Data Processing Addendum

Unique AG

Version 2.0 (Jul 2025)

This Data Processing Addendum (“DPA”) forms part of the Contract / Main Agreement, Unique Terms of Service (accessible via https://www.unique.ai/terms-of-service), the Privacy Policy (https://www.unique.ai/privacy-policy), or other agreement governing the use of Unique’s service (collectively, the “Agreement”) entered by and between you (“you”, “your”, “Customer“, “Client”), and Unique AG (“Unique”, “provider”).

This DPA sets out the terms that apply with regard to the Processing of Personal Data (as defined below) by Unique, on behalf of Customer, in the course of providing the Unique Service to Customer under the Agreement.

All capitalized terms not defined herein will have the meaning outlined in the Terms of Service and the Main Agreement.

By clicking the "I agree" button/box on the Unique website, accessing the Unique website, utilizing the Service (e.g. Unique AI), or signing the DPA, you accept this DPA, you agree to be bound by this DPA and you represent and warrant that you have full authority to bind the Customer to this DPA.

1 DEFINITIONS

“Affiliate” means any entity that directly or indirectly controls is controlled by or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.1 “Authorized Affiliate” means any of Customer’s Affiliate(s) which (a) is subject to the Data Protection Laws and Regulations, and (b) is permitted to use the Service pursuant to the Agreement between the Customer and Unique and is not a “Customer” as defined under the Agreement.

1.2 “Authorized User” means any individual authorized or otherwise enabled by Customer to use the Service through Customer’s account.

1.3 “Controller” means the entity which determines the purposes and means of the Processing of Personal Data.

1.4 “Customer Data” means what is defined in the Agreement as “Customer Data”.

1.5 "Data Protection Laws" means all privacy and data protection laws and regulations applicable to the processing of personal data under the Agreement in the jurisdiction(s) specified in the MSA.

1.6 “Data Subject” means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.7 “Deployment options” means the three different deployment models Unique is currently offering: 1. Multi-tenant on Unique cloud, 2. Single tenant on Unique cloud and 3. Customer-manged tenant on customer cloud.

1.8 “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.9 “Personal Data” or “Personal Information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with a particular Data Subject or household, which is included in Customer Data Processed by Unique on behalf of Customer under the Agreement.

1.10 “Personal Data Breach” means a 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 by Unique on behalf of Customer under the Agreement.

1.11 “Personnel” means persons authorized by Unique to Process Customer’s Personal Data.

1.12 “Process” or “Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.

1.13 “Processor” means the entity that processes Personal Data on behalf of the Controller.

2 PARTIES AND ROLES

Details on the identities of the parties can be found in the main agreement. In this context and for the purposes of relevant Data Protection Laws, the Customer is the Data Controller, and Unique is the Data Processor (for multi-tenant and single-tenant deployment options on Unique cloud).

3 DATA PROCESSING

3.1 This DPA applies when Personal Data is Processed by Unique strictly on behalf of the Customer, as part of Unique's provision of the Service.

3.2 **Subject Matter**

Unique Processes Customer's Personal Data as part of providing Customer with the Service, pursuant to the specifications under the Agreement.

3.3 **Processing by Subprocessors**

Unique may engage third-party service providers to Process Personal Data on behalf of the Customer ("Sub-Processors"). The Sub-Processors are listed in **Appendix A**.

3.4 Technical and organizational measures are listed in **Appendix B**.

3.5 Insofar as a data processing operation falls within the scope of the GDPR, the competent authority in the EEA/EU is the authority according to art. 77 GDPR. A list of competent national data protection authorities in the EEA/EU can be found at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

3.6 Insofar as persons in Switzerland are affected or the data is processed in or from Switzerland, the competent authority is the Federal Data Protection and Information Commissioner (FDPIC). The contact details of the FDPIC can be found at https://www.edoeb.admin.ch.

3.7 Insofar as a data processing operation falls within the scope of the UK GDPR, the competent supervisory authority is the Information Commissioner's Office (ICO) in the United Kingdom.

3.8 Insofar as a data processing operation falls within the scope of applicable US federal or state privacy laws, the competent authority varies by jurisdiction and may include the Federal Trade Commission (FTC) at the federal level, state attorneys general, or other designated regulatory bodies as specified under the relevant state privacy legislation.

3.9 Insofar as a data processing operation falls within the scope of the Personal Data Protection Act (PDPA) in Singapore, the competent authority is the Personal Data Protection Commission (PDPC). The contact details of the PDPC can be found at https://www.pdpc.gov.sg.

