Data Processing Agreement

between

as Controller (hereinafter "**Controller**"),

and

Varify Sofware GmbH, Südliche Münchner Straße 55, 82031 Grünwald, Germany

as Data Processor (hereinafter „**Data Processor**",

Controller and Data Processor jointly the "**Parties**")

Preamble

The controller has commissioned the data processing company in the general terms and conditions (hereinafter "main contract") for the services specified therein. Part of the execution of the contract is the processing of personal data. Art. 28 GDPR in particular places certain requirements on such data processing. In order to comply with these requirements, the following agreement on data processing (hereinafter "Agreement") is part of the main contract, the fulfillment of which is not remunerated separately, unless this is expressly agreed.

§ 1 Definitions

(1) Pursuant to Art. 4 (7) GDPR, the Controller is the entity that alone or jointly with other Controllers determines the purposes and means of the processing of personal data.

(2) Pursuant to Art. 4 (8) GDPR, a Data Processor is a natural or legal person, authority, institution, or other body that processes personal data on behalf of the Controller.

(3) Pursuant to Art. 4 (1) GDPR, personal data means any information relating to an identified or identifiable natural person (hereinafter "**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Personal data requiring special protection are personal data pursuant to Art. 9 GDPR revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of Data Subjects, personal data pursuant to Art. 10 GDPR on criminal convictions and criminal offenses or related security measures, as well as genetic data pursuant to Art. 4 (13) GDPR, biometric data pursuant to Art. 4 (14) GDPR, health data pursuant to Art. 4 (15) GDPR, and data on the sex life or sexual orientation of a natural person.

(5) According to Article 4 (2) GDPR, the processing is any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(6) Pursuant to Article 4 (21) GDPR, the supervisory authority is an independent state body established by a Member State pursuant to Article 51 GDPR.

§ 2 Subject of the contract

(1) The Data Processor provides the services specified in the Main Contract for the Controller. In doing so, the Data Processor obtains access to personal data, which the Data Processor processes for the Controller exclusively on behalf of and in accordance with the Controller's instructions. Further details of the data processing by the Data Processor are set out in **Annex 1**, the Main Contract and any associated

service descriptions. The Controller shall be responsible for assessing the admissibility of the data processing.

(2) The Parties conclude the present Agreement to specify the mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Main Contract.

(3) The provisions of this contract shall apply to all activities related to the Main Contract in which the Data Processor and its employees or persons authorized by the Data Processor come into contact with personal data originating from the Controller or collected for the Controller.

(4) The term of this Agreement shall be governed by the term of the Main Contract unless the following provisions give rise to further obligations or termination rights.

§ 3 Right of instruction

(1) The Data Processor may only collect, process or use data within the scope of the Main Contract and in accordance with the instructions of the Controller. If the Data Processor is required to carry out further processing by the law of the European Union or the Member States to which it is subject, it shall notify the Controller of these legal requirements prior to the processing.

(2) The instructions of the Controller shall initially be determined by this Agreement. Thereafter, they may be amended, supplemented, or replaced by the Controller in writing or text form by individual instructions (Individual Instructions). The Controller shall be entitled to issue such instructions at any time. This includes instructions with regard to the correction, deletion, and blocking of data.

(3) All instructions issued shall be documented by the Controller. Instructions that go beyond the service agreed in the Main Contract shall be treated as a request for a change in service.

(4) If the Data Processor is of the opinion that an instruction of the Controller violates data protection provisions, it shall notify the Controller thereof without undue delay. The Data Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller. The Data Processor may refuse to carry out an obviously unlawful instruction.

§ 4 Types of data processed, group of Data Subjects, third country

(1) Within the scope of the implementation of the Main Contract, the Data Processor shall have access to the personal data specified in more detail in **Annex 2**.

(2) The group of Data Subjects affected by the data processing is listed in **Annex 3**.

(3) A transfer of personal data to a third country may take place under the conditions of Art. 44 et seq. GDPR.

