TRUE AIM AG
DATA PROCESSING AGREEMENT

Version: 1.0
Effective date: 2026-05-19
Last updated: 2026-05-19

This Data Processing Agreement (DPA) applies to the processing of personal data by True Aim AG, Metallstrasse 9, 6300 Zug, Switzerland (the Company) on behalf of any client (the Client) that has entered into a Master Services Agreement with the Company incorporating this DPA by reference.

1 Preamble

1.1 This DPA applies to all processing of personal data by the Company as processor on behalf of the Client as controller in connection with the Services provided under the Master Services Agreement between the Parties (the Agreement). Terms defined in the Agreement have the same meaning in this DPA unless otherwise stated.

1.2 This DPA sets out the rights and obligations of the Company as processor of personal data that it receives and processes on behalf of the Client in connection with the performance of the Agreement.

1.3 This DPA is concluded in compliance with Article 9 of the Swiss Federal Act on Data Protection (FADP) and, to the extent the processing falls within the scope of the European General Data Protection Regulation (GDPR), in compliance with Article 28 GDPR.

1.4 In the event of any inconsistency between this DPA and the Agreement, the Agreement prevails unless this DPA expressly states otherwise.

1.5 The Company may update this DPA from time to time to reflect changes in applicable law, regulatory guidance, industry best practice or the Company's processing activities. The Company shall maintain or improve the level of data protection afforded to personal data in any such update. In the event that a proposed update would alter the scope of processing, the categories of personal data processed or the jurisdictions in which processing takes place, the Company shall notify affected Clients at least 30 calendar days before the update takes effect. If a Client objects to any such update within that period, the process set out in the Agreement shall apply.

1.6 A version history of this DPA is maintained at the end of this document. Each version is identified by a version number and effective date. The Client may request a copy of any prior version from the Company.

2 Definitions

2.1 The terms cited and defined in this clause supplement the definitions of the applicable data protection legislation and of the Agreement. They have the meaning set out below whenever they appear in this DPA, whether in the singular or plural.

"Applicable Data Protection Law" means the FADP and, to the extent applicable, the GDPR, and any national implementing legislation, in each case as amended or replaced from time to time.

"Controller" means the natural or legal person that determines the purposes and means of the processing of personal data; in the context of this DPA, the Client.

"Data Subject" means an identified or identifiable natural person to whom personal data relates, including claimants, policyholders, beneficiaries and their representatives.

"Personal Data" means any information relating to a Data Subject.

"Processing" / "Process" means any operation performed on personal data, regardless of the means or method used, including the collection, storage, use, modification, disclosure, archiving, deletion and destruction of personal data.

"Processor" means the legal person that processes personal data on behalf of the Controller; in the context of this DPA, the Company.

"Sensitive Personal Data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation, as well as data on administrative or criminal proceedings or sanctions, and data on social assistance measures.

"Sub-Processor" means any third party engaged by the Processor to process personal data on behalf of the Controller in connection with the Services.

3 Subject Matter and Legal Basis

3.1 This DPA governs the processing of personal data by the Company as Processor on behalf of the Client as Controller in connection with the provision of the Services under the Agreement.

3.2 The applicable legal framework is the FADP and, to the extent the processing falls within the territorial scope of the GDPR, the GDPR. Where both instruments apply, the stricter standard prevails.

3.3 The legal basis for the processing of personal data under this DPA is the performance of the Agreement between the Parties. Responsibility for establishing and maintaining a valid legal basis for the processing vis-a-vis Data Subjects (including, where required, obtaining consent) lies with the Client as Controller.

4 Nature and Purpose of Processing

4.1 **Categories of Data Subjects.** The following categories of Data Subjects may be affected by the processing: claimants, policyholders, insured persons, beneficiaries, third-party service providers (and their employees and representatives) and the Client's own personnel who access the Platform.

