Data Processing Agreement

between

as the controller (hereinafter the “Controller”),

and

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

as the processor (hereinafter the “Processor”,
Controller and Processor jointly the “Parties”)

Recitals

The Controller has engaged the Processor under the general terms and conditions (hereinafter the "Main Agreement") for the services set out therein. The performance of the Main Agreement involves the processing of personal data. Art. 28 GDPR in particular sets out certain requirements for such processing on behalf of a controller. In order to meet those requirements, the following Data Processing Agreement (hereinafter the "Agreement") forms part of the Main Agreement; its performance is not remunerated separately unless expressly agreed otherwise.

§ 1 Definitions

(1) Controller means, pursuant to Art. 4(7) GDPR, the body which alone or jointly with other controllers determines the purposes and means of the processing of personal data.

(2) Processor means, pursuant to Art. 4(8) GDPR, a natural or legal person, public authority, agency or other body which 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 the "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 means 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 relating to criminal convictions and offences 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 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 which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, 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 of the Agreement

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

(2) The Parties enter into this Agreement in order to specify their mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement take precedence over the provisions of the Main Agreement.

(3) The provisions of this Agreement apply to all activities connected with the Main Agreement in the course of which the Processor, its employees or persons engaged by the Processor come into contact with personal data originating from the Controller or collected for the Controller.

(4) The term of this Agreement follows the term of the Main Agreement, unless the provisions below give rise to obligations or termination rights extending beyond it.

(5) The Processor offers the Controller optional AI-supported features. Use of these features is voluntary and requires separate activation by the individual user. Before first use, the user is informed that inputs may be transmitted to third-party AI services and agrees not to enter any personal data. Within the AI features, the Processor itself does not transfer any personal data to the services listed in Annex 5 under A5.3 to A5.6. Responsibility for the content of the inputs lies with the Controller or the respective user.

§ 3 Right to Issue Instructions

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

(2) The Controller's instructions are initially laid down in this Agreement and may thereafter be amended, supplemented or replaced by the Controller by way of individual instructions in written or text form (individual instruction). The Controller is entitled to issue such instructions at any time. This includes instructions regarding the rectification, erasure and blocking of data.

(3) All instructions issued must be documented by the Controller. Instructions going beyond the services agreed in the Main Agreement are treated as a request for a change of services.

(4) If the Processor is of the opinion that an instruction of the Controller infringes data protection provisions, it shall inform the Controller thereof without undue delay. The Processor is entitled to suspend performance of the instruction concerned until it is confirmed or amended by the Controller. The Processor may refuse to carry out a manifestly unlawful instruction.

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

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

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

(3) Personal data may be transferred to a third country (outside the EEA) subject to the conditions of Art. 44 et seq. GDPR.

(4) The Parties agree that, to the extent personal data are 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 Implementing Decision (EU) 2021/914 of the European Commission 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 form an integral part of this Agreement.

(5) Transfers of personal data to sub-processors in third countries take place on the basis of an adequacy decision or, where no such decision exists, on the basis of the Standard Contractual Clauses (Module 3 – processor to processor), which the Processor concludes with the respective sub-processor. Details are set out in Annex 5.

§ 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 sphere to third parties or expose it to their access. Documents and data must be secured against access by unauthorised persons, taking into account the state of the art.

(2) Within its area of responsibility, the Processor shall structure its internal organisation in such a way that it meets the specific requirements of data protection. It has implemented the technical and organisational measures set out

in Annex 4 for the adequate protection of the Controller's data pursuant to Art. 32 GDPR, which the Controller acknowledges as adequate. A level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by the processing is ensured for the specific processing. To that end, the protection objectives of Art. 32(1) GDPR – such as confidentiality, integrity and availability of systems and services and their resilience – are taken into account in relation to the nature, scope, circumstances and purpose of the processing in such a way that the risk is permanently mitigated by appropriate technical and organisational remedial measures. The Processor reserves the right to modify the security measures taken, ensuring that the contractually agreed level of protection is not undercut.