3.10 **Categories of data subjects whose personal data is processed**

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following Categories of Data Subjects:

a) Prospects, customers, business partners, and vendors of Customers (who are natural persons)

b) Employees or contact persons of Customer's prospects, customers, business partners, and vendors

c) Employees, agents, advisors, and freelancers of Customers (who are natural persons)

d) Customer's Users authorized by Customer to use the Services

3.11 **Categories of personal data processed**

Unique collects information that alone or in combination with other information could be used to identify ("Personal Information"). Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following Categories of Personal Data:

a) First and last name

b) Title

c) Position

d) Employer

e) Contact information (company, email, phone, physical business address)

f) ID data

g) Professional life data

h) Personal life data

i) Localization data

The processor may collect further categories of Personal Data depending on how end users use Unique Services:

j) **Account Information**: When a Controller's End User creates an account with Unique, Unique may collect information associated with an End User account, including the End User's name and email address (collectively, "Account Information").

k) **User Content**: When the Controller uses Unique Services, Unique may collect Personal Information that is included in the input, file uploads, output, or feedback that the Controller provides to Unique's Services ("Content").

l) **Communication Information**: If the Controller's End Users communicate with Unique via a support channel, Unique may collect the Controller's End User name, contact information, and the contents of any messages you send ("Communication Information").

3.12 **Sensitive categories of data processed**

Customer may submit Special Categories of Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of Uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.13 **Nature of processing**

The nature of data processing is the collection and processing of the information of the persons involved during a recording.

3.14 **Purposes for Processing Personal Data on behalf of the Controller**

Recording use case:

The Processor will process contact information (company, email, phone, physical business address), start time of the recording, end time of the recording, and language in which conversations are held. The Processor stores and processes the voice and transcript of the conversations during a video call or an offline meeting via the Unique app. If video call services such as Zoom and MS Teams are used, video footage may be recorded if enabled.

The purpose of the data processing is to analyze and evaluate the conversation (e.g. generate GPT-based summaries, and follow-up emails) and to provide advice to the customer on the improvement of their sales process. All participants who have consent to the recording, transcription, and analyses of meetings and subsequent conversations and the transfer of respective data from the customers to the Processor are entitled to withdraw the given consent at any time with effect for the future. The withdrawal can be given without reason. To do so, these data subjects can contact us by email at privacy@unique.ch. As a consequence of the revocation, neither the customers nor Unique may continue to process the data based on this consent in the future.

Chat use case:
The Processor will store and process

a) internal documents and document texts that have been uploaded or connected to the Service by the Controller.

b) Account information provided by the Controller's End Users

c) prompts and answers of the Controller's end users.

Further, the Processor uses the Customer's personal data and meta data for the following purposes:

d) To facilitate, operate, enhance, and provide the Services;

e) To provide the Customers and users with assistance and support;

f) To gain a better understanding on how individuals use and interact with our Sites and Services, and how we could improve their and others' user experience, and continue improving our products, offerings and the overall performance of our Services;

g) To contact the Customers with general service-related messages,

h) To support and enhance the Processor's data security measures, including for the purposes of preventing and mitigating the risks of fraud, error, or any illegal or prohibited activity;

i) To comply, and maintain compliance, with applicable laws, regulations, and standards.

3.15 **Duration of processing**

Unique will retain the Customer's personal data for as long as is reasonably necessary to maintain and provide its services, to comply with its legal and contractual obligations, or to protect Unique from any potential disputes (i.e. as required by law for log-keeping, record keeping, and accounting purposes, and to have evidence and proof of its relationship with the Customer in the event that any legal issues arise after the Customer ceases to use the Services), all in accordance with Unique's Data Retention Policy. Please note that except as required by applicable law or the specific agreements between the Provider and the Customer, Unique will not be obligated to retain personal data for any particular period (except, audit logs will be kept for 10 years), and are free to securely delete it or restrict access to it for any reason and at any time, with or without notice to the client. Questions about the data retention policy of the client can be asked by email at privacy@unique.ch.

4 Data Protection

4.1 The Provider must, at all times, take all necessary security and protective measures against, in particular, destruction, loss, access by unauthorized third parties or alteration of or to data provided or administered by the Client or its subcontractors to which the Provider has access for the purposes of fulfilling its obligations under the Agreement.

4.2 The Provider undertakes to and shall ensure to report to Client any incident impacting the confidentiality, integrity, and availability of Client's or its subcontractors' data, promptly and without undue delay, but in no event later than 24 hours after becoming

aware of any incident, by sending an email to Uniques Enterprise address and by calling the contact person designated (from time to time) by the Client. The email must detail the known details of the incident, the implications, and the Provider's actions undertaken in response to such an event.

