02/2025

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 categories of personal data as defined by the client when creating the surveys in the specific case:

☐ 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	☐ Personnel management	☐ Qualification data
☐ Video recordings	☐ Health information	

3) Categories of Data Subjects
The categories of data subjects defined by the client when creating the surveys in the specific case:

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

§ 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:

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

heyData GmbH
Schützenstraße 5
10117 Berlin

www.heydata.eu
datenschutz@heydata.eu

Data protection coordinator & contact person
Dennis Wegner, CEO
E-mail: privacy@easy-feedback.com

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

2) 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.

3) The processor undertakes to treat confidentially the documents and data made available or developed within the scope of the contractual relationship as well as any other information made known to him and to use them only within the scope of the activity for this contractual relationship. This obligation shall continue to exist after the end of the contractual relationship.

4) 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].

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

6) 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.

7) 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.

8) 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.

9) Traceability of technical and organizational measures against the persons responsible as part of its supervisory powers under paragraph 7 of this contract.

§ 6 Subcontracting

1) The processor is not entitled to involve subcontractors in the collection, processing or use of personal data of the person responsible without the prior written consent of the person responsible. The processor will immediately inform the controller about the intended assignment of a subcontractor. If the responsible person does not reject a subcontracting in writing (including by e-mail) within a period of 14 days after receipt of the notification, the consent to subcontracting is deemed to have been given.

2) Subcontracting relationships within the meaning of this provision are understood to be those services which are directly related to the provision of the main service. This does not include ancillary services which the Contractor uses e.g. as telecommunications services, postal/transport services or maintenance and user service or other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, in order to guarantee the data protection and data security of the data controller, the processor is obliged to take appropriate and legally compliant contractual agreements as well as control measures in order to guarantee the data protection and data security of the data controller even in the case of outsourced ancillary services.

3) The person responsible agrees to the assignment of the subsequent subcontractors under 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
Cronon GmbH	Otto-Ostrowski-Straße 7 10249 Berlin	Data Center: Data storage and processing
The following service providerssci-an GmbH are only used when using the separate “Chat surveys” and “AI analysis in the Result STUDIO” and are optional:		
sci-an GmbH	Bergheimer Straße 104 D-69115 Heidelberg	Providing the “chat survey” technology including analysis of the results using the AI language model “OpenAI” (following)

OpenAI OpCo, LLC	1960 Bryant Street, San Francisco, CA 94110	Providing ar cial intelligence to analyze data: The language model of the company “OpenAI” in the professional version is used to analyze the survey results. All data supplied to OpenAI are not used for training purposes and are automatically deleted a er 30 days. The data are only stored for 30 days for billing purposes. Each data set transmitted stands alone and cannot be linked to other data/ participations. The following data will be transmitted for the AI analysis - Question title, answer options - Percentage of the selected answer option - Frequency distribution of the selected answers - ø values - Free text answers The data always sent anonymously to the OpenAI. A personal reference to a participant, the sender of the survey or the company is not possible. If a participant enters a name in a free text response, this will be transmitted - unless you anonymize the free text response before transmission.

Outsourcing to sub-processors or changing existing sub-processors is permitted, provided that a contractual agreement in accordance with Art. 28 Paragraph 2-4 GDPR is used.

4) 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.

5) 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.

6) 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 controller may verify the technical and organizational measures of the processor before commencing data processing and then annually. For this purpose, he may, for example, obtain information from the processor, have existing certificates from experts, certifications or internal audits presented to him or personally check the technical and organizational measures of the processor after timely consultation during normal business hours or have them checked by a competent third party, provided that the latter is not in a competitive relationship with the processor. The controller shall only carry out checks to the extent necessary and shall not disproportionately disrupt the processor's operations.

2) The processor undertakes to provide the controller with all information and evidence necessary to carry out a check of the technical and organizational measures of the processor within a reasonable period of time upon the controller's oral or written request.

3) The controller shall document the result of the check and inform the processor of it. In the event of errors or irregularities that the controller discovers, in particular during the review of order results, the controller shall inform the processor immediately. If circumstances are identified during the inspection that require changes to be made to the prescribed procedure in order to prevent them in the future, the controller shall inform the processor of the necessary procedural changes without delay.

§ 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 can claim compensation for additional support services that are not included in the service description or are not due to misconduct on the part of the Supplier. In such a case, the Supplier will inform the person responsible about the costs incurred.

§ 9 Authority of the Client to issue instructions

1) The processor may not process the data that is processed in the order without authorization, but only according to documented instructions from the person responsible. The person responsible alone decides on the purposes and means of processing the personal data. Processing for other purposes, especially for the processor's own purposes, is not permitted.

2) Verbal instructions are confirmed by the responsible person without delay (at least in text form).

3) The processor must immediately inform the responsible person if he believes that an instruction violates data protection regulations. The processor is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the person responsible.

