DATA PROCESSING ADDENDUM

Unique AG, Version 2.0 (March 2024)

This Data Processing Addendum (“DPA”) forms part of the Unique Order Form/ POC contract / main agreement, Unique Terms of Service (accessible via https://www.unique.ch/terms), the Privacy Policy (https://www.unique.ch/privacy) 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 set forth in the Terms of Service and the Order Form / POC contract / main agreement.

By clicking the "I agree" button/box on the Unique website or the box in the Order Form, accessing the Unique website or by utilizing the Service (e.g. Unique FinanceGPT) or by 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

1.1 “**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.

1.2. “**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 Customer and Unique, but has not signed its own Order Form with Unique and is not a “Customer” as defined under the Agreement.

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

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

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

1.6 "**Data Protection Laws**" means all privacy and data protection laws and regulations, including the laws and regulations of the European Union, the European Economic Area and its Member States and Switzerland, applicable to the processing of personal data under the Agreement.

1.7. “**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.

1.8 “**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.

1.9. “**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).

1.10. “**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.

1.11. “**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.

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

1.13. “**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.

1.14. “**Processor**” means the entity which Processes Personal Data on behalf of the Controller.

1.15. “**S-DPA**” is the Swiss Data Protection Act of September 25th, 2020, in force since September 1st, 2023.

2. PARTIES AND ROLES

Parties involved and distribution of roles under data protection law: Details on the identities of the parties can be found in the Unique Order Form/ POC contract / main agreement. In this context and for the purposes of the GDPR, S-DPA or any similar Data Protection Laws, 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. Scope. This DPA applies when Personal Data is Processed by Unique strictly on behalf of 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 Sub processors. Unique may engage third-party service providers to Process Personal Data on behalf of Customer ("Sub-Processors"). The Sub-Processors are listed in **Appendix A**.

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

3.5. Applicable Rules for the processing. The rules of the EU Standard Contractual Clauses (SCC) between controllers and processors within the European Economic Area (EEA) in Appendix C, according to the European Commission Implementing Decision 2021/915 of 4 June 2021 under Article 28 (7) of Regulation (EU) 2016/279 of the European Parliament and of the Council, apply. References to the GDPR are to be understood as references to the S-DPA insofar as data processing is subject to the S-DPA.

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.

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.

3.6. Categories of data subjects whose personal data is processed. The Personal Data transferred concern the following Categories of Data Subjects:

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by 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 Customer (who are natural persons)

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

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

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

3.7. Categories of personal data processed. The Personal Data transferred concern the following Categories of Data:

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) Localisation data

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

- 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").

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

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

3.8. Sensitive categories of data processed. The Personal Data transferred concern the following sensitive Categories of Data:

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.

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

3.10. Purpose(s) for which the personal data is processed 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 Unique app. If video call services such as Zoom and MS Teams are used, video footage may be recorded if enabled.

Purpose of the data processing is to analyze and evaluate the conversation (e.g. generate GPT-based summaries, follow up emails) and to provide advise 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, art. 7 para. 3 GDPR / art. 30 para 2 letter b S-DPA. The withdrawal can be given without reasons. 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 for the future.

Chat use case:
The Processor will store and process

- internal documents and document texts that have been uploaded or connected to the Service by the Controller.
- account information provided by Controller's End Users
- prompts and answers of the Controller's end users.

Further, the Processor uses the Customers' personal data for the following purposes:

- To facilitate, operate, enhance, and provide the Services;
- To provide the Customers and users with assistance and support;
- 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;

- To contact the Customers with general service-related messages,
- To support and enhance the Processors data security measures, including for the purposes of preventing and mitigating the risks of fraud, error or any illegal or prohibited activity;
- To comply, and maintain the compliance, with applicable laws, regulations and standards.

3.11. 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 your personal data for any particular period (except, audit logs will be kept for 10 years), and we are free to securely delete it or restrict access to it for any reason and at any time, with or without notice to you. If you have any questions about our data retention policy, please contact us by e-mail at privacy@unique.ch.

4. GOVERNING LAW AND EXCLUSIVE COURTS

Unless the GDPR is mandatory, 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.

5. SIGNATURE

Unique:

Name:

Title:

Date:

Signature:

Manuel Grenacher, CEO Unique AG
Zurich, 29/03/2024

SES **Simple electronic signature**
Signed on Skribble.com

Customer:

Name:

Title:

Date:

Signature:

Name:

Title:

Date:

Signature:

Sina Wulfmeyer

27/03/2024

SES **Simple electronic signature**
Signed on Skribble.com

Name:

Title:

Date:

Signature:

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

Deployment model	Public/ Multi tenant	Single tenant at Unique cloud	Customer-managed single tenant at Customer Cloud
Sub-processors	• Microsoft Inc. • Feedbear • Intercom • Mixpanel • MongoDB	Microsoft Inc.	no sub-processors

Details on sub-processors activities:

Name	Solution	Purpose	Location	More information
Microsoft, Inc.	Chat + Recording	Infrastructure	CH	Azure cloud computing, networking, and storage provider.
MongoDB	Recording	Database	CH	DBMX Provider. Data stored on Azure.

Name	Solution	Purpose	Location	More information
Microsoft, Inc. (Azure SMTP)	Chat + Recording	Emails	CH	Processing of user email and meeting meta data for the purpose of sending emails
Feedbear	Recording	Feedback	EU	**OPTIONAL**, processing of username, email and avatar image for the purpose of collecting feedback on features and improvements. *No feedback possible if deactivated.*
Intercom	Recording	Messaging	EU	**OPTIONAL**, processing of username, email, avatar image for the purpose of collecting support requests from users. *No support requests available if deactivated.*
Hotjar, Ltd	Recording	Tracking	EU	**OPTIONAL**, processing of username and website usage for the purpose of tracking user behavior to improve usability.
Mixpanel	Recording	Tracking	EU	**OPTIONAL**, processing of username and avatar image for the purpose of tracking user behavior to improve usability. *No user impact if deactivated.*

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

- in accordance with article 32 GDPR / art. 8 S-DPA -

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 it maintains 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 Section 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 operation 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 revoked.
- Unique has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and default passwords to be changed on first login. Personalized user IDs are assigned for authentication. All passwords must fulfil 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.

- 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 and 9001 certified. SOC 2 and FINMA-report (related to 2018/3 Outsourcing Circular) are in preparing (planned for Q4 2023).

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.
- 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

APPENDIX C – EU-STANDARD CONTRACTUAL CLAUSES

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor’s opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of Uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

   (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

   (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

   (4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial
notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

<u>SECTION III – FINAL PROVISIONS</u>

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

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: *Stockerstrasse 34, 8002 Zürich*

Contact person's name, position and contact details: *Manuel Grenacher, CEO, manuel@unique.ch*

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

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

as specified in the DPA.

Categories of personal data processed

as specified in the DPA

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

as specified in the DPA

Nature of the processing

as specified in the DPA

Purpose(s) for which the personal data is processed on behalf of the controller

as specified in the DPA

Duration of the processing

as specified in the DPA

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

as specified in the DPA

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

as specified in the DPA

ANNEX IV: LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).

Omitted as Option 2 has been selected. A list of sub-processors can be found in the DPA.