(3) Persons engaged in data processing by the Processor are prohibited from collecting, processing or using personal data without authorisation. The Processor shall place all persons entrusted by it with the handling and performance of this Agreement (hereinafter "Employees") under a corresponding obligation (confidentiality undertaking, Art. 28(3)(b) GDPR) and shall ensure compliance with that obligation with due care.

(4) The Processor has appointed a data protection officer. The Processor's data protection officer is Martin Bastius, heyData GmbH, Schützenstraße 5, 10117 Berlin, e-mail: datenschutz@heydata.eu, www.heydata.eu. The same details are set out in Annex 4, section A4.1.1.

§ 6 Information Obligations of the Processor

(1) In the event of disruptions, suspected personal data breaches or breaches of the Processor's contractual obligations, suspected security-relevant incidents or other irregularities in the processing of personal data by the Processor, by persons engaged by it in performing the assignment or by third parties, the Processor shall inform the Controller without undue delay. The same applies to inspections of the Processor by the data protection supervisory authority. A notification of a personal data breach shall contain at least the following information:

a) a description of the nature of the personal data breach, where possible including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
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 without undue delay take the necessary measures to secure the data and to mitigate possible adverse consequences for the data subjects, shall inform the Controller thereof and shall request further instructions.

(3) The Processor is furthermore obliged to provide the Controller with information at any time to the extent that the Controller's data are affected by a breach pursuant to paragraph 1.

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

§ 7 Audit Rights of the Controller

(1) The Controller may satisfy itself of the Processor's technical and organisational measures before the start of the processing and annually thereafter. For this purpose it may, for example, obtain information from the Processor, request the submission of existing expert attestations, certifications or internal audit reports, or inspect the Processor's technical and organisational measures itself during normal business hours after reasonable prior arrangement, or have them inspected by a qualified third party, provided that the latter is not in a competitive relationship with the Processor. The Controller shall carry out audits only to the extent necessary and shall not disproportionately disrupt the Processor's business operations.

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

(3) The Controller documents the audit result and communicates it to the Processor. In the event of errors or irregularities which the Controller identifies in particular when reviewing the results of the processing, it shall inform the Processor without undue delay. Where the audit reveals circumstances the future avoidance of which requires changes to the prescribed procedure, the Controller shall notify the Processor of the necessary procedural changes without undue delay.

§ 8 Engagement of Service Providers

(1) The contractually agreed services are performed with the involvement of the service providers named in Annex 5 (hereinafter “Sub-processors”). The Controller grants the Processor its general authorisation 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 of any intended change concerning the addition or replacement of a sub-processor. The Controller may object to an

intended addition or replacement of a sub-processor on important grounds relating to data protection law.

(3) An 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 is deemed approved. If important grounds relating to data protection law exist and no mutually acceptable solution can be found between the Controller and the Processor, the Processor has a right of extraordinary termination effective at the end of the month following the objection.

(4) When engaging sub-processors, the Processor shall impose obligations on them corresponding to 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 ancillary services only. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without a specific connection to the services the Processor provides to the Controller, and security services. Maintenance and testing services constitute sub-processing relationships subject to approval to the extent that they are provided for IT systems which are also used in connection with the provision of services to the Controller.

§ 9 Requests and Rights of Data Subjects

(1) The Processor shall, as far as possible, assist the Controller with appropriate technical and organisational measures in fulfilling its obligations under Art. 12–22 and Art. 32 to 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 act on its own initiative but shall refer the data subject to the Controller and await the Controller's instructions.

(3) Where applicable and to the extent that 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 may not sell or share such personal data as defined therein.

§ 10 Liability

(1) In the internal relationship with the Processor, the Controller alone is responsible vis-à-vis the data subject for compensation of damage suffered by a data subject as a result of processing or use that is inadmissible or incorrect under data protection law within the scope of the processing on behalf of the Controller.

