Agreement for Data Processing

in according to Article 28 General Data Protection Regulation (GDPR)

between

easyfeedback GmbH

Ernst-Abbe-Straße 4

56070 Koblenz, Germany

= the Processor

and

_____

_____

_____

_____

_____

= the Controller

Preamble

The Controller commissions the Supplier with the collection, processing and/or use of personal data (hereinafter: Supplier Data) by supplying survey software for conducting online surveys. In order to specify the rights and duties arising from the order or contract pursuant to the statutory obligations the parties conclude the following agreement:

Insofar as the Supplier has access to personal data and other confidential information or operating secrets of the Controller within the scope of its aforesaid activities in the Controller's company, it and its members of staff employed must treat this data and information in strict confidence.

Personal data are data of any kind on an identified or identifiable natural person, irrespective of whether an employee, a customer or a supplier. Data without direct relevance to personal details (e.g. without a name being given) can be personal data, if the identity of the associated person can be deduced (e.g. staff number, PC user ID, vehicle registration).

Confidential information within the meaning of this statement is all oral or written information, data, documents, materials and details, which the Supplier receives directly or indirectly from the Controller for the purpose of implementing the order or contract or into which it gains insight during its activities. This applies in particular if these documents, materials or information are marked as confidential or their confidential nature arises from their subject-matter or other circumstances.

The following data protection and data security provisions therefore apply to all of the Supplier's services performed for the Controller and to all activities, during which the Supplier's employees or third parties commissioned by the Supplier may come into contact with the Controller's personal data.

§ 1 Subject matter and duration of the Order or Contract

(1) The subject-matter of use arises from the services ordered by the Controller and is laid down in Annex 1 to this agreement: Specification of Order or Contract.

(2) The term of this agreement comes into force on the signature of both parties. It ends with the termination of the collection, processing and/or use of the Controller's data, unless more extensive obligations of the Supplier arise from the provisions of this agreement.

§ 2 Specification of the Order or Contract Details

(1) Nature and purpose of the anticipated processing of data: a more detailed specification of the object of the order or contract with respect to the nature and purpose of the Suppliers tasks is provided in Annex 1.
The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

(2) Type of Data
The Subject Matter of the processing of personal data comprises the following data types/categories:

- ☐ Address data
- ☐ Contact data
- ☐ Contractual information
- ☐ Bank information
- ☐ Account data
- ☐ Invoice data
- ☐ Performance data
- ☐ Financial data
- ☐ Offer data
- ☐ Call history
- ☐ Transaction data
- ☐ Information
- ☐ Employee data
- ☐ Personal management
- ☐ Qualification data
- ☐ Video recordings
- ☐ Health information

☐ Other:

(3) Categories of Data Subjects
The Categories of Data Subjects comprise:

- ☐ Employees
- ☐ Retirees
- ☐ Trainees
- ☐ Trainees
- ☐ Former employees
- ☐ Applicants
- ☐ Dependents
- ☐ Relatives
- ☐ Clients
- ☐ Potential customers
- ☐ Suppliers/Service providers
- ☐ Consultants
- ☐ Brokers
- ☐ Intermediaries
- ☐ Tenants
- ☐ Shareholders
- ☐ Injured parties
- ☐ Witnesses
- ☐ Contacts
- ☐ Press representatives

☐ Other:

§ 3 Technical and Organizational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organizational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/ audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix 2]

(3) The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

§ 4 Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

§ 5 Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. The Supplier has appointed Mr. René Rautenberg as Data Protection Officer:

ER Secure GmbH
Mr. René Rautenberg
CEO

In der Knackenau 4
82031 Grünwald

Datenschutzkoordinator & Ansprechpartner
Dennis Wegner, CEO
E-mail: privacy@easy-feedback.com

The Client shall be informed immediately of any change of Data Protection Officer.

b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organizational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 2].

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

h) Verifiability of the Technical and Organizational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

§ 6 Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company, legal form	Address	Description of type and scope of commissioning
Strato AG Berlin	Pascalstraße 10 10587 Berlin	Data Center: Data storage and processing
Zeusware GmbH	Fähenweg 5 12527 Berlin	Server management: Care and maintenance of the easyfeedback server

Changing the existing subcontractor are permissible when
a) The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and

b) The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and

c) The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

§ 7 Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

☐ Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;

☐ Certification according to an approved certification procedure in accordance with Article 42 GDPR;

☒ Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor);

☐ A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

§ 8 Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a personal data breach immediately to the Client.

c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.

d) Supporting the Client with its data protection impact assessment.

e) Supporting the Client with regard to prior consultation of the supervisory authority.

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

§ 9 Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

§ 10 Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

§ 11 Special security guidelines

The following terms shall apply during processing if:

- Service Provider access to the premises of the Client is necessary
- The Client's systems are to be used
- Access to the internal network of the Client is required (e.g. remote maintenance)

1. In the buildings and on the site of the Client, the Service Provider shall be subject to the control mechanisms of the Service Provider (access control).

2. For the duration of the necessary measures, the Client may remove encryption/access protection to establish connection, if necessary.

3. IT services provided outside of the Client's monitoring shall be recorded by the Service Provider. The records are to be kept for 2 years for the purposes of control and provided upon request.

4. The Service Provider shall not be permitted to connect IT devices, which have not been provided by the Client, to the Client's internal networks or telecommunication facilities without having been granted permission.

_____ , Date _____

_____

Signature, Position held in the Client's company

_____ , Date _____

_____

Signature, Position held in the Service Provider's company

Appendix 1: Specification of order processing
Appendix 2: Technical and Organizational Measures

Appendix 1: Specification of order processing

The supplier provide on his website www.easy-feedback.de and www.easy-feedback.com an online-based survey software (Software as a Service) to conduct and evaluate online surveys.