(4) The Parties agree that, to the extent personal data is transferred to a third country without an adequacy decision pursuant to Art. 45 GDPR, the Standard Contractual Clauses (Module 2 – Controller to Processor) as set out in the European Commission Implementing Decision (EU) 2021/914 are hereby incorporated by reference and shall apply. In such cases, the Controller is the data exporter and the Data Processor is the data importer. The incorporated clauses form an integral part of this Agreement.

§ 5 Protective measures of the Data Processor

(1) The Data Processor shall be obliged to observe the statutory provisions on data protection and not to disclose information obtained from the Controller's domain to third parties or expose it to their access. Documents and data shall be secured against disclosure to unauthorized persons, taking into account the state of the art.

(2) The data processing company shall design the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. It has taken the technical and organizational measures listed in **Annex 4** for the appropriate protection of the controller's data in accordance with Art. 32 GDPR, which the controller recognizes as appropriate. A level of protection appropriate to the risk to the rights and freedoms of natural persons affected by the processing is ensured for the specific data processing. For this purpose, the protection objectives of Art. 32 para. 1 GDPR, such as confidentiality, integrity and availability of the systems and services as well as their resilience with regard to the type, scope, circumstances and purpose of the processing, are taken into account in such a way that the risk is permanently contained by appropriate technical and organizational measures. The data processing company reserves the right to change the security measures taken, whereby it shall ensure that the contractually agreed level of protection is not undercut.

(3) The persons employed in the data processing by the Data Processor are prohibited from collecting, processing or using personal data without authorization.

The Data Processor shall oblige all persons entrusted by it with the processing and performance of this contract (hereinafter "**Employees**") accordingly (obligation of confidentiality, Art. 28 (3) lit. b GDPR) and shall ensure compliance with this obligation with due care.

(4) The Data Processor has appointed a data protection officer. The Data Processor's data protection officer is heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information obligations of the Data Processor

(1) In the event of disruptions, suspected data protection violations or breaches of contractual obligations of the Data Processor, suspected security-related incidents or other irregularities in the processing of personal data by the Data Processor, by persons employed by it within the scope of the contract or by third parties, the Data Processor shall inform the Controller without undue delay. The same shall apply to audits of the Data Processor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

(a) a description of the nature of the personal data breach, including, to the extent possible, the categories and the number of Data Subjects affected, the categories affected and the number of personal data records affected;

(b) a description of the measures taken or proposed by the Data Processor to address the breach and, where applicable, measures to mitigate its possible adverse effects;

(c) a description of the likely consequences of the personal data breach.

(2) The Data Processor shall immediately take the necessary measures to secure the data and to mitigate any possible adverse consequences for the Data Subjects, inform the Controller thereof and request further instructions.

(3) In addition, the Data Processor shall be obliged to provide the Controller with information at any time insofar as the Controller's data are affected by a breach pursuant to paragraph 1.

(4) The Data Processor shall inform the Controller of any significant changes to the security measures pursuant to Section 5 (2).

§ 7 Control rights of the Controller

(1) The Controller may satisfy itself of the technical and organizational measures of the Data Processor prior to the commencement of data processing and thereafter regularly on a yearly basis. For this purpose, the Controller may, for example, obtain information from the Data Processor, obtain existing certificates from experts, certifications or internal audits or, after timely coordination, personally inspect the technical and organizational measures of the Data Processor during normal business hours or have them inspected by a competent third party, provided that the third party is not in a competitive relationship with the Data Processor. The Controller shall carry out checks only to the extent necessary and shall not disproportionately disrupt the operations of the Data Processor in the process.

(2) The Data Processor undertakes to provide the Controller, upon the latter's verbal or written request and within a reasonable period of time, with all information and evidence required to carry out a check of the technical and organizational measures of the Data Processor.

