DATA PROCESSING AGREEMENT (ARTICLE 28 GDPR)

Last updated 01.06.2026

This Data Processing Agreement ("DPA") forms part of the SurveyEngine Terms of Service and applies automatically to all customers maintaining an active paid subscription to SurveyEngine Services.

This DPA is entered into between:

SurveyEngine GmbH

Viktoria-Luise-Platz 7

10777 Berlin

Germany

and

the legal entity or individual that has purchased a paid subscription to SurveyEngine Services ("Customer").

This DPA becomes effective automatically upon commencement of a paid subscription and remains in force for the duration of the Services.

Preamble

This Data Processing Agreement (DPA) details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller. The Platform Subscription (hereinafter "Services"), the purchased subscriber platform terms (https://surveyengine.com/corporate/terms/service-terms) and this DPA forms the entire Agreement (hereinafter, the "Agreement)

Applicability of this DPA

This DPA applies solely to paid subscriptions and paid services purchased from SurveyEngine and its regulations shall apply to any and all activities associated with the Agreement, in whose scope Supplier and its authorised subprocessors process Company's personal data (hereinafter, "Data") on behalf of Company as a controller (hereinafter, "Contract Processing").

Free trials, demonstration accounts, evaluation accounts, expired subscriptions and other unpaid use of the platform are not covered by this DPA unless expressly agreed in writing by SurveyEngine.

1. Scope, duration and specification of contract processing of Data

The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the following Data:

DATA TYPE	PURPOSE	DATA SUBJECTS
ACCOUNT INFORMATION	User management and platform access	Customer users
SURVEY CONFIGURATION DATA	Survey delivery	Customer users
SURVEY RESPONSE DATA	Collection and storage of research data	Respondents
TECHNICAL METADATA	Security, quality assurance, fraud detection and platform operation	Users and respondents
SUPPORT COMMUNICATIONS	Customer support	Customer users

Except where this annex stipulates obligations beyond the term of the Agreement, the term of this annex shall be the term of the Agreement.

The principal administrative account holder of the Services named by email is solely authorised by the Company (Controller) to issue binding instructions to the Supplier (Processor) in connection with the processing of personal data under this Agreement:

The Company may update or replace the above-named persons at any time by administrator changes through the platform.

Until such notice is received, the Supplier shall treat the persons named above as authorised to give instructions on behalf of the Company.

Customer instructions shall be limited to functionality available through the Services and requests required under applicable data protection law.

2. Scope of application and responsibilities

(a) Supplier shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work.. Within the scope of this Agreement, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(b) Company's individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Company shall, subsequently, be entitled to, in writing or in a machine- readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Agreement shall be treated as requests requests outside the scope of the Services. Company shall, without undue delay, confirm in writing or in text form any instruction issued orally.

3. Supplier's obligations

(a) Except where expressly permitted by Article 28 (3)(a) of the GDPR, Supplier shall process data subjects' Data only within the Services. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

(b) Supplier shall, within Supplier's scope of responsibility, organise supplier's internal organisation so it satisfies the specific requirements of data protection. Supplier shall implement technical and organisational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organisational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk.

The detailed technical and organisational measures applied by Supplier are described in Annex 1 ("Technical and Organisational Measures / TOMs") which forms an integral part of this Agreement. Supplier may update these measures provided that the level of protection is not reduced; Supplier shall inform Company of any material changes.

(c) Supplier shall support Company, to the extent reasonably required and proportionate to the Services., insofar as is agreed upon by the parties, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR. Requests requiring substantial manual effort may be chargeable.

(d) Supplier warrants that all employees involved in Contract Processing of Company's Data and other such persons (e.g., external IT administrators, maintenance engineers, or auditors explicitly engaged by Supplier for technical support) as may be involved in Contract Processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

Processing is performed using cloud infrastructure operated by approved subprocessors and through secure administrative access controls.

(e) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility. Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.

(f) Supplier shall notify to Company the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

(g) Supplier warrants that Supplier fulfills its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(h) Supplier shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Supplier shall, based on Company's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Company. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

In specific cases designated by Company, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

(i) Customer may export data using platform functionality prior to termination.

(j) Standard subscriptions are hosted within Google Cloud Platform's Frankfurt (Germany) region. Alternative approved hosting regions may be available under higher tier subscriptions at the Company's request.

(h) SurveyEngine does not use Customer Content, Personal Data, survey responses or project data for the training of artificial intelligence or machine learning models unrelated to the provision of the Services.