5 Data Property

All Confidential Information is and shall remain the Client's exclusive property, and shall be treated as the Client's Confidential Information. Likewise, the information generated by the systems, such as application logs, tables, reports, accounts, and printed material of any and all types (account statements, etc.), is the Client's exclusive property. The Provider shall acquire no rights over this information or data and only use the Confidential Information to the extent necessary for the performance of the Services. Unless written approval from the Client is given in advance, Confidential Information must not be, notably:

a) used by the Provider and/or its employees, agents, or representatives other than for the strict fulfillment of those obligations stipulated in the Agreement, which implies the data shall be rigorously physically and/or logically segregated from data of the Provider's other users;

b) disclosed, sold, given, handed over, or made accessible in any other way by the Provider and/or by its employees, agents, or representatives to third parties.

6 Data Storage, Return, and Destruction

6.1 The Provider will accurately and completely collect and maintain information regarding the storage location, media, and method of storage of all Confidential Information on an ongoing basis. The storage shall remain in Switzerland. At the Client's request and by the termination of the Agreement at the latest, the Provider undertakes, at its own costs,

a) to return to the Client, within a reasonable time and in its existing format, data which the Provider has knowledge of, and

b) to delete or destroy all or part of any such data that might remain in the Provider's possession or of which the Provider might have retained a copy (especially in archived or backed-up files) which is subject to the applicable legal provisions, particularly record keeping.

6.2 Except in those cases where the Provider is using the Client's material, the Provider shall guarantee a backup policy on its material to enable recovery of the data related to the Services in the event of data loss. Any associated costs shall be borne by the Provider.

7 GOVERNING LAW AND EXCLUSIVE COURTS

Unless the GDPR is mandatory or otherwise specified in the MSA, this Agreement shall be governed exclusively by Swiss substantive law, without regard to its choice of law or conflicts

of law principles, Customer and Unique consent to the exclusive jurisdiction and venue in the courts in Zurich 1, Switzerland.

APPENDIX A – LIST OF THE SUB-PROCESSORS OF THE DPA

Details on sub-processors activities:

Name	Purpose	Location	More information
Microsoft, Inc.	Infrastructure, Cognitive Services, Azure OpenAI services, Emails	CH or chosen location by the client	Azure cloud computing, networking and storage provider. Processing of audio streams for the purpose of live transcription into spoken text. Processing of conversation transcripts and meta data for the purpose of creating reports. Processing of user email and meeting meta data for the purpose of sending emails.

APPENDIX B - TECHNICAL AND ORGANIZATIONAL MEASURES (TOM) Unique AG

TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define Unique's current security measures. Unique may change these at any time without notice so long as they maintain a comparable or better level of security. This may mean that individual measures are replaced by new measures that serve the same purpose without diminishing the security level.

Physical Access Control.

Unauthorized persons are prevented from gaining physical access to premises, buildings, or rooms where data processing systems that process and/or use Personal Data are located.

Measures:

- Unique protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.
- In general, buildings are secured through access control systems.
- As a minimum requirement, the outermost entrance points of the building must be fitted with a certified key system including modern, active key management.
- Depending on the security classification, buildings, individual areas, and surrounding premises may be further protected by additional measures.
- Access rights are granted to authorized persons on an individual basis according to the System and Data Access Control measures (see Sections 1.2 and 1.3 below). This also applies to visitor access. Guests and visitors to Unique buildings must register their names at reception and must be accompanied by authorized Unique personnel.

Additional measures for Data Centers:

- All Data Centers adhere to strict security procedures enforced by guards, surveillance cameras, motion detectors, access control mechanisms and other measures to prevent equipment and Data Center facilities from being compromised. Only authorized representatives have access to systems and infrastructure within the Data Center facilities. To ensure proper functionality, physical security equipment (e.g., motion sensors, cameras, etc.) undergo maintenance on a regular basis.
- Unique and all third-party Data Center providers log the names and times of persons entering Unique's private areas within the Data Centers.

System Access Control.

Data processing systems used to provide the Unique Services must be prevented from being used without authorization.

Measures:

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Processes are in place to ensure that authorized users have the appropriate authorization to add, delete, or modify users.
- All users access Unique's systems with a Unique identifier (user ID).
- Two-factor authentication is enforced in data center operations and for critical systems.
- Unique has procedures in place to ensure that requested authorization changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorization). If a user leaves the company, his or her access rights are immediately revoked after his or her last working day.
- Unique has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and default passwords to be changed on the first login. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months in compliance with the requirements for complex passwords. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- Security patch management is implemented to ensure regular and periodic deployment of relevant security updates.
- Full remote access to Unique's corporate network and critical infrastructure is protected by strong authentication.

