Data Processing Agreement

between

as Controller (hereinafter "Controller"),

and

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

as Processor (hereinafter "Processor",
Controller and Processor collectively the "Parties")

Preamble

The Controller has engaged the Processor under the general terms and conditions (hereinafter "Main Agreement") for the services specified therein. Part of the contract execution involves the processing of personal data. In particular, Art. 28 GDPR sets out specific requirements for such processing. To comply with these requirements, the following Data Processing Agreement (hereinafter "Agreement") forms part of the Main Agreement, the fulfillment of which is not separately remunerated unless expressly agreed otherwise.

§ 1 Definitions

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

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

(3) Personal data means, pursuant to Art. 4(1) GDPR, 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) Special categories of personal data are personal data pursuant to Art. 9 GDPR revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, personal data pursuant to Art. 10 GDPR relating to criminal convictions and offences, 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 concerning a natural person's sex life or sexual orientation.

(5) Processing means, pursuant to Art. 4(2) GDPR, any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

(6) Supervisory authority means, pursuant to Art. 4(21) GDPR, an independent public authority established by a Member State pursuant to Art. 51 GDPR.

§ 2 Subject Matter

(1) The Processor provides the Controller with the services specified in the Main Agreement. In doing so, the Processor receives access to personal data, which the Processor processes for the Controller exclusively on behalf of and in accordance with the instructions of the Controller. Further information on data processing by the Processor is set out in Annex 1, the Main Agreement, and any associated service descriptions. The Controller is responsible for assessing the lawfulness of the data processing.

(2) To specify the mutual data protection rights and obligations, the Parties enter into this Agreement. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Main Agreement.

(3) The provisions of this Agreement apply to all activities related to the Main Agreement in which the Processor and its employees or agents come into contact with personal data originating from or collected for the Controller.

(4) The term of this Agreement shall be governed by the term of the Main Agreement, unless the following provisions provide for obligations or termination rights that extend beyond this.

(5) The Processor offers the Controller optional AI-powered features. The use of these features is voluntary and requires separate activation by the respective user. Prior to first use, the user is informed that inputs may be transmitted to third-party AI services, and agrees not to enter any personal data. The Processor does not itself transmit any personal data to the services listed under Sub-Processors 3–6 in Annex 5 in the context of the AI features. Responsibility for the content of inputs lies with the Controller or the respective user.

§ 3 Right to Issue Instructions

(1) The Processor may only collect, process, or use data within the scope of the Main Agreement and in accordance with the Controller's instructions. If the Processor is required by EU or Member State law to carry out further processing, it shall inform the Controller of these legal requirements prior to processing.

(2) The Controller's instructions are initially set out in this Agreement and may subsequently be amended, supplemented, or replaced by the Controller in writing or in text form through individual instructions. The Controller is entitled to issue such instructions at any time. This includes instructions regarding the rectification, erasure, and restriction of data.

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

(4) If the Processor considers that an instruction from the Controller violates data protection provisions, it shall immediately notify the Controller. The Processor is entitled to suspend execution of the instruction until it is confirmed or amended by the Controller. The Processor may refuse to execute an obviously unlawful instruction.

§ 4 Types of Data Processed, Categories of Data Subjects, Third Countries

(1) In the course of performing the Main Agreement, the Processor receives access to the personal data specified in more detail in Annex 2.

(2) The categories of data subjects affected by the data processing are set out in Annex 3.

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

(4) The Parties agree that, insofar as 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) pursuant to the European Commission Implementing Decision (EU) 2021/914 are hereby incorporated into this Agreement by reference and shall apply. In such cases, the Controller is the data exporter and the Processor is the data importer. The incorporated clauses are an integral part of this Agreement.

§ 5 Protective Measures of the Processor

(1) The Processor is obliged to comply with the statutory data protection provisions 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 unauthorized access, taking into account the state of the art.

(2) The Processor shall organize its internal operations to meet the specific requirements of data protection. It has implemented the technical and organizational measures listed in Annex 4 for the adequate protection of the Controller's data pursuant to Art. 32 GDPR, which the Controller acknowledges as adequate. An appropriate level of protection is ensured for the specific processing, taking into account the protection objectives of Art. 32(1) GDPR. The Processor reserves the right to modify the security measures implemented, provided that the contractually agreed level of protection is not reduced.

(3) Persons employed in data processing by the Processor are prohibited from collecting, processing, or using personal data without authorization. The Processor shall bind all persons entrusted with the performance of this Agreement to confidentiality (Art. 28(3)(b) GDPR) and ensure compliance with due diligence.