§ 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 backup 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 dataprotection 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 Requests from affected persons

If a person concerned contacts the processor with requests for correction, deletion or information, the processor will refer the person concerned to the person responsible, provided that an assignment to the person responsible is possible according to the information provided by the person concerned. The processor informs the person responsible and forwards the request of the data subject immediately. He continues to support the person responsible in fulfilling his obligations according to Chapter III GDPR to the extent required.

§ 12 Liability and Compensation

The person responsible and the processor are liable to data subjects in accordance with the provisions of Art. 82 GDPR.

§ 13 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

Koblenz, Germany , Date: _____

_____

Signature, Position held in the Service Provider’s company

Appendix 1: Specification of order processing

Appendix 2: Technical and Organizational Measures

Appendix 3: Confidentiality Agreement (NDA)

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, online questionnaires, forms or information content
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 Cronon GmbH, 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 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:** - Reception and security service - Individual, documented and role-dependent access authorizations (cards, transponders and keys) - Employee and visitor passes - Visitors are only allowed in the building when accompanied by an employee - Alarm and burglar alarm system - Office rooms are locked outside working 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:** - Formal user and authorization procedures - Login only with user name, password and where required 2-factor authentication - Systemically enforced password policies - VPN for remote access and through devices managed by the responsible person - Mobile device management - Mobile data carriers are encrypted - Automatic locking of desktops after a few minutes of inactivity - Clean desk policy **easyfeedback:** - Assignment of user rights - Authentication with username / password - Password policy incl. Password length, password change - Log files are used for recording - Always up-to-date secure cryptographic procedures (SSL, TLS with SHA256 Hash AES-GCM) - Cryptographic Measures Policy - 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:** - Maintaining asset registers and deriving measures on the basis of data classification - Use of cryptographic procedures (e.g., encryption) - Implementation of authorization concepts according to the need-to-know principle - Separation of application and administration accesses - Logging of access attempts - Establishment of administrator workstations - Minimum number of administrators - Use of document destruction **easyfeedback:** - Authorization concept with differentiated authorizations - Always up-to-date secure cryptographic procedures (SSL, TLS with SHA256 Hash AES-GCM) - Cryptographic Measures Policy - AES-256 encryption for data at rest - Administration of rights by system administrator - Number of administrators reduced to the "most necessary" (need to know) - Password policy incl. Password length, password change - Use of shredders security level 5 - 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:** - Separation of development, test and productive environment - Personal data must not be used for test purposes - Multi-client capability / logical separation of data for relevant applications: Separate databases, schema separation in databases, authorization concepts and/or structured file storage. **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 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:** - Provision of data via encrypted connections (e.g. SFTP) - Transfer of personal data in line with the need-to-know / need-to-do principle - Personal data is classified according to its need for protection, with confidential data only being transferred via secure communication channels. - E-mail encryption is used wherever possible - Where possible, personal data is transmitted only in pseudonymized or anonymized form - Documentation of the transfer of physical storage media - Transfer of paper documents containing personal data in a sealed opaque envelope **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:** - Technical logging of the entry, modification and deletion of personal data as well as control of the logs - Traceability of input, modification and deletion of data through individual user names (not user groups) - Role-based authorization concept (read, write, and delete rights) - Logging of administrative changes **easyfeedback:** - Logging of the entry, modification, and deletion of data - 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 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:** - Use of hardware and software firewalls - Intrusion detection systems - Overvoltage protection of the building exterior against lightning strikes - Uninterruptible power supply (UPS) - Emergency manuals for data recovery, protection against accidental destruction and loss - Performance of recovery tests - Use of redundant systems (e.g. RAID) where necessary - Regular testing of data backups - External audits and security tests **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 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

- Data protection officers and an information security officer have been appointed
- Establishment of a data protection and information security organization
- All employees are obligated to maintain confidentiality when handling personal data and are made aware of the telecommunications secrecy obligation
- Employees are sensitized to the handling of personal data
- New employees receive information material regarding the handling of personal data
- A register of processing activities is maintained and data protection impact assessments are carried out as required
- Processes for exercising data subject rights are established

Order control

- Data that is processed on behalf of the customer is only processed in accordance with the customer's instructions.
- Contractors are carefully selected with regard to technical and organizational measures taken to protect personal data
- Instructions on the handling of personal data are documented in text form.
- Where necessary, order processing agreements or suitable guarantees for the transfer of data to third countries are concluded.

Privacy-friendly default settings

- Processes are in place to ensure that systems and products are developed in a data protection-friendly manner
- Only those personal data are collected that are required for the respective purpose

Incident-Response-Management

- Documented process for detecting, reporting and documenting data security breaches with the involvement of the data security officer
- Documented process for handling security incidents with the involvement of the information security officer

Appendix 3: Confidentiality Agreement (NDA)

In order to maintain confidentiality and to safeguard or protect important information marked as confidential (hereinafter collectively referred to as "Confidential Information"), the Controller and the Processor - together hereinafter referred to as the "Party" or the "Parties" - agree on the following agreement:

1. Definitions

"**Third Parties**" shall mean Affiliates of a Party and Consultants acting on behalf of a Party or its Affiliates.

