Article 82 GDPR. The Processor shall coordinate with the Controller any fulfilment of liability claims.

(2) Irrespective of the applicable data protection regulation, the liability within the scope of this DPA, in particular the monetary extent of the liability and the nature of the liable acts, shall correspond to the liability cap of the Main Contract.

(3) Should no explicit provisions regarding liability be foreseen in the Main Contract, the following will apply : the Processor’s liability is unlimited for damages arising out of intentional or grossly negligent conduct. The Processor's liability for direct damages is limited to a maximum amount of CHF 20'000. Any further liability of the Processor is excluded to the extent permitted by applicable law. In all cases, the Processor shall not be liable for indirect or consequential damages, including loss of profit, loss of data, business interruption, or reputational harm.

§ 10

TERMINATION

(1) After termination of the Main Contract or otherwise at the termination of the DPA, the Processor shall return to the Controller the personal data or delete them at the Customer's request, unless such a deletion is prohibited by applicable law.

§ 11

REPRESENTATIVE IN THE EUROPEAN UNION

As representative under Article 27 Subsection (1) GDPR, the Processor has appointed:

Atwork Spain SL, Av. de Reina Victoria 35, 39004 Santander, Spain, gdpr@atwork.ai.

§ 12

FINAL PROVISIONS

(1) The **Annexes 1, 2 and 3** are essential parts of this DPA.

(2) To be valid, any changes and amendments to this DPA must be made in writing or by any means allowing for proof by text. This applies also to a change of this formal requirement.

(3) This DPA shall be governed by and construed in accordance with Swiss Law. The international private law shall not be applicable.

(4) The sole place of jurisdiction is Zurich (Switzerland).

(5) Should any provision of this DPA be invalid or become partially or entirely invalid or unenforceable, the remainder of this DPA shall remain valid and in force.

ANNEX 1: DESCRIPTION OF THE PERSONAL DATA CATEGORIES BEING PROCESSED AND THE GROUPS OF DATA SUBJECTS AFFECTED

Categories of personal data, being subject of the processing:

☒ first and/or family name
☒ contact data
☐ bank account data
☐ performance data
☐ offering data
☐ information data
☒ personnel administration
☐ working hour data
☐ applicants data
☐ telephone numbers
☐ personnel numbers
☐ emails
☐ archive files
☐ videos

☐ address data
☐ contract master data
☐ account data
☐ financial data
☐ transaction data
☒ personnel data
☒ qualification data
☐ travel reservation data
☐ payment data
☒ employee assessment
☐ identification numbers
☐ email attachments
☐ statistical data
☐ texts

Other:

____
____
____

Sensitive personal data as of Article 5(b) FDPA / Special categories of personal data according to Article 9 GDPR and personal data relating to criminal convictions and offences according to Article 10 GDPR, being subject of the processing:

☐ health data
☐ biometric data
☐ trade union membership
☐ religious belief
☐ sex life
☐ racial origin
☐ criminal convictions and offences or related security measures

☐ patient files
☐ genetic data
☐ political opinions
☐ philosophical belief
☐ sexual orientation
☐ ethnic origin

Other:

____

____
____

Groups of data subjects affected by the processing:

☐ clients
☐ suppliers/service providers
☐ business partners
☐ members
☒ employees
☐ apprentices
☐ ex-employees
☐ dependents
☐ brokers
☐ tenants
☐ damaged persons

☐ interested persons
☐ consultants
☐ associates
☐ persons receiving advertisement
☐ retired persons
☐ trainees
☐ applicants
☐ relatives
☐ agents
☐ users
☐ witnesses

Other:

____
____
____

ANNEX 2: PROCESSOR'S TECHNICAL AND ORGANISATIONAL MEASURES ACCORDING TO ARTICLE 32 SUBSECTION (1) GDPR AND ARTICLE 8 FDPA

No.	Measures	Practical implementation of such measures by Processor
1.	**Confidentiality**	
	Physical access control No unauthorized person may gain access to data processing systems containing personal data.	Data is stored in the Microsoft Azure Cloud, where it is subject to strict security measures, e.g.: • key-operated security locks • locked doors during periods of absence • locked windows during periods of absence • defined security areas • access control system (e.g. magnetic cards, chip cards) • card reader • code locks • logging of arrivals and departures • access control system for non-employees • reception
	Logical access control No unauthorized persons may use data processing systems.	• keyboard security locks • identification and authentication • logging • evaluation/logging • firewall
	Data entry control It must be ensured that persons entitled to use a data processing system have access only to the data to which they have the right of access, and that personal data cannot be read, copied, modified or removed without corresponding authorisation.	• back-up concept • organisational and technical safeguards for authorisations, and encryption
	Separation control It must be ensured that data collected for different purposes can be processed separately.	• Logical separation

	Pseudonymization Personal data should preferably be processed in such a way that the data can no longer be assigned to a specific person without the need for additional information.	• The pseudonymization of personal data (applies to all “Strategic Surveys”, but not to all “Custom Surveys”, as “Custom Surveys” can also optionally be launched as “non-anonymous”.
2.	**Integrity**	
	Transmission control It must be ensured that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission, transport on data carriers or during storing, and that it is possible to check and establish to which entities the transfer of personal data is envisaged.	In case of required transfer of persona data, the following measures are applied: • Labeling of the data carrier • Encryption of personal data on data carriers • Safe transport of physical data medium • Specification of persons authorised to release data carriers or to undertake electronics transmissions • Specification of recipients of data • Rules for transporting of data carriers • Cryptographic encryption of transmitted data • remote maintenance system
3.	**Availability and resilience of systems and services**	
	Availability control It must be ensured that personal data is protected from accidental destruction or loss.	Data is stored in the Microsoft Azure Cloud, where it is subject to strict protection measures, e.g.: • back-up concept • emergency plan • uniterruptible power supply (UPS) • fire detectors/alarms • additional security copies with storage in specially protected locations
4.	**Procedures for periodic review and evaluation**	
	Data protection Management	• development and implementation of internal processes, especially at the organisational level, to ensure the effectiveness of the technical and organisational measures
	Control of Data Processors It must be ensured that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the Controller.	• Written specification of instructions • Regular internal checks and documentation by Processor

ANNEX 3: APPROVED SUBCONTRACTORS

Use of the listed sub-processors is deemed approved. Processor may update server locations within the EEA/Switzerland without requiring additional approval.

Name of sub-processors	Location of servers	Purpose	Data processed
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Zurich, Switzerland	Hosting, data anonymisation (Azure)	Profile information, uploaded content
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855, Luxembourg	Frankfurt, Germany	Email (AWS Simple Email Services)	Contact information (incl. email address)