(4) The Processor has appointed a Data Protection Officer. The Data Protection Officer of the Processor is Martin Bastius of heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 6 Information Obligations of the Processor

(1) In the event of disruptions, suspected data protection violations, breaches of contractual obligations, suspected security-relevant incidents, or other irregularities in the processing of personal data, the Processor shall immediately inform the Controller. The same applies to audits of the Processor by a 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, where possible, the categories and approximate number of data subjects affected and the categories and approximate number of personal data records affected;

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

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

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

(3) The Processor is further obliged to provide the Controller with information at any time insofar as the Controller's data is affected by a breach pursuant to paragraph 1.

(4) The Processor shall notify the Controller of material changes to the security measures pursuant to § 5(2).

§ 7 Audit Rights of the Controller

(1) The Controller may satisfy itself of the technical and organizational measures of the Processor before the commencement of data processing and annually thereafter. The Controller may, for example, obtain information from the Processor, have existing certificates from experts, certifications, or internal audits presented, or personally inspect the Processor's technical and organizational measures after timely coordination during normal business hours, or have them inspected by a qualified third party, provided that such third party is not in a competitive relationship with the Processor. The Controller shall carry out inspections only to

the extent necessary and shall not unreasonably disrupt the Processor's business operations.

(2) The Processor undertakes to provide the Controller, upon oral or written request, within a reasonable period, with all information and evidence necessary to carry out an inspection of the Processor's technical and organizational measures.

(3) The Controller shall document the inspection results and communicate them to the Processor. In the event of errors or irregularities discovered during the inspection, the Controller shall immediately inform the Processor. If the inspection reveals circumstances requiring changes to the ordered procedural workflow, the Controller shall immediately communicate the necessary procedural changes to the Processor.

§ 8 Use of Service Providers

(1) The contractually agreed services shall be performed with the involvement of the service providers listed in Annex 5 (hereinafter "Sub-Processors"). The Controller grants the Processor general authorization within the meaning of Art. 28(2) sentence 1 GDPR to engage further Sub-Processors or replace existing ones within the scope of its contractual obligations.

(2) The Processor shall inform the Controller before any intended change regarding the addition or replacement of a Sub-Processor. The Controller may object to an intended addition or replacement of a Sub-Processor for important data protection reasons.

(3) The objection to the intended addition or replacement of a Sub-Processor must be raised within 2 weeks of receipt of the information about the change. If no objection is raised, the addition or replacement shall be deemed approved. If an important data protection reason exists and an amicable resolution between the Controller and the Processor is not possible, the Processor shall have a special right of termination effective at the end of the month following the objection.

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

(5) A sub-processing relationship within the meaning of these provisions does not exist where the Processor engages third parties for services that are to be regarded as purely ancillary services. These include, for example, postal, transport, and shipping services, cleaning services, telecommunications services without specific reference to services provided by the Processor for the Controller, and security services. Maintenance and testing services constitute sub-processing

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 Data Subject Requests and Rights

(1) The Processor shall support the Controller, where possible, with appropriate technical and organizational measures in fulfilling its obligations under Art. 12–22 and Art. 32–36 GDPR.

(2) If a data subject asserts rights, such as the right to information, rectification, or erasure of their data, directly against the Processor, the Processor shall not respond independently but shall refer the data subject to the Controller and await its instructions.

(3) To the extent applicable and insofar as the Processor processes personal data of California residents on behalf of the Controller, the Processor acts as a "service provider" within the meaning of §1798.140(v) of the California Consumer Privacy Act (CCPA/CPRA) and shall not sell or share such personal data as defined therein.

§ 10 Liability

(1) For damages suffered by a data subject due to unlawful or incorrect data processing or use in the context of the processing, the Controller alone shall be responsible to the data subject in the internal relationship with the Processor.

(2) The Processor shall be liable without limitation for damages insofar as the cause of damage is based on an intentional or grossly negligent breach of duty by the Processor, its legal representatives, or vicarious agents.

(3) For negligent conduct, the Processor shall only be liable in case of breach of an obligation whose fulfillment is essential for the proper execution of the Agreement and on whose compliance the Controller regularly relies and may rely, but limited to the typical, foreseeable damage. Otherwise, the liability of the Processor – including for its vicarious agents – is excluded.

(4) The limitation of liability pursuant to § 10(3) shall not apply to claims for damages arising from injury to life, body, or health, or from the assumption of a guarantee.

§ 11 Termination of the Main Agreement

(1) Upon termination of the Main Agreement, the Processor shall return to the Controller all documents, data, and data carriers provided to it, or – at the Controller's request, unless there is an obligation to store the personal data under EU or German law – delete them. This also applies to any data backups held by

the Processor. The Processor shall provide documented proof of proper deletion upon request.