"**Affiliated Companies**" of a Party shall mean affiliated companies pursuant to Section 15 of the German Stock Corporation Act.

"**Confidential Information**" means.

1.1) All documents, specifications, designs, plans, drawings, software materials, data, samples or prototypes in written, oral or electronically recorded form, as well as

1.2) Intangible information such as business idea or concepts disclosed by a Party in connection with the discussions referred to above; and

1.3) The fact that the Parties will hold discussions.

The duty of confidentiality shall apply regardless of whether or not the information in question has been expressly marked as confidential by the disclosing party

2. Secrecy

Each party undertakes to use all confidential information received

2.1) to use it exclusively for the purpose stated in the Preamble

2.2) to make the Confidential Information available only to those of its employees and employees of third parties who need the Confidential Information for the intended purpose, provided that such employees and the respective third parties are obligated in writing to treat the Confidential Information in a manner at least equivalent to this Agreement; and

2.3) to maintain secrecy and to exercise the same degree of care as with respect to its own information and data of similar importance, but at least a reasonable degree of care.

3. Exceptions

The obligations contained in Section 2 of this Agreement shall not apply to Confidential Information that

3.1) was already lawfully known to the Receiving Party prior to its disclosure without an obligation of confidentiality

3.2) is or becomes publicly available through no fault of the receiving party or the third parties to whom the confidential information was made available by the receiving party

3.3) is lawfully made available to the Receiving Party by a third party without any obligation of confidentiality, provided that the third party - to the knowledge of the Receiving Party - does not breach any obligation of confidentiality of its own when making the information available

3.4) has been independently developed by the receiving party or

3.5) have been released in writing by the transferring party.

The burden of proof for the existence of the above exceptions shall be borne by the party invoking them. The Receiving Party may disclose Confidential Information of the Transferring Party to the extent the Receiving Party is obligated to do so due to an official or judicial order or mandatory legal provisions, provided that the Receiving Party immediately notifies the Transferring Party thereof in writing for the purpose of exercising its rights and that the Receiving Party does what it can reasonably be expected to do to ensure that the Confidential Information is kept confidential.

4. Exclusion of Rights & Liability

4.1) No licenses or other rights of any kind whatsoever shall be granted by this Agreement, nor shall any corresponding obligation to grant such rights arise herefrom. The receiving party shall not be entitled to apply for patents or other statutory property rights with the confidential information. The provision of the Confidential Information shall not give rise to any rights of prior use for the Receiving Party.

4.2) The confidential information shall be made available free of charge. Any warranty or liability with regard to the correctness, freedom from errors, freedom from property rights of third parties, completeness and/or usability of the confidential information shall be excluded to the extent permitted by law.

4.3) For the unauthorized disclosure or disclosure of Confidential Information by a third party to whom the Receiving Party has made Confidential Information available, the Receiving Party shall be liable to the Transferring Party as if it were the Receiving Party's own acts or omissions.

5. Term & Return

5.1) This Agreement shall expire 5 years after the termination of the Main Agreement and the collection and processing of Data via the Processor. However, the obligations arising from this Agreement shall continue for each party for a period of 4 years after the end of this Agreement.

5.2) Confidential Information received shall be returned or destroyed at the request of the transferring Party at the option of the receiving Party. This does not apply to routinely made backup copies of electronic data traffic and copies that are subject to a more extensive retention obligation under mandatory law, provided that such Confidential Information is kept secret by the Receiving Party and third parties for an unlimited period of time in accordance with the provision of this Agreement. The fulfillment of the obligations under this Section 5.2 shall be confirmed in writing to the Transferring Party upon request.

6. Final Provisions

6.1) German law shall apply exclusively to all disputes arising from or based on this agreement. The exclusive place of jurisdiction is the registered office of easyfeedback GmbH in Koblenz.

6.2) This agreement does not preclude any changes in the type and number of employees of the party receiving the information.

6.3) This agreement does not establish a partnership or a joint venture between the parties.

6.4) Neither party may transfer this Agreement or any rights or obligations under this Agreement to any third party without the written consent of the other party.

6.5) Amendments and supplements to this Agreement must be made in writing. This written form requirement may only be waived in writing.

6.6) If any provision of this confidentiality agreement becomes invalid or unenforceable, this shall not affect the validity of the remaining provisions. The same shall apply if the confidentiality agreement contains a loophole. Instead of the invalid or unenforceable provision, an appropriate provision shall be made in accordance with the purpose of the agreement and the economic interests of the parties. A loophole can only be replaced by a provision which the parties would have made if they had known and considered this loophole from the outset.