Should Supplier intend to transfer data to a third country, Supplier shall inform Company in advance and may do so only with Company's prior consent and subject to the standard contractual clauses (Art. 46 GDPR).

4. Company's obligations

(a) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.

(b) Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with Article 82 of the GDPR. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

(c) Company shall notify to Supplier the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

(d) Company retains ownership of Customer Content, including survey instruments, response data, uploaded materials and project data. SurveyEngine processes such data solely in accordance with Company instructions and this DPA.

5. Enquiries by data subjects

(a) Where a data subject assert claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction insofar as agreed upon. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner. Requests requiring substantial manual effort may be chargeable.

6. Options for documentation

SurveyEngine satisfies its documentation obligations through this DPA, its published compliance documentation, subprocessor disclosures, privacy documentation, and any certifications or compliance reports made generally available to customers. Except where legally required, SurveyEngine is not required to provide customer-specific documentation, complete customer-specific questionnaires, participate in procurement meetings, or modify its standard security controls, processes, infrastructure, or documentation.

(a) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this exhibit by appropriate measures.

(b) Compliance information is provided through documentation, policies, questionnaires and certifications made available by SurveyEngine.

(c) Where specific types of documentation and proof can be identified, with regard to compliance with the obligations agreed upon, Supplier may make available to Company codes of conduct (as stated in SOPs) approved in accordance with Article 40 of the GDPR.

(b) On-site audits are only available where legally required. Where, in individual cases, audits and inspections by Company or an auditor appointed by Company are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Supplier's operations, upon prior notice, and observing an appropriate notice period. Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Supplier shall be entitled to rejecting auditors which are competitors of Supplier.

(c) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

7. Subcontractors (further processors on behalf of Company)

(a) Supplier shall use subcontractors (further processors) on behalf of Company only where approved in advance by Company.

(b) Supplier shall use subcontractors listed in Annex 2 ("Sub-Processors").

(c) Supplier shall ensure that all subcontractors provide a level of data protection equivalent to that required under this Agreement and the GDPR.

(d) If Supplier intends to engage additional subcontractors, Supplier shall notify Company in writing at least 30 days in advance. Company may object for justified reasons within that period. If no reasonable alternative exists, Customer's sole remedy is termination.

8. Obligations to inform, mandatory written form, choice of law

(a) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the GDPR.

(b) No modification of this Agreement and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(c) In case of any conflict, the data protection regulations of this Agreement shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this Agreement shall not be affected.

(d) Customer-specific security questionnaires, procurement reviews, compliance assessments, legal reviews and meetings beyond SurveyEngine's standard documentation may be treated as additional professional services.

(e) This Agreement is subject to the laws of Germany.

9. Liability and damages

(a) Company and Supplier shall be liable to data subject in accordance with Article 82 of the GDPR.

Annex 1
Technical and organizational measures of the contractor (TOMs)

The Contractor shall take the following technical and organizational measures for data security within the meaning of Art. 32 DS-GVO:

1. Confidentiality

1.1 Physical access control

Services are hosted on Google Cloud Platform. Physical security controls are provided by Google Cloud Platform in accordance with its published security and compliance programmes. Standard subscriptions are hosted within the Frankfurt (Germany) region.

1.2 Online access control

How are permissions granted to access data or systems?

Access is restricted through role-based permissions. Customer users may access only their own account data. Administrative access is restricted to authorised personnel.

The customer's access authorization to self-managed accounts (SaaS) is granted automatically when the account is created by the customer (SaaS sign-up).

SurveyEngine personnel may access customer systems only where required for support, operational maintenance, security monitoring, incident response, quality assurance, fraud detection, or at the customer's request. Such access is restricted to authorised personnel and is subject to authentication, logging and access control procedures.

Is the granting and revocation of authorizations logged? Who has access to the logs?

Authorised personnel.

What IT System is is used for data management?

Standard platform subscriptions are hosted within Google Cloud Platform's Frankfurt (Germany) region. Alternative hosting regions may be available under Global Compliance subscriptions.

The system provides comprehensive logging of file accesses, users and permission changes. Administrative access is restricted to authorised personnel with a legitimate operational requirement.

Are granted authorisations periodically reviewed with regard to a further requirement? If yes, how often?

Access rights are reviewed and revoked when no longer required.

Is there a password policy?

Strong authentication controls are enforced. Multi-factor authentication is mandatory. Passwords are protected using Argon2 hashing.

How are IT systems protected against viruses and malware?

Administrative systems are maintained using supported operating systems, security updates and endpoint protection controls.