(2) The Controller has the right to verify the complete and contractually compliant return or deletion of data at the Processor in an appropriate manner.

(3) The Processor is obliged to treat any data that has come to its knowledge in connection with the Main Agreement as confidential even beyond the end of the Main Agreement. This Agreement shall remain valid beyond the end of the Main Agreement for as long as the Processor has personal data that was provided by the Controller or collected on its behalf.

§ 12 Final Provisions

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

(2) Amendments and supplements to this Agreement require text form. This also applies to the waiver of this formal requirement. The precedence of individual contractual agreements remains unaffected.

(3) Should individual provisions of this Agreement be or become wholly or partially invalid or unenforceable, the validity of the remaining provisions shall not be affected.

(4) This Agreement is governed by German law.

(5) In the event of a 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:

Processor

Name: Steffen Schulz

Position: CEO

Date:

Signatures:

Controller

Processor

Annexes

Annex 1 – Subject Matter of Data Processing

Conducting A/B tests for the optimization and improvement of web services, software, user interfaces, or other digital products.

Optional: Provision of AI-powered features to support website optimization, the use of which requires separate activation by the user.

Annex 2 – Description of Data / Data Categories

- Network data: source and destination IP addresses, network traffic details
- Log data: metadata on network events (e.g. requests to websites, applications, or APIs), information about visitors or authorized users
- Geolocation data: derived from IP addresses to route 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 Data Subjects / Groups of Data Subjects

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

Annex 4 – Technical and Organizational Measures of the Processor

1. Introduction

1.1. Data Protection Officer

Our Data Protection Officer is Martin Bastius via heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, email: datenschutz@heydata.eu.

1.2. Subject of This Document

This document summarizes the technical and organizational measures taken by the Processor within the meaning of Art. 32(1) GDPR. An appropriate level of protection is ensured for the specific processing, taking into account the risk to the rights and freedoms of natural persons affected by the processing.

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

2.1. Physical Access Control

The following implemented measures prevent unauthorized persons from gaining physical access to data processing facilities:

- Working from home office: instruction to employees to work in separate rooms where possible
- Manual locking system (e.g. keys)
- Key management / key register
- Authorization granted on a need-to-know basis
- Video surveillance of entrances
- Fencing of the premises
- Visitors only accompanied by employees
- Secured entry gates
- Doors with knob on the outside
- Reception / front desk
- Instruction to employees not to work in publicly accessible premises (e.g. cafés)

2.2. System Access Control

The following implemented measures prevent unauthorized access to data processing systems:

- Company-wide “Clean Desk” policy
- Authentication with username and password
- Regulated authorization management and user administration
- Use of firewalls
- Use of antivirus software
- Virtual tenant separation
- Automatic screen lock with password activation

2.3. Data Access Control

The following implemented measures ensure that unauthorized persons cannot access personal data:

- Instruction to employees to print only essential data
- Instruction not to connect external storage devices
- Regulations for the management of user roles
- Regular review and logging of authorizations
- Encryption of mobile devices and storage media

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 where possible when transferring or after expiry of the legal retention period

- Multi-tenant capable system
- Creation of an authorization concept
- Tagging of data records with purpose attributes/data fields
- Separation of development, test, and production systems
- Separation of test and production data

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

3.1. Transfer Control

It is ensured that personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or storage, and that it can be verified which persons or entities have received personal data. The following measures are implemented:

- WLAN encryption (WPA2 with strong password)
- Email encryption
- Provision of data via encrypted connections such as SFTP or HTTPS
- Logging of access and retrieval

3.2. Input Control

The following measures ensure that it can be verified who has processed personal data at what time in data processing facilities:

- Clear responsibilities for deletion
- Logging of data entry, modification, and deletion
- Traceability of data entry, modification, and deletion through individual usernames (not user groups)
- Assignment of rights for data entry, modification, and deletion based on an authorization concept
- Data processing occurs only on instruction

4. Availability and Resilience (Art. 32(1)(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 protection
- Disk mirroring
- Fire protection concept
- Air conditioning systems
- Fire and smoke detection systems
- Hosting (at least of the most important data) with a professional hosting provider

- Regular review of 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(1)(d) GDPR; Art. 25(1) GDPR)

5.1. Data Protection Management

The following measures ensure that an organization meeting the fundamental data protection requirements is in place:

- Use of the heyData platform for data protection management
- Appointment of the heyData Data Protection Officer
- Commitment of employees to data secrecy
- Regular employee training in data protection
- Maintaining a record of processing activities (Art. 30 GDPR), regularly updated
- Control and regular review of technical and organizational measures
- Annual audits/reviews
- Process for handling data subject rights
- Deletion concepts
- Authorization concepts