4.2 **Categories of Personal Data.** The following categories of personal data may be processed: identification data (name, date of birth, address, contact details); policy and claim reference data (policy numbers, claim numbers, case identifiers); claim-related

data (description of the incident, loss or damage, supporting documentation, correspondence); financial data (bank details, payment records, invoices, cost assessments); and, where the nature of the claim requires, Sensitive Personal Data (in particular health data in connection with personal injury or medical claims). Documents uploaded to the Platform by the Client or by Data Subjects may contain any of the foregoing categories.

4.3 **Purposes of Processing.** The Company processes personal data solely for the purpose of providing the Services to the Client under the Agreement, including: case intake and handling; claim registration and triage; document ingestion, data extraction and structuring; claims assessment and decision support; fraud intelligence analysis; communications management; generation and retention of the Audit Trail Record; and any ancillary processing reasonably necessary for the foregoing.

4.4 **Nature of Processing.** Processing is performed by means of storage, display, structuring, analysis, modification and deletion of personal data on the Platform, including through the use of artificial intelligence technologies such as cloud-hosted large language models accessed via the Company's cloud infrastructure for document analysis, classification and visual interpretation, and optical character recognition (OCR) for text extraction from documents and images uploaded to the Platform.

4.5 **Automated Decision Support.** The Platform may, depending on the modules and automation tier activated for the Client under the Agreement, perform fully or partially automated analyses or generate recommendations that may have legal effect or similarly significantly affect Data Subjects. The Client is solely responsible for determining whether and to what extent it relies on automated outputs and for ensuring compliance with the requirements of Article 21 FADP and, where applicable, Article 22 GDPR, including the provision of appropriate safeguards and the right of the Data Subject to request human review.

4.6 **Duration.** Processing shall continue for the term of the Agreement. Following termination, the provisions of clause 13 of this DPA shall apply.

5 Obligations of the Client

5.1 The Client is responsible for the lawfulness of the processing of personal data under this DPA. The Client shall ensure compliance with all applicable data protection legislation in connection with the collection, use and disclosure of personal data processed through the Platform.

5.2 The Client warrants that Data Subjects have been informed of the processing in accordance with applicable law and that, where required, the Client has obtained valid consent or can rely on another lawful basis for the processing, including any processing of Sensitive Personal Data.

5.3 The Client has the right to issue instructions to the Company regarding the nature, scope and method of processing of personal data, subject to the terms of the Agreement. Instructions shall be issued in writing or by email. The Client shall designate the persons authorised to issue instructions.

5.4 Where an instruction from the Client is, in the Company's reasonable assessment, incompatible with the applicable data protection legislation, the Company shall notify

the Client without undue delay. The Company may suspend the execution of such instruction until the Client confirms or modifies it. Responsibility for the lawfulness of instructions remains with the Client.

5.5 The Client shall indemnify and hold the Company harmless against any claims by Data Subjects arising from the unlawful processing of personal data attributable to the Client's instructions, actions or omissions.

6 Obligations of the Processor

6.1 The Company shall process personal data only in accordance with this DPA, the Agreement and the documented instructions of the Client, unless processing is required by applicable law, in which case the Company shall inform the Client of such legal requirement before processing, unless prohibited by law from doing so.

6.2 The Company shall ensure that all persons authorised to process personal data under this DPA have committed to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.3 The Company shall not process personal data for any purpose other than the provision of the Services under the Agreement, including for its own purposes, except as expressly permitted in this DPA or the Agreement.

6.4 The Company shall implement and maintain the technical and organisational measures set out in Schedule 1 to this DPA, in compliance with Article 8 FADP and Article 32 GDPR.

6.5 **Breach Notification.** The Company shall notify the Client without undue delay, and in any event within 48 hours, of becoming aware of a breach of the security of personal data processed under this DPA. The notification shall include, to the extent available: the nature of the breach; the categories and approximate number of Data Subjects and personal data records affected; the likely consequences; and the measures taken or proposed to address the breach and to mitigate its effects.

6.6 **DPIA and Prior Consultation.** The Company shall assist the Client, taking into account the nature of the processing and the information available to the Company, in complying with its obligations under Articles 22 and 23 FADP and, where applicable, Articles 35 and 36 GDPR (data protection impact assessment and prior consultation with the supervisory authority).