(3) The Controller shall document the results of the inspection and notify the Data Processor thereof. In the event of errors or irregularities which the Controller discovers, in particular during the inspection of the results of the inspection, the Controller shall inform the Data Processor without undue delay. If facts are found during the control, the future avoidance of which requires changes to the ordered procedure, the Controller shall notify the Data Processor of the necessary procedural changes without delay.

§ 8 Use of service providers

(1) The contractually agreed services shall be performed with the involvement of the service providers named in **Annex 5** (hereinafter "**Sub-processors**"). The Controller grants the Data Processor its general authorization within the meaning of Article 28 (2) s. 1 GDPR to engage additional Sub-processors within the scope of its contractual obligations or to replace Sub-processors already engaged.

(2) The Data Processor shall inform the Controller before any intended change in relation to the involvement or replacement of a Sub-processor. The Controller can object to the intended involvement or replacement of a Sub-processor for an important reason under data protection law.

(3) The objection to the intended involvement or replacement of a Sub-processor must be raised within 2 weeks of receiving the information about the change. If no

objection is raised, the involvement or replacement shall be deemed approved. If there is an important reason under data protection law and an amicable solution is not possible between the Controller and the Processor, the Controller has a special right of termination at the end of the month following the objection.

(4) When engaging Sub-processors, the Data Processor shall oblige them in accordance with the provisions of this Agreement.

(5) A Sub-processor relationship within the meaning of these provisions does not exist if the Data Processor commissions third parties with services that are regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific reference to services provided by the Data Processor to the Controller and guarding services. Maintenance and testing services constitute Sub-processor relationships requiring consent insofar as they are provided for IT systems that are also used in connection with the provision of services for the Controller.

§ 9 Requests and rights of Data Subjects

(1) The Data Processor shall support the Controller with suitable technical and organizational measures in fulfilling the Controller's obligations pursuant to Articles 12-22 and 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as the right of access, correction or deletion with regard to his or her data, directly against the Data Processor, the latter shall not react independently but shall refer the Data Subject to the Controller and await the Controller's instructions.

(3) Where applicable, and to the extent the Data Processor processes personal information of California residents on behalf of the Controller, the Data Processor shall act as a "Service Provider" as defined under §1798.140(v) of the California Consumer Privacy Act (CCPA/CPRA) and shall not sell or share such personal information as defined therein.

§ 10 Liability

(1) In the internal relationship with the Data Processor, the Controller alone shall be liable to the Data Subject for compensation for damage suffered by a Data Subject due to inadmissible or incorrect data processing under data protection laws or use within the scope of the commissioned processing.

(2) The Data Processor shall have unlimited liability for damage insofar as the cause of the damage is based on an intentional or grossly negligent breach of duty by the Data Processor, its legal representative or vicarious agent.

(3) The Data Processor shall only be liable for negligent conduct in the event of a breach of an obligation, the fulfillment of which is a prerequisite for the proper performance of the contract and the observance of which the Controller regularly relies on and may rely on, but limited to the average damage typical for the contract. In all other respects, the liability of the Processor - including for its vicarious agents - shall be excluded.

(4) The limitation of liability pursuant to § 10.3 shall not apply to claims for damages arising from injury to life, body, health or from the assumption of a guarantee.

§ 11 Termination of the Main Contract

(1) After termination of the Main Contract, the Data Processor shall return to the Controller all documents, data and data carriers provided to it or - at the request of the Controller, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete them. This shall also apply to any data backups at the Data Processor. The Data Processor shall on request provide documented proof of the proper deletion of any data.

(2) The Controller shall have the right to control the complete and contractual return or deletion of the data at the Data Processor in an appropriate manner.

(3) The Data Processor shall be obligated to keep confidential the data of which it has become aware in connection with the Main Contract even beyond the end of the Main Contract. The present Agreement shall remain valid beyond the end of the Main Contract as long as the Data Processor has personal data at its disposal which have been forwarded to it by the Controller or which it has collected for the Controller.