5.2. Incident Response Management

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

- Reporting process for data protection violations pursuant to Art. 4(12) GDPR to supervisory authorities (Art. 33 GDPR)
- Reporting process for data protection violations pursuant to Art. 4(12) GDPR to data subjects (Art. 34 GDPR)
- Involvement of the Data Protection Officer in security incidents and data breaches

5.3. Privacy by Default (Art. 25(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 instructions:

- Written contracts exist with sub-processors
- Instructions are clearly regulated
- Data is deleted no later than the end of the contract
- Written instructions to the contractor or instructions in text form (e.g. through the data processing agreement)
- Ensuring the destruction of data after completion of the engagement, e.g. by requesting corresponding confirmations
- Confirmation from contractors that they bind 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 Processing:	AWS with its 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
Processing Location:	Data center Frankfurt
Data Protection Contractual Relationship:	An adequacy decision (the Data Privacy Framework) exists and the provider is certified accordingly. In the event that the decision is revoked, Standard Contractual Clauses have been concluded.

Sub-Processor 2:

Name:	Cloudflare
Address:	Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA
Description of Processing:	Cloudflare is used to cache server requests in order to improve response times and reduce hosting costs.
Data Categories Affected:	IP addresses, log data (metadata on network events), geolocation data (derived from IP addresses), browser and device information
Processing Location:	Global, depending on the user's location
Data Protection Contractual Relationship:	An adequacy decision (the Data Privacy Framework) exists and the provider is certified accordingly. In the event that the decision is revoked, Standard Contractual Clauses have been concluded.

Note: Sub-Processors 3–6 listed below are used exclusively when the Processor's optional AI services are activated. If the Controller does not activate or use any AI features, no data processing by these sub-processors shall take place.

Sub-Processor 3 (AI Service):

Name:	Anthropic (Claude)
Address:	Anthropic, PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA
Description of Processing:	Provision of AI-powered language models (Claude) for processing text inputs and generating text outputs as part of the Processor's optional AI features.
Data Categories Affected:	User text inputs (prompts) that may contain personal data; generated text outputs
Processing Location:	USA (Google Cloud / AWS data centers)
Data Protection Contractual Relationship:	Data Processing Addendum (DPA) concluded with Anthropic. Standard Contractual Clauses pursuant to EU 2021/914 agreed. Zero Data Retention (no storage of API inputs for training).

Sub-Processor 4 (AI Service):

Name:	OpenAI (Codex)
Address:	OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
Description of Processing:	Provision of AI-powered language models (Codex) for automated code generation and text processing as part of the Processor's optional AI features.
Data Categories Affected:	User text inputs (prompts) that may contain personal data; generated text outputs
Processing Location:	USA (Microsoft Azure data centers)
Data Protection Contractual Relationship:	Data Processing Addendum (DPA) concluded with OpenAI. An adequacy decision (the Data Privacy Framework) exists and the provider is certified accordingly. Standard Contractual Clauses agreed. Zero Data Retention (no storage of API inputs for training).

Sub-Processor 5 (AI Service):

Name:	Google (Gemini)
Address:	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
Description of Processing:	Provision of AI-powered language models (Gemini) for processing text inputs and generating text outputs as part of the Processor's optional AI features.
Data Categories Affected:	User text inputs (prompts) that may contain personal data; generated text outputs

Processing Location:	EU/EEA (Google Cloud data centers, incl. Ireland, Netherlands, Finland); potentially USA
Data Protection Contractual Relationship:	Google Cloud Data Processing Addendum (DPA) concluded. EU data centers available. For third-country transfers: adequacy decision (Data Privacy Framework) and Standard Contractual Clauses agreed.

Sub-Processor 6:

Name:	Firecrawl (SideGuide Technologies, Inc.)
Address:	SideGuide Technologies, Inc. d/b/a Firecrawl, 800 Haight Street, San Francisco, CA, USA
Description of Processing:	Provision of a web scraping and data extraction API for preparing web content for AI-powered features as part of the Processor's optional AI services. Firecrawl extracts publicly accessible web content and converts it into structured data.
Data Categories Affected:	URLs and web content of publicly accessible websites; personal data potentially contained on these pages (e.g. legal notice data, contact information)
Processing Location:	USA (cloud infrastructure)
Data Protection Contractual Relationship:	Use pursuant to Firecrawl Terms of Service. Only publicly accessible web content is processed. Standard Contractual Clauses for third-country transfers agreed.