How are unauthorized third-party accesses to IT systems detected and prevented?

For the SurveyEngine data collection platform hosted by Google Cloud Europe, SSL is used as the default for all browser HTTP traffic, preventing man-in-the-middle attacks. Administrative infrastructure access is restricted through authenticated and logged secure administrative channels.

How is care taken to ensure that only carefully selected and vetted service providers come into contact with personal data?

Subprocessors are assessed through supplier management procedures appropriate to the services provided.

2. Technical access control

How is it ensured that permissions are differentiated?

Access rights are granted according to role-based permissions and reviewed periodically. Administrative access is restricted to authorised personnel with a legitimate operational requirement.

3. Separation

How is it ensured that data processed for different purposes are processed separately?

Customer survey content and response data are maintained in customer-specific databases. Access controls prevent customers from accessing data belonging to other customers.

4. Pseudonymisation & Encryption

Is pseudonymization or encryption of data used? If yes, please describe this as specifically as possible.

SurveyEngine supports pseudonymisation, encryption and IP anonymisation controls where required by the customer.

5. Input control

How do you ensure that it can be determined at any time who has entered, changed or deleted personal data and how?

Data collected on data collection servers cannot be changed by respondents or users after the respondent has completed their survey.

Administrative actions affecting customer data are logged and auditable.

How long do you store evidence of these entries, changes and deletions ("logs")?

Logs are retained in accordance with operational, legal and security requirements.

Who has access to these logs?

Only people with administrator rights.

6. Transfer control

How is personal data transferred between the client and the contractor?

Data is transferred through encrypted network connections using industry-standard transport encryption.

7. Deletion

How is it ensured that data is securely deleted after the job is completed?

Customer data is retained and deleted in accordance with the applicable retention policy and customer actions performed through the Services.

Accounts administered by the customer must independently ensure that the deletion of the data is initiated by deleting the projects in their account.

How is the deletion documented?

Selected metadata is stored in the company records as customer name, date and project synopsis. Server-side deletion is documented in the access logs.

8. Availability and resilience

Services are hosted on Google Cloud Platform and benefit from the physical, environmental and infrastructure controls provided by Google. Customer data is backed up regularly and backups are encrypted.

As per Google Cloud guidelines.

Certifications (including ISO 27001): https://cloud.google.com/security/compliance/

Please describe your data backup and recovery process.

There are 2 schemes used for backups of the data collection servers.

a) Daily backup of the entire disk image and

b) Backup of the file system folders.

Where are backups stored?

On a separate server in a physically separate data center in the same jurisdiction (e.g. DE server receive DE backup server).

Are data backups encrypted?

Yes.

Is there a contingency plan?

Yes.

How is rapid data recovery ensured?

For the data acquisition software, file system backups (see above) allow quick recovery or restoration of a working server and data within at least 2 hours.

9. Procedures for regular review, assessment and evaluation

Has the company management taken responsibility for data protection and information security ("guideline")?

Yes.

Has a data protection officer been appointed?

Yes.

What measures are taken to implement data protection through technology design and through data protection-friendly default settings (Art. 25 GDPR)?

The DS-GVO have been incorporated into the corporate guidelines for system design and are already taken into account in the requirements analysis in order to consider minimal data collection and appropriate anonymization / pseudonymization and encryption. In the design of the user UI, default settings are set in favor of the more restrictive storage in each case.

How is it ensured that data breaches are detected and reported immediately?

Unusual activity on the application servers is monitored and administrators are notified. We also rely on the detection and reporting procedures of our IT system provider: Google.

Is there a process for conducting data protection impact assessments (DPIAs)?

Yes.

How is it ensured that requests from affected parties are processed in a timely manner?

Requests are forwarded to the support system, assigned a ticket noting the status of deletion, and agents are required by company policy to prioritize these requests highly and process them by the deadline; when tickets approach the deadline, they are also escalated to the next level.

Is there a register of processing activities within the meaning of Article 30 (1) and (2) of the GDPR?

Yes

What other measures have been taken to ensure the implementation of the requirements of the GDPR in the company?

In accordance with the GDPR / company privacy policy

http://surveyengine.com/gdpr.html

http://surveyengine.com/privacy.html

Has a data protection management system (DSMS) been implemented?

Yes

Annex 2
Subprocessors

The current Subprocessor List is maintained at https://surveyengine.com/compliance and incorporated by reference into this DPA.

Annex 3
Persons authorised to receive instructions from the Company

The recipients of instructions at the Contractor are:

SurveyEngine Support Team

support@surveyengine.com