Data Processing Addendum (DPA)
according to Article 28 Section 3 GDPR

between

_____

_____

_____

_____

later referred to as «**Customer**»

and

enuvo GmbH
Seefeldstrasse 25
8008 Zurich
Switzerland

later referred to as «**enuvo**»

1. Subject Matter

enuvo processes Personal Data of the Customer according to Article 3 Section 2 and Article 28 GDPR on the basis of this agreement.

If the agreed upon processing service is not being executed within a member state of the European Union or in a state that is member of the European Economic Area, processing may only take place in that third country if the special requirements of Article 44 ff. GDPR are being complied with.

2. Duration of the Agreement

This agreement is concluded for an indefinite period.

The Customer can terminate the contract at any time without notice if there has been a serious breach of data protection regulations or of this agreement, caused by enuvo, under the conditions that enuvo cannot or refuses – in breach of this agreement – to comply with the Customer's instructions or if enuvo refuses to comply with the Customer's control rights. In particular, failure to comply with the obligations agreed upon in this contract constitutes a serious breach.

3. Type and Purpose of Processing; Type of Data and Data Subjects

enuvo allows the Customer to conduct online surveys. The Customer creates and designs online surveys and questionnaires independently. enuvo is only providing the software to do so. Survey questions can be freely formulated, and the survey participants are determined and invited by the Customer themselves. enuvo solely ensures that the Customer's surveys are accessible via the Internet and that the responses of survey participants are stored securely. enuvo then enables the Customer to view and analyze the collected survey results.

The Customer can conduct surveys to a multitude of topics that are not pre-defined. This may be employee surveys, customer satisfaction surveys, website visitor surveys, market research surveys, and many more. Therefore, the type of data that can be collected through such surveys is indefinite. Mainly, however, the collected data represents answers to questions within such a survey. This can typically be Personal Data such as name, e-mail address, postal address, telephone number, occupation, age and other information that can be used in combination with other data to identify an individual person. The type of Personal Data collected is determined by the Customer, since they define the questions within a questionnaire that need to be answered.

Depending on the type of survey, the type of survey participants can vary. These may be employees, customers, website visitors, or random people who are willing to participate in the survey (for example in a market research survey). The circle of those affected is determined by the Customer.

4. Obligations of the Customer

The Customer is solely responsible for assessing the admissibility of the processing pursuant to Article 6 Section 1 GDPR and for safeguarding the rights of the data subjects pursuant to Articles 12 to 22 GDPR.

The Customer is obliged to confidentially treat all knowledge of business secrets and data security measures of enuvo acquired within the scope of the contractual relationship. This obligation shall continue to apply even after termination of this agreement.

5. Obligations of enuvo

enuvo shall maintain confidentiality when processing the Customer's Personal Data in accordance with this agreement. This shall continue to apply even after termination of the agreement.

enuvo shall process data and processing results exclusively within the framework of the Customer's instructions. If enuvo receives a legally binding order to deliver data from the Customer, enuvo must - if legally permissible - inform the Customer immediately and refer the authority to them. Likewise, processing Customer's Personal Data for enuvo's own purposes requires written permission from the Customer.

enuvo confirms that they have obligated all employees and parties entrusted with data processing to maintain confidentiality or that they are subject to an appropriate statutory duty of confidentiality prior to commencing their work. The confidentiality obligation of these employees and parties shall remain in force even after termination of their activities and termination of their employment with enuvo.

enuvo confirms that they have taken all necessary measures to guarantee the security of the processing in accordance with Article 32 GDPR. The corresponding Technical and Organizational Measures are part of this agreement as **Annex 1**.

enuvo ensures Technical and Organizational Measures so that the Customer can comply with the legal requirements set in Chapter III of the GDPR (information and access to Personal Data, rectification, erasure, right to object and automated individual decision-making) within the legal deadlines. If such a request is submitted directly to enuvo, the data processor, instead of to the Customer, the data controller, enuvo shall immediately forward the request to the Customer and inform the requester accordingly.

enuvo assists the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR (security of processing, notification of a Personal Data breach to the supervisory authority,

communication of a Personal Data breach to the data subject, data protection impact assessment and prior consultation).

The Customer is granted the right to inspect and control the data processing facilities at any time with regard to the processing of data provided by them, including third parties commissioned by them. enuvo undertakes to provide the Customer with the information necessary to monitor compliance with the obligations set out in this agreement. enuvo may claim remuneration for enabling Customer inspections.

After termination of this agreement, enuvo is obliged to destroy all processing results and documents containing data on behalf of the Customer. The storage and archiving of data in accordance with legal requirements remains unaffected.

enuvo shall immediately inform the Customer if they consider that an instruction from the Customer violates data protection regulations of the GDPR.

6. Communication in the Case of Infringements

enuvo shall immediately inform the Customer of any infringements or irregularities concerning the processing of the Customer's Personal Data that enuvo has become or was made aware of. enuvo assures to adequately support the Customer in their reporting and notification obligations under Articles 33 and 34 GDPR, if necessary. enuvo may claim compensation for support services which are not included in enuvo's description of services and which are not attributable to failures caused by enuvo.