6.7 **Audit and Inspection.** The Company shall, on reasonable written request from the Client and subject to reasonable advance notice, make available to the Client all information necessary to demonstrate compliance with this DPA and shall support audits and inspections conducted by the Client or an independent auditor appointed by the Client. Audits shall be conducted during normal business hours and shall not unreasonably disrupt the Company's operations. The Client shall bear the costs of any such audit.

6.8 Where personal data processed under this DPA is threatened by seizure, attachment, insolvency proceedings or other measures by third parties, or must be disclosed to third parties including authorities, the Company shall notify the Client without undue

delay. The Company shall inform all relevant parties that the personal data is under the authority of the Client as Controller.

6.9 Where an instruction from the Client infringes applicable data protection legislation, the Company shall notify the Client. Responsibility for the lawfulness of instructions remains with the Client.

6.10 Services rendered by the Company under clauses 6.6 and 6.7 that go beyond the notification of data protection breaches shall be compensated at a rate of CHF 200 per hour (excl. VAT), unless otherwise agreed in writing.

7 Technical and Organisational Measures

7.1 The Company shall observe the principles of lawful processing of personal data and shall monitor compliance on an ongoing basis.

7.2 The Company warrants the implementation and maintenance of the technical and organisational measures set out in Schedule 1 to this DPA, in compliance with Article 8 FADP and Article 32 GDPR.

7.3 The technical and organisational measures are subject to technical progress and development. The Company may update the measures from time to time, provided that the agreed level of protection is not reduced. Material changes shall be documented and, on request, communicated to the Client.

8 Data Subject Rights

8.1 Where a Data Subject exercises any right under applicable data protection legislation (including the right of access, rectification, erasure, restriction, data portability and objection) in respect of personal data processed under this DPA, the Company shall assist the Client in fulfilling such requests, taking into account the nature of the processing.

8.2 Where a Data Subject contacts the Company directly to exercise any such right, the Company shall forward the request to the Client without undue delay and shall not respond to the Data Subject directly unless instructed by the Client.

8.3 Where the Platform performs fully or partially automated individual decision-making within the meaning of Article 21 FADP or Article 22 GDPR, the Company shall, on the Client's instruction, provide the Data Subject with meaningful information about the logic involved, the significance and the anticipated consequences of such processing. The Data Subject's right to obtain human intervention and to contest the decision remains with the Client as Controller.

9 Sub-Processors

9.1 The Company may engage Sub-Processors to process personal data on behalf of the Client, subject to the requirements of this clause 9. The Sub-Processors currently engaged by the Company are listed in Schedule 2 to this DPA.

9.2 The Client hereby provides general written authorisation for the Company to engage Sub-Processors in accordance with this clause 9. The Company shall update Schedule

2 to this DPA before any new Sub-Processor begins processing personal data. The Client may object to any intended change by written notice to the Company within 30 calendar days of the date of the update. In the event of an objection, the Parties shall negotiate in good faith to reach a mutually acceptable solution. If no agreement is reached, either Party may terminate the Agreement on 30 calendar days' written notice. If the Client does not object within the 30-day period, consent to the change is deemed given.

9.3 The Company shall select Sub-Processors with due care and shall engage only those that provide adequate guarantees of compliance with applicable data protection legislation. The contractual arrangements with each Sub-Processor shall impose data protection obligations equivalent to those set out in this DPA, in particular, appropriate technical and organisational measures commensurate with the sensitivity of the data processed.

9.4 The sub-processing relationship shall be concluded in compliance with Article 9 FADP and Article 28 GDPR. The Client shall be granted corresponding audit rights in respect of Sub-Processors. The Client shall bear the costs of any such audits.

9.5 The Company remains fully liable to the Client for the performance of any Sub-Processor as if the Company had performed the relevant processing itself.

10 International Data Transfers

10.1 Personal data shall be processed within Switzerland and the European Economic Area (EEA). Processing in any other country (a "Third Country") is permitted only with the prior written consent of the Client and provided that the applicable legal requirements are met.