The client can choose between different services (licenses), which differ in the number of surveys, functions and duration. The services of the survey license are defined on the easyfeedback website.

The duration of each services and agreement ends with the cancelation automatically. Cancelation of the service can be done monthly or annually, depending on the chosen billing period.

Supplement for § 2 Scope, type, and purpose of data processing

The client uses the suppliers survey software in the following scope and for the purpose of feedback management:

1. Create and conduct surveys
2. Invite people to participate
3. Evaluate and download survey results

Appendix 2: Technical and Organizational Measures

Control goals and description of the technical and/or organizational security measures at the data center of Strato AG, hereinafter referred to as „**Data Center**“ , and easyfeedback GmbH, hereinafter referred to as „**easyfeedback**“.

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

Control Objectives with respect to the handling of personal data	**Measures**
1. Physical Access Control (Rooms and buildings) Objective: No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems	**Data Center:** - Determination of security areas - Implementation of effective access control - Determination of authorized personnel - Recording of entries - Management and documentation of personal access authorizations for the entire life cycle - Escorting of visitors and external staff - Monitoring of rooms outside of business hours **easyfeedback:** - Guidelines for escorting and identifying guests in the building - Access management for external staff - Documentation of key assignment by name
2. Electronic Access Control (IT Systems, applications) Objective: No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media	**Data Center:** - Determination of protection requirements - Determination of authorized individuals - Access control (authentication) - Implementation of secure access procedures, high authentication or low authentication depending on security needs - Access records - Secured transmission of authentication credentials in the network - Management and documentation of personal authentication media and access authorization - Automatic or manual access block - Implementation of data encryption in laptops **easyfeedback:** - Assignment of user rights - Authentication with username / password - Password strength: at least 8 characters, at least 1 capitalized letter, at least 1 special character, at least 1 number - Passwords must be updated every 90 days - Log files are used for recording - Always up-to-date secure cryptographic procedures (SSL, TLS with SHA246 Hash AES-GCM) - Locked screen with password authentication

3. Internal Access Control (permissions for user rights of access to and amendment of data) Objective: Internal Access Control (permissions for user rights of access to and amendment of data). No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events	**Data Center:** - Authorization concepts - Implementation of access limitations - Allocation of minimum authorizations - Management and documentation of personal access authorizations - Prevention of function concentration **easyfeedback:** - Authorization concept with differentiated authorizations - Always up-to-date secure cryptographic procedures (SSL, TLS with SHA246 Hash AES-GCM) - Administration of rights by system administrator - Number of administrators reduced to the "most necessary" - Password policy incl. Password length, password change - Use of shredders - Directive / prohibition on the private use of external data carriers All authorized persons shall be able to access only data relevant to them and must be trained in and comply with data protection laws and regulations according to the GDPR.
4. Isolation Control (Purpose-driven) Objective: The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;	**Data Center:** - Establishment of guidelines and work instruction - Establishment of procedural documentation - Implementation of programming regulation - Regulation of system and program checks - Implementation of a poll and control system **easyfeedback:** - Logical separation of datasets - Internal multi-client capability - Creation of an authorization concept - Separated testing and production environment

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

Control Objectives with respect to the handling of personal data	Measures
5. Data Transfer Control (Data) Objective: No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;	**Data Center:** - Determination of persons/entities authorized to receive/ transfer - Verification of legality for international transfers - Safe data transfer between server and client - Minimized risk by means of separate networks - Implementation of security gateways at points of interconnection - Strengthening of backend systems - Description of all interfaces and transferred personal data fields - Implementation of machine-machine authentication - Safe storage of data, including backups - Process for collection and disposal - Introduction of data protection compliant deletion and destruction processes - Maintenance of deletion records **easyfeedback:** - SSL encryption SHA256 (SSL 3.0 fallback deactivated) of the data transfer to storage media - Directive / prohibition on the private use of external data carriers - Training of parties involved in compliance with data protection laws

6. Data Entry Control (Data processing systems) Objective: Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management	**Data Center:** - Input recording - Documentation of input authorizations **easyfeedback:** - Records are created using log files - Traceability of input, modification and deletion of data by individual user names (not user groups) - Assignment of rights to enter, change and delete data based on an authorization concept - SSL SHA256 (SSL 3.0 fallback deactivated) secured - storage of log files

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

Control Objectives with respect to the handling of personal data	Measures
7. Availability Control (Data) Objective: Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning	**Data Center:** - Establishment and implementation of a concept for conducting regular data backups - Establishment and regular maintenance of emergency generators and surge protectors - Monitoring of operating parameters for data centers - Emergency planning - Provisions for the adoption of crisis and emergency management **easyfeedback:** - Daily backup retroactively activated for 14 days - Emergency plan, Master Recovery - Fire detector - Firewall/virus protection - Redundant computer services

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

Control Objectives with respect to the handling of personal data	Measures
8. Order or Contract Control Objective: No third party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.	**Data Center:** - Conclusion of contract on order data processing - Recording of contract implementation on the part of Service Provider **easyfeedback:** - Selection of the order processor under due diligence (in particular with regard to data security) - Written instructions to the processor (for example, by order processing contract) - Obligation of the employees of the processor to data secrecy according to §53 Federal Data Protection Act - Ongoing inspection of the processor and his activities - Proof of a data protection management system according to GDPR

Additional Procedure for order control:

- **Data Protection Management >** ER Secure Management System
- **Incident-Response-Management >** Master Recovery Plan
- **Data Protection by Design and Default (Article 25 Paragraph 2 GDPR) >** Authorization concept, possibility of data portability, deletion of data, protolling of input, modification, deletion of data