§ 12 Final provisions

(1) To the extent that the Data Processor does not expressly perform support actions under this Agreement free of charge, it may charge the Controller a reasonable fee therefore, unless the Data Processor's own actions or omissions have made such support directly necessary.

(2) Amendments and supplements to this Agreement must be made in writing. This shall also apply to any waiver of this formal requirement. The priority of individual contractual agreements shall remain unaffected.

(3) If individual provisions of this Agreement are or become wholly or partially invalid or unenforceable, this shall not affect the validity of the remaining provisions.

(4) This agreement is subject to German law.

(5) In case of conflict between this Agreement and the incorporated Standard Contractual Clauses, the latter shall prevail for the purpose of cross-border data transfers.

Controller

Name:

Position:

Data processor

Name: Steffen Schulz

Position: CEO

Date:

Signatures:

Controller

Data processor

Annex

Annex 1 - Subject matter of the processing

Performance of A/B tests to optimize and improve web services, software, user interfaces or other digital products.

Annex 2 - Description of the data/data categories

- Network data: Source and destination IP addresses, network traffic details
- Log data: Metadata about network events (e.g. requests to websites, applications or APIs), information about visitors or authorized users
- Geolocation data: Derived from IP addresses to direct requests to the nearest server
- Browser and device information: Information used to optimize content based on the user's device and browser

Annex 3 - Description of affected Data Subject/groups of affected Data Subjects

Users of websites and/or mobile apps that use varify.io

Annex 4 - Technical and organizational measures of the Data Processor

1. Introduction

1.1 Data protection officer

Our data protection officer is Martin Bastius through heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, e-mail: datenschutz@heydata.eu.

1.2 Subject of the document

This document summarizes the technical and organizational measures taken by the processor within the meaning of Art. 32 para. 1 GDPR. A level of protection appropriate to the risk to the rights and freedoms of natural persons affected by

the processing is ensured for the specific data processing. To this end, the protection objectives of Art. 32 para. 1 GDPR, such as confidentiality, integrity and availability of the systems and services as well as their resilience with regard to the type, scope, circumstances and purpose of the processing operations are taken into account in such a way that the risk is permanently mitigated by appropriate technical and organizational measures.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1 Entry control

The following implemented measures prevent unauthorized persons from gaining access to the data processing systems:

- Work in the home office: instruction to employees to work in a separate office from their living space if possible
- Manual locking system (e.g. key)
- Key regulation / key book
- Authorization assignment is reduced to a minimum
- Video surveillance of the entrances
- Fencing around the company premises
- Visitors must be accompanied by employees
- Secured entrance gates
- Doors with knob on the outside
- Reception / Reception

- Instruction to employees not to work in publicly accessible areas (e.g. cafés)

2.2 Admission control

The following implemented measures prevent unauthorized persons from gaining access to the data processing systems:

- Cleandesk corporate guideline
- Authentication with user and password
- Regulated authorization management and user administration
- Use of firewalls
- Use of antivirus software
- Virtual client separation
- Automatic screen lock with password activation

2.3 Access control

The following implemented measures ensure that unauthorized persons have no access to personal data:

- Instruction to employees that only absolutely necessary data is to be printed out
- Instruction not to connect external data carriers
- Rules for the administration of user roles
- Regular checking and logging of authorizations

- Encryption of mobile devices and data carriers

2.4 Separation control

The following measures ensure that personal data collected for different purposes is processed separately:

- Internal instruction to anonymize/pseudonymize personal data in the event of disclosure or after expiry of the statutory deletion period, if possible.
- Multi-client capable system
- Creation of an authorization concept
- Providing data records with purpose attributes/data fields
- Separation of development, test and production systems
- Separation of test and production data

3. Integrity (Art. 32 para. 1 lit. b GDPR)

3.1 Transfer control

It is ensured that personal data cannot be read, copied, changed or removed without authorization during transmission or storage on data carriers and that it is possible to check which persons or bodies have received personal data. The following measures have been implemented to ensure this:

- WLAN encryption (WPA2 with strong password)
- E-mail encryption
- Provision of data via encrypted connections such as SFTP or HTTPS

- Logging of accesses and retrievals

3.2 Input control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Clear responsibilities for deletions
- Logging the entry, modification and deletion of data
- Traceability of data entry, modification and deletion through individual user names (not user groups)
- Assignment of rights to enter, change and delete data on the basis of an authorization concept
- Data processing only takes place on instruction

4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Regular backups
- Backup concept with data backup
- Hard disk mirroring
- Fire protection concept
- Air conditioning systems

- Fire and smoke detection systems
- Hosting (at least of the most important data) with a professional hoster
- Regular checks of the systems for security vulnerabilities
- Monitoring of all relevant servers
- Measures against DDoS attacks
- Patch and vulnerability management

5. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

5.1 Data protection management

The following measures are intended to ensure that the organization meets the basic requirements of data protection law:

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Obligation of employees to maintain data secrecy
- Regular data protection training for employees
- Maintaining an overview of processing activities (Art. 30 GDPR), which is updated regularly
- Monitoring and regular testing of technical and organizational measures
- Annual audits/reviews

- Process for dealing with data subject rights
- Deletion concepts
- Authorization concepts

5.2 Incident response management

The following measures are intended to ensure that reporting processes are triggered in the event of data protection breaches:

- Reporting process for data protection violations in accordance with Art. 4 No. 12 GDPR to the supervisory authorities (Art. 33 GDPR)
- Notification process for data breaches in accordance with Art. 4 No. 12 GDPR to the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches

5.3 Data protection-friendly default settings (Art. 25 para. 2 GDPR)

The following implemented measures take into account the requirements of the principles of "privacy by design" and "privacy by default":

- Training of employees in "privacy by design" and "privacy by default"
- No more personal data is collected than is necessary for the respective purpose.

5.4 Order control

The following measures ensure that personal data can only be processed in accordance with the instructions:

- There are written contracts with sub-processors
- Instructions are clearly regulated
- Data will be deleted after the end of the contract at the latest
- Written instructions to the contractor or instructions in text form (e.g. through a data processing agreement)
- Ensuring the destruction of data after completion of the order, e.g. by requesting corresponding confirmations
- Confirmation from contractors that they commit their own employees to data secrecy (typically in the data processing agreement)
- Sub-processors are carefully selected

Annex 5 – Current Sub-processors

Sub-processor 1:

Name:	Amazon AWS
Address:	Amazon Web Services EMEA Sàrl, Avenue John F. Kennedy 38, 1855 Luxembourg, Luxembourg
Description of the processing:	AWS with the data center in Frankfurt serves as a hosting platform to store and manage the hosted software and its data.
Data categories affected:	Network data: Source and destination IP addresses, network traffic details
Place of processing, in particular third country processing:	Data center Frankfurt

Data protection contractual relationship with the subcontractor:	There is an adequacy decision (the Data Privacy Framework) and the provider is certified accordingly. Standard contractual clauses have been concluded in the event that the decision no longer applies.

Sub-processor 2:

Name:	Cloudflare
Address:	Cloudflare, Inc. 101 Townsend St San Francisco, CA 94107 USA
Description of the processing:	Cloudflare is used to cache server requests in order to improve response times and reduce hosting costs.
Categories of data concerned:	1. IP addresses: This is the most common type of personal data processed in the context of traffic management, security and performance optimization. 2. log data: Metadata about network events, such as requests to websites, applications or APIs. This may include information about visitors or authorized users. 3. geolocation data: Derived from IP addresses to optimize content delivery by directing requests to the nearest Cloudflare server. 4. browser and device information: Used to optimize the delivery of content based on the device and browser used by the user.
Place of processing, in particular third country processing:	Global, depending on the location of the user

Data protection contractual relationship with the subcontractor:	There is an adequacy decision (the Data Privacy Framework) and the provider is certified accordingly. Standard contractual clauses have been concluded in the event that the decision no longer applies.