10.2 Where personal data is transferred to a Third Country that does not benefit from an adequacy decision under the applicable data protection legislation, the Parties shall ensure that appropriate safeguards are in place, including the execution of the European Commission's Standard Contractual Clauses (in the version current at the time of transfer) and, where required, any supplementary measures necessary to ensure an adequate level of protection.

10.3 For transfers subject to the FADP, the Company shall comply with Articles 16 and 17 FADP and shall observe the list of countries providing an adequate level of data protection published by the Swiss Federal Council.

10.4 All data transfers shall be protected by appropriate technical and organisational measures.

11 Anonymisation and Aggregation

11.1 The Company is entitled to create anonymised copies of personal data by removing all identifying attributes relating to a Data Subject and transferring the resulting data to a separate database ("Anonymised Data"). Anonymisation shall be carried out in a manner that renders the data irreversibly non-attributable to any identified or identifiable natural person, taking into account all means reasonably likely to be used for identification.

11.2 The Parties agree that Anonymised Data no longer constitutes personal data within the meaning of the applicable data protection legislation and falls outside the scope of this DPA from the point of anonymisation.

11.3 Following anonymisation, the Company shall become the owner of the Anonymised Data and may use it at its sole discretion, including for analytical purposes, benchmarking, platform improvement and the generation of aggregated insights for the benefit of its clients. This right is subject to and consistent with the relevant provisions of the Agreement.

11.4 The Company warrants that it shall not attempt, and shall contractually prohibit any third party with whom it shares Anonymised Data from attempting, to re-identify any natural person or to link Anonymised Data to any individual Client or Data Subject.

12 Cookies and Platform Access Data

12.1 The Company may use cookies and comparable technologies on the Platform to enable and support the provision of the Services, including session management, security and platform optimisation.

12.2 The Platform currently sets only strictly necessary cookies (session and security). No non-essential, marketing or analytics cookies are deployed. Should the Company introduce non-essential cookies in the future, they shall be deactivated by default and the Client shall be informed in advance; deactivation of certain cookies may affect the functionality of the Platform.

12.3 The Company may collect access and usage data of the Client's authorised users (such as browser type, access times and accessed Platform elements) for the purpose of operating, securing and optimising the Platform. Such data shall be processed in accordance with applicable data protection legislation.

12.4 The Company does not currently use third-party analytics services in connection with the Platform; Platform telemetry is processed via the Company's cloud infrastructure in the Switzerland North region. Should the Company engage a third-party analytics service in the future, the Client shall be informed of the identity and location of such provider, and any transfer of data to analytics providers outside Switzerland and the EEA shall be subject to the requirements of clause 10.

13 Data Retention and Deletion

13.1 Personal data processed under this DPA shall be retained in accordance with the retention schedules agreed in the Agreement. To the extent that the Audit Trail Record contains personal data, the personal data elements shall be deleted or anonymised in accordance with the retention schedules set out in this DPA, while the non-personal process record shall be retained for the full retention period specified in the Agreement.

13.2 The Client is responsible, independently of the availability of the Platform, for maintaining in its own systems all personal data necessary for the orderly conduct of its business. The Company shall make personal data available to the Client by means of interfaces for the purpose of data backup, archiving and synchronisation with the Client's own systems.

13.3 Where a Data Subject requests deletion of personal data held by the Company, the Company shall inform the Client without undue delay and shall carry out the deletion upon the Client's instruction.

14 Term and Termination

14.1 The term of this DPA is coterminous with the Agreement.

14.2 Upon termination or expiry of this DPA, the Company shall, subject to clause 11, return to the Client or, at the Client's election, securely delete or destroy all personal data (including all copies and backups) within a reasonable period, unless applicable law requires continued storage. The Company shall confirm deletion in writing upon request.