7. Sub-contracting with Sub-processors

enuvo may appoint and engage Sub-processors. enuvo must inform the Customer in good time of the intended appointment of a new Sub-processor, so that they can raise an objection if necessary. As a condition to permitting a third-party Sub-processor to process Personal Data, enuvo will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those found in this agreement, to the extent applicable to the nature of the Services provided by such Sub-processor.

At present, various Sub-processors are engaged to process Personal Data for the Customer. A complete list of all Sub-processors can be found in **Appendix 1**. The Customer declares his agreement to their assignment.

8. Miscellaneous

If any provision of this agreement is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed, and the remainder of the agreement will remain in full effect. The invalid or unenforceable provisions shall be replaced by a provision that comes as close as possible to the economic purpose of the invalid or unenforceable provisions. The same applies in the case of loopholes.

Any agreements on data processing previously made between enuvo and the Customer will be replaced by this agreement as of May 25, 2018. Otherwise, this agreement shall enter into force immediately.

On behalf of enuvo:

enuvo GmbH
Seefeldstrasse 25
8008 Zurich
Switzerland

Data Protection Officer:
Lionel Marbot
lionel.marbot@enuvo.ch

Date

May 24, 2018

Signature

Lionel Marbot

On behalf of Customer:

Name of signatory:

_____

Role of signatory:

_____

Email address of signatory:

_____

Date

_____

Signature

_____

Appendix 1: Technical and Organizational Measures

Technical and organizational measures

enuvo GmbH (hereinafter also referred to as “enuvo”, “vendor”, “we”, “us”, etc.) is the operator of the online survey platform, later referred to as “platform”. The company is headquartered in Zurich, Switzerland. The headquarter contains only office space, which serves the support as well as the further development of the platform.

Data collected by enuvo (survey responses, etc.) is being stored and processed exclusively in European data centers (Ireland and Germany) powered by Amazon Web Services (AWS). In Zurich, data is only processed temporarily in order to fulfil support requests from the customer.

1. Pseudonymization and encryption of personal data

We offer access to our software exclusively encrypted via SSL. Unencrypted calls to http:// are automatically forwarded to https://.

All data transferred from our data centers to our support team in Zurich is encrypted via HTTPS (SSL). This is the same encryption that customers (survey creators) and their end customers (survey respondents) use to access online surveys.

All passwords as well as sensitive tokens (e.g. to reset a password) stored in the database are securely "salted" and "hashed" and therefore not readable in plain text by anyone, not even system administrators. This procedure is irreversible.

All data can only be accessed through authenticated and authorized access. In addition, all databases, including backups, are protected by port and IP filters at a network level. During maintenance work by enuvo on a database, the IP address of enuvo is briefly whitelisted. Access to the database is then possible for enuvo, but still only after successful authentication and authorization. Our databases or backups are never exposed to third parties over the Internet.

The network settings for accessing the databases can be adjusted by the designated system administrator. This administration access to AWS is currently only available to one person (Lionel Marbot, owner). Access is protected by two-factor authentication.

Due to the high level of security described above, no other data encryption is currently used.

Personal data collected by the customer is not structured and can be found everywhere in a respondent’s responses. For this reason, pseudonymization of this data is not possible.

2. Ensuring confidentiality

Office for customer support and software development, Zurich, Switzerland

Our offices are only accessible with an appropriate key. Each employee has a personal key to get to their workplace. Relevant for the work is the access to the platform, which is only possible with valid credentials (user name and password). Processing of personal data in private spaces (telework or home work of employees of enuvo) is permitted, provided that the measures pursuant to Art. 32 GDPR are still ensured.

Every employee must sign in to the platform to be able to work. Employees have personal credentials known only to themselves. Each employee is assigned appropriate user privileges according to their needs. All employees are also instructed to lock their computers when they leave their workplace, even if only for a short period of time (e.g. coffee break).

All computers are password-protected, have secure anti-virus software installed and are behind a hardware firewall.

No personal data of customers is permanently stored in Zurich. Production data is also never used in development environments.

Data centers, Europe (Ireland and Germany)

enuvo provides “Software as a Service” which is being run completely on the IT infrastructure of Amazon Web Service, Inc. (AWS). Both hardware and software are operated in data centers of this sub-processor within the EU (Dublin and Frankfurt). Data collected by enuvo will never be stored or processed outside the EU.

Please refer to Article 8, Sub-processors, to learn more about how AWS complies with GDPR.

3. Ensuring integrity

enuvo's survey platform is operated as Software as a Service (SaaS). All customer data is stored and processed on the same infrastructure. All customers identify themselves with our service using their personal credentials. We use a logical data separation (enforced with software), meaning that each customer can only access their own data. It is not possible for customers to access data of other customers.