Data Access Control.

Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified, or removed without authorization in the course of processing, use, and storage.

Measures:

- As part of the Unique Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Unique Information Classification standard.
- Access to personal, confidential, or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. Unique uses authorization concepts that document how authorizations are assigned and which authorizations are assigned to whom. All personal, confidential, or otherwise sensitive data is protected in accordance with the Unique security policies and standards. Confidential information must be processed confidentially.
- The Provider must, at all times, take all necessary security and protective measures against, in particular, destruction, loss, access by unauthorized third parties or alteration of or to data provided or administered by the Client or its subcontractors to which the Provider has access for the purposes of fulfilling its obligations under the Agreement
- All production servers are operated in the Data Centers or in secure server rooms. Security measures that protect applications processing personal, confidential, or other sensitive information are regularly checked. To this end, Unique conducts internal and external security checks and penetration tests on its IT systems.

- Unique does not allow the installation of personal software or other software that has not been approved by Unique.
- A Unique security standard governs how data and data carriers are deleted or destroyed once they are no longer required.
- External audits in place: Unique is ISO 27001, 9001 and 42001 certified. Furthermore, Unique also has SOC 2 Type 2 certification and adheres to all relevant FINMA standards (refers to the 2018/3 Outsourcing Circular).

Data Transmission Control.

Except as necessary for the provision of the Services in accordance with the relevant service agreement, Personal Data must not be read, copied, modified, or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at Unique to ensure the agreed-upon service levels (for example, encryption and lead-lined containers).

Measures:

- Personal Data transfer over Unique internal networks are protected in the same manner as any other confidential data according to Unique Security Policy.
- When data is transferred between Unique and its customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant Agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of Unique-controlled systems (e.g. data being transmitted outside the firewall of the Unique Data Center).

Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from Unique data processing systems.

Measures:

- Unique only allows authorized persons to access Personal Data as required in the course of their work.
- Unique has implemented a logging system for input, modification and deletion, or blocking of Personal Data by Unique or its subprocessors within Unique's Products and Services to the fullest extent possible.

Job Control

Personal Data being processed on commission (i.e., Personal Data processed on a customer's behalf) is processed solely in accordance with the relevant agreement and related instructions of the customer.

Measures:

- Unique uses controls and processes to ensure compliance with contracts between Unique and its customers, subprocessors, or other service providers.
- As part of the Unique Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the Unique Information Classification standard.

- All Unique employees and contractual subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of Unique customers and partners.
- For on-premise support services, Unique provides a specially designated, secure support ticket facility, in which Unique provides a special access-controlled and monitored security area for transferring access data and passwords. Unique customers have control over their remote support connections at all times. Unique employees cannot access a customer system without the knowledge or full active participation of the customer.

Availability Control

Personal Data will be protected against accidental or unauthorized destruction or loss.

Measures:

- Unique employs backup processes and other measures that ensure rapid restoration of business-critical systems as and when necessary.
- Except in those cases where the Provider is using the Client's material, the Provider shall guarantee a backup policy on its material to enable recovery of the data related to the Services in the event of data loss. Any associated costs shall be borne by the Provider
- Unique uses uninterrupted power supplies (for example: UPS, batteries, generators, etc.) to ensure power availability to the Data Centers.
- Unique has defined contingency plans as well as business and disaster recovery strategies for the provided Services.
- Emergency processes and systems are regularly tested.

Data Separation Control

Personal Data collected for different purposes can be processed separately.

Measures:

- Unique uses logical separation to achieve data separation among Personal Data originating from multiple customers, and physical separation to achieve data separation among Personal Data origination from multiple enterprise customers.
- Unique uses strictly separated production and testing environments.
- Customers (including their Affiliates) have access only to their own data.
- If Personal Data is required to handle a support incident from a specific customer, the data is assigned to that particular message and used only to process that message; it is not accessed to process any other messages. This data is stored in dedicated support systems.

Data Integrity Control

Personal Data will remain intact, complete, and current during processing activities. Unique has implemented a multi-layered defense strategy as a protection against unauthorized modifications.

Measures:

- Firewalls;

- Security Monitoring Center;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures;
- Risk management;
- Privileged access management

ANNEX I: LIST OF PARTIES

Controller(s):

Name: *as specified in the DPA*

Address: *as specified in the DPA*

Contact person's name, position, and contact details: *as specified in the DPA*

Signature and accession date: *as specified in the DPA*

Processor(s):

Name: *Unique AG*

Address: *Stockerstr. 34, 8002 Zürich*

Contact person's name, position, and contact details: *Manuel Grenacher, CEO*

Signature and accession date: *as specified in the DPA*