14.3 The obligations in this clause apply equally to any Sub-Processors engaged by the Company.

SCHEDULE 1 TO THIS DPA
TECHNICAL AND ORGANISATIONAL MEASURES

The Company undertakes to implement and maintain the following technical and organisational measures in connection with the processing of personal data under this DPA:

1 Confidentiality

1.1 **Physical Access Control.** The Company operates no on-premises infrastructure and processes no personal data outside cloud-hosted environments; staff work from home offices on managed endpoints. All production personal data resides in Microsoft Azure datacentres in the Switzerland North region, whose physical security controls are operated by the cloud provider and governed by its ISO 27001 and SOC 2 Type II certifications. The cloud provider's certificates and most recent SOC 2 Type II report are available to the Client on reasonable request.

1.2 **System Access Control.** Access to the Platform is authenticated by email and password using industry-standard password hashing, with secure session management, cross-site request forgery (CSRF) protection, and login rate-limiting and abuse throttling. Multi-factor authentication is enforced on the Platform's first-party authentication flow for all users. Access to underlying cloud infrastructure by Company personnel is restricted to named engineers and protected by multi-factor authentication.

1.3 **Data Access Control.** Application-level access follows role-based access control with least-privilege defaults, with logical tenant isolation in the application database and enforcement at the application's authorisation layer. Access rights are reviewed at least quarterly by the CTO of the Company, with records retained in the access-review register. A document-level data classification scheme distinguishes Personal Data, Sensitive Personal Data (including health data) and operational metadata, and is documented in the Company's record of processing activities. Comprehensive audit logging of authentication and authorisation events is forwarded to centralised log aggregation.

2 Integrity

2.1 **Transfer Control.** All connections to the Platform and between the Platform's components are encrypted in transit using current industry-standard protocols. Internal service-to-service authentication uses managed-identity-based access with short-lived credentials. All processing endpoints that handle personal data are deployed in the Switzerland North region. Transfers to Sub-Processors are governed by clause 9 of this DPA.

2.2 **Input Control.** Every change to personal data records on the Platform is attributable: each record carries actor, timestamp and state-transition fields, and document ingestion lifecycle events are emitted as structured logs to centralised log aggregation. Database transaction logs preserve a forensic record of database mutations within the retention window.

3 Availability and Resilience

3.1 **Availability Control.** Production runs on Microsoft Azure (region: Switzerland North) with data tiers operated in zone-redundant high-availability mode and stateless compute with rapid cross-zone recovery. Recovery objectives are RPO ≤ 24 hours and RTO ≤ 4 hours. Continuous vulnerability scanning, malware scanning and software composition analysis are operated across the production environment, with findings tracked to closure in the corrective-action register. Platform health monitoring and alerting are operated across the Platform's components. An external black box penetration test is performed at least annually by a qualified third-party provider, and findings are tracked to closure.

3.2 **Recoverability.** Production databases are protected by continuous point-in-time recovery, retained for a minimum of 30 days. Object and secret stores provide accidental-deletion protection. Recovery objectives are a Recovery Point Objective of no more than 24 hours and a Recovery Time Objective of no more than 4 hours to restore one tenant's data to a validated state. Restore drills are performed at least quarterly per the Company's Disaster Recovery Plan.

3.3 **Encryption at Rest.** All personal data stored by the Platform is encrypted at rest using AES-256 with cloud-provider-managed keys. Cryptographic keys are managed by the cloud provider within the Switzerland North region; key rotation, hardware-security-module protection and cryptographic separation are governed by the provider's ISO 27001 and SOC 2 Type II controls. Application-level secrets managed by the Company are stored in a managed secret-store with accidental-deletion protection.

4 Data Retention and Deletion

4.1 **Retention Periods.** Personal-data retention follows the schedules set out in the Company's Data Retention Schedule and is consistent with clause 13 of this DPA and the applicable retention provisions of the Agreement: the personal-data elements of the Audit Trail Record are retained for the period necessary to fulfil the Services, and may be deleted or anonymised independently of the non-personal process record, which is retained for the full seven-year ATR retention period under the Agreement. Short-lived session and rate-limit data is purged automatically. Default retention targets for claim documents (seven years after claim closure), invitations (30 days after acceptance or expiry) and user and membership records (90 days after soft-delete) are enforced by automated cleanup jobs operated by the Company.