Only employees responsible for customer support have the necessary privileges to enter, modify and delete data on behalf of the customers. Each employee only has the authorizations necessary to fulfil

their duties. Every employee has as many privileges as necessary, but as little as possible. Managing privileges is only possible for the system administrator.

Employees are contractually bound to comply with data secrecy and due diligence. Employees and their activities are constantly monitored.

enuvo confirms that it complies with all legal requirements on data protection and data secrecy and that it trains and regularly monitors compliance by its employees.

4. Ensuring availability

AWS provides various "regions" worldwide in which its services can be used. Each region has at least two independent data centers where the services can also be shared for increased resilience.

We currently use the region “Ireland” for our services and have replicated our servers and databases to three data centers within Ireland. This ensures that in the unlikely event of a system failure within a data center, automatic fail over is made to one of the two other data centers. This automatic "fail-over" procedure enables us to operate redundant and highly available software.

Our databases are automatically backed up, saving the data from the last 35 days (rolling backups). For larger software updates, we also create manual backups that do not automatically expire.

Backups of databases are all made and stored in these European data centers. As mentioned in Article 1, Pseudonymization and encryption of personal data, access to backups is not possible for third parties. No backups are stored in Zurich.

5. Resilience of processing systems and services

The security of customer data is of the utmost importance to enuvo. Employees are continuously trained in a wide variety of data security topics and receive sufficient time and resources to incorporate this knowledge into their work. This not only concerns the technical security of the software, but also the avoidance of social engineering, e.g. phishing attempts, etc.

Our application was also subjected to an extensive penetration test by Protect7 (www.protect7.com) and any found vulnerabilities were corrected immediately. In the event of a fundamental software renewal, we would have new tests carried out.

The physical resilience of our data centers is guaranteed by the sub-processor AWS.

6. Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Backups of our databases described in Article 4, Ensuring availability, can be recovered to any point-in-time within the last 35 days. In the unlikely event of a total failure that would not be automatically resolved by our redundant IT infrastructure, manual processes for restoring operation and access to software and its data would be applied.

7. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

Just like any other company that is operating software, it is normal to regularly experience (minor) technical issues, for example caused by hardware failure, corrupt updates, etc. Thanks to our redundant IT infrastructure, such issues are automatically eliminated via fail-over with zero downtime. Every incident represents a successful test of our technical measures under real conditions.

Furthermore, there are often survey creators (customers) who accidentally delete their own data from our system. We can then restore this data by performing a full restore of a backup. Such a recovery is the same as it would be necessary to restore the entire system. Thus, the system recovery is regularly checked and optimized.

8. Sub-processors

enuvo has executed Data Processing Addendums (DPA) with each individual sub-processor, according to Article 28, Section 4, GDPR.

Amazon Web Services, Inc., 410 Terry Avenue North, Seattle, WA 89109-5210, USA

All personal data is stored and processed in European data centers of our sub-processor Amazon Web Services (AWS).

enuvo has executed a Data Processing Addendum with AWS, namely "AWS DATA PROCESSING ADDENDUM", which complies with the standard contractual clauses (also referred to as model clauses) defined and approved by the European Commission. The agreement with AWS is an integral part of these technical and organizational measures. Due to an integrated non-disclosure agreement, the DPA cannot be viewed by third parties.

AWS is GDPR-compliant and is ISO 27001, 27017 and 27018 certified. ISO 27018 is a code of conduct for the protection of personal data in the cloud. It is based on the ISO 27002 information security standard and serves as a guideline for the implementation of ISO 27002-controls that apply to personal data that uniquely identifies a person in the public cloud. The standard provides additional controls and guidelines for the protection requirements of personal data that are not taken into account by the current controls of ISO 27002.

By complying with this standard, AWS has a system of control mechanisms that are specifically concerned with the protection of private data. By complying with this internationally recognized guide and independently reviewing it, AWS demonstrates its commitment to customer content privacy.

Further information on our sub-processors and their certifications can be found here:
https://aws.amazon.com/compliance/gdpr-center/

Hostpoint AG, Neue Jonastrasse 60, 8640 Rapperswil-Jona, Switzerland

Hostpoint is a Swiss hosting provider that we use for smaller projects and websites. This provider may be used to temporarily store customer data in the process of responding to customer support requests.

Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Google operates our e-mail infrastructure (Gmail) with their product "G Suite", which we use to ensure customer support and communicate internally. If you send us an e-mail, for example, this e-mail will be processed by Gmail.

However, the sending of survey invitations, etc., is not processed via Google, but via Amazon Web Services. Google does not generally process survey data.

Trello, Inc., 55 Broadway, 25th Floor, New York, NY 10006, USA

Trello is an online software service that we use for internal project management. We use this service mainly in connection with the further development of our own software. When recording new customer requirements for our software, we may, for example, also store the content of a customer e-mail in Trello.

Slack Technologies, Inc., 500 Howard Street, San Francisco, CA 94105, USA

Slack is an online messenger that we use for internal communication. It is possible that we refer to customers in the context of our internal communication (e.g. on the basis of the customer e-mail address).