4.2 **Backup Deletion.** Backups age out automatically at the end of their retention window, and no manual backup deletion is required or performed. Soft-deleted objects in object and secret stores are permanently deleted at the end of their soft-delete retention period. Any out-of-band backup or export taken for restore-drill or migration purposes is destroyed by the responsible engineer in a reasonable period after the drill, with a record kept under the Company's Disaster Recovery Plan.

5 Review, Assessment and Evaluation

5.1 **Ongoing Review.** The Company operates an Information Security Management System aligned with ISO/IEC 27001. The ISMS includes an annual internal audit

programme, quarterly access reviews, annual security-awareness, privacy and incident-response training for all staff and additional secure-development and AI-specific training for engineering staff. All personnel are bound by written confidentiality obligations in their employment or contractor agreements, and contractors are subject to identity verification and reference checks proportionate to the access being granted. External assurance includes an annual external black box penetration test by a qualified third-party provider; technical and organisational measures are reviewed at least annually and on material change.

5.2 **Incident Response.** The Company maintains a documented incident- and breach-response procedure covering detection, triage, containment (revocation of sessions, memberships and credentials; pausing processing; isolating tenant access), scope assessment, internal escalation, controller notification, and support for any authority or Data Subject notifications. Detection sources include user and Client reports, platform monitoring and alerting, and Sub-Processor notifications. The Client is notified without undue delay and in any event within 48 hours of confirmed awareness of a personal-data breach, in line with clause 6.5 of this DPA; authority notification, where the Client requires support, is supported within the 72-hour GDPR window. Post-incident reviews are conducted by the CTO of the Company and findings are tracked to closure in the corrective-action register.

5.3 **Processing Control.** The Company processes personal data under this DPA exclusively in accordance with the instructions of the Client as Controller. The Client's inspection rights are as specified in the Agreement.

Date of last update: 2026-05-19

SCHEDULE 2 TO THIS DPA
SUB-PROCESSORS

The following Sub-Processors are currently engaged by the Company in connection with the processing of personal data under this DPA:

Entity: Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland

Service: Cloud infrastructure and hosting (Microsoft Azure), including compute, database, storage, AI model inference, document processing, key management, monitoring and networking services deployed within the Company's Azure tenant.

Personal Data Affected: All categories of Personal Data listed in clause 4.2 (identification, policy and claim reference, claim-related data including Sensitive Personal Data where the claim requires it, and financial data), together with platform telemetry (request metadata, error traces) and authorised-user account data.

Location: Switzerland North (Zurich) for all data at rest and primary processing. No ancillary Azure service processes Personal Data outside Switzerland or the EEA.

Entity: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland

Service: Business productivity and communications suite (Google Workspace), including email, document storage and calendar services used for client communications and operational coordination, including correspondence that may contain claim-related Personal Data submitted by the Client outside the Platform.

Personal Data Affected: Identification data and any claim-related Personal Data voluntarily included by the Client or Data Subjects in email correspondence or shared documents.

Location: European Union (Google Workspace data region configured for Europe). Governed by the Google Cloud / Workspace Data Processing Addendum and EU Standard Contractual Clauses.

Entity: Slack Technologies Limited, 4th Floor, One Park Place, Hatch Street Upper, Dublin 2, D02 W085, Ireland

Service: Internal team-communication platform used by Company personnel for operational coordination and troubleshooting, in which claim-related Personal Data may be referenced.

Personal Data Affected: Identification data and any claim-related Personal Data voluntarily referenced by personnel in messages, threads or shared files.

Location: European Union (Slack EU data residency configured for messages and shared files at rest). Governed by the Slack Customer Terms of Service Data Processing Addendum.

Date of last update: 2026-05-19

VERSION HISTORY

Version | **Effective Date** | **Summary of Changes**

1.0 | 2026-05-19 | Initial publication