(2) The Processor is liable without limitation for damage to the extent that the cause of the 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 is liable only in the event of a breach of a duty the fulfilment of which is essential to the proper performance of the Agreement and on the observance of which the Controller regularly relies and may rely, but limited to the typical foreseeable damage. In all other respects, the liability of the Processor – including for its vicarious agents and persons employed in performing its obligations – is excluded.

(4) The limitation of liability pursuant to § 10.3 does not apply to claims for damages arising from injury to life, limb 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 Union law or the law of the Federal Republic of Germany – erase them. This also applies to any backups held by the Processor. The Processor shall keep documented evidence of proper erasure and provide it upon request.

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

(3) The Processor is obliged to treat data that has become known to it in connection with the Main Agreement as confidential even beyond the end of the Main Agreement. This Agreement remains valid beyond the end of the Main Agreement for as long as the Processor holds personal data transferred to it by the Controller or collected by it for the Controller.

§ 12 Final Provisions

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

(2) Amendments and additions to this Agreement must be made in text form. This also applies to any waiver of this formal requirement. The precedence of individual contractual arrangements remains unaffected.

(3) Should individual provisions of this Agreement be or become wholly or partly 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 the Processing

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

Optional: provision of AI-supported features to assist website optimisation, the use of which requires separate activation by the user.

Optional: evaluation of test results via Varify Realtime Tracking, the use of which requires activation in the Controller's account.

Annex 2 – Description of the 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 authorised users
- Geolocation data: derived from IP addresses in order to route requests to the nearest server
- Browser and device information: information used to optimise content based on the user's device and browser

Annex 3 – Description of the Data Subjects / Groups of Data Subjects

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

Annex 4 – Technical and Organisational Measures of the Processor

Only the technical and organisational measures listed in this Annex 4 apply. There is no separate document setting out technical and organisational measures.

A4.1 Introduction

A4.1.1 Data Protection Officer

Our data protection officer is Martin Bastius, heyData GmbH, Schützenstraße 5, 10117 Berlin, e-mail: datenschutz@heydata.eu, www.heydata.eu. The same details are set out in § 5(4) of this Agreement.

A4.1.2 Purpose of this Document

This document summarises the technical and organisational measures taken by the Processor within the meaning of Art. 32(1) GDPR. A level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by the processing is ensured for the specific processing.

A4.2 Confidentiality (Art. 32(1)(b) GDPR)

A4.2.1 Physical Access Control

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

- Working from home: employees are instructed to work, where possible, in a study separated from living areas
- Manual locking system (e.g. keys)
- Key policy / key register
- Allocation of authorisations is reduced to a minimum
- Video surveillance of entrances
- Fencing of the business premises
- Visitors only when accompanied by employees
- Secured entrance gates
- Doors with a knob on the outside
- Reception desk
- Employees are instructed not to work in publicly accessible premises (e.g. cafés)

A4.2.2 System Access Control

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

- Company policy “Clean Desk”
- Authentication with user name and password

- Mandatory multi-factor authentication (MFA) for all company accounts
- Structured authorisation management and user administration
- Use of firewalls
- Use of antivirus software
- Virtual separation of tenants
- Automatic screen lock with password activation

A4.2.3 Data Access Control

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

- Employees are instructed to print only data that is strictly necessary
- Instruction not to connect external data carriers
- Rules on the administration of user roles
- Regular review and logging of authorisations
- Encryption of mobile devices and data carriers

A4.2.4 Separation Control

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

- Internal instruction to anonymise/pseudonymise personal data where possible in the event of disclosure or after expiry of the statutory retention period.
- Multi-tenant capable system
- Preparation of an authorisation concept
- Tagging of data records with purpose attributes/data fields
- Separation of development, test and production systems
- Separation of test and production data

A4.3 Integrity (Art. 32(1)(b) GDPR)

A4.3.1 Transfer Control

It is ensured that personal data cannot be read, copied, altered or removed without authorisation during transmission or while stored on data carriers, and that it can be verified which persons or bodies have received personal data. The following measures are implemented to ensure this:

- Wi-Fi encryption (WPA2 with a strong password)
- E-mail encryption
- Provision of data via encrypted connections such as SFTP or HTTPS
- Logging of access and retrievals

A4.3.2 Input Control

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

- Clear responsibilities for erasures
- Logging of the entry, modification and erasure of data
- Traceability of the entry, modification and erasure of data through individual user names (not group accounts)
- Granting of rights to enter, modify and erase data on the basis of an authorisation concept
- Data processing takes place only on instruction

A4.4 Availability and Resilience (Art. 32(1)(b) GDPR)

The following measures ensure that personal data are protected against accidental destruction or loss and remain available to the client at all times:

- Regular backups
- Backup concept including data backup
- 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 the systems for security vulnerabilities
- Monitoring of all relevant servers
- Measures against DDoS attacks
- Patch and vulnerability management

A4.5 Procedures for Regular Review, Assessment and Evaluation

(Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

A4.5.1 Data Protection Management

The following measures are intended to ensure that an organisation meeting the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Appointment of heyData as data protection officer
- Obligation of employees to maintain data secrecy
- Regular data protection training for employees

- Maintaining a record of processing activities (Art. 30 GDPR) which is updated regularly
- Monitoring and regular review of the technical and organisational measures
- Annual audits/reviews
- Process for handling data subject rights
- Erasure concepts
- Authorisation concepts

A4.5.2 Incident Response Management

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

- Notification process for personal data breaches pursuant to Art. 4(12) GDPR towards the supervisory authorities (Art. 33 GDPR)
- Notification process for personal data breaches pursuant to Art. 4(12) GDPR towards the data subjects (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches

A4.5.3 Data Protection by Default (Art. 25(2) GDPR)

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

- Employee training on "Privacy by design" and "Privacy by default"
- No more personal data are collected than are necessary for the respective purpose.

A4.5.4 Instruction Control

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

- Written contracts are in place with sub-processors
- The issuing of instructions is clearly regulated
- Data are erased at the latest after the end of the contract
- Written instructions to the contractor or instructions in text form (e.g. by way of a data processing agreement)
- Ensuring the destruction of data after completion of the assignment, e.g. by requesting corresponding confirmations
- Confirmation from contractors that they place their own employees under an obligation of data secrecy (typically in the data processing agreement)
- Sub-processors are selected with care

Annex 5 – Current Sub-processors

A5.1 Amazon AWS

Name:	Amazon AWS
Address:	Amazon Web Services EMEA Sàrl, Avenue John F. Kennedy 38, 1855 Luxembourg, Luxembourg
Description of the processing:	AWS, with its data centre in Frankfurt, serves as the hosting platform for storing and managing the hosted software and its data.
Categories of data concerned:	Network data: source and destination IP addresses, network traffic details
Place of processing:	Frankfurt data centre
Data protection contractual relationship:	An adequacy decision (the Data Privacy Framework) is in place and the provider is certified accordingly. Standard Contractual Clauses have been concluded in case that decision ceases to apply.

A5.2 Cloudflare

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:	IP addresses, log data (metadata on network events), geolocation data (derived from IP addresses), browser and device information
Place of processing:	Global, depending on the user's location
Data protection contractual relationship:	An adequacy decision (the Data Privacy Framework) is in place and the provider is certified accordingly. Standard Contractual Clauses have been concluded in case that decision ceases to apply.

Note: the sub-processors A5.3 to A5.6 listed below are used exclusively where the optional AI services of the Processor are used. If the Controller does not activate or use any AI features, no data processing by these sub-processors takes place.

A5.3 Anthropic (Claude) – AI service

Name:	Anthropic (Claude)
Address:	Anthropic, PBC, 548 Market St, PMB 90375, San Francisco, CA 94104, USA
Description of the processing:	Provision of AI-supported language models (Claude) for processing text inputs and generating text outputs within the optional AI features of the Processor.
Categories of data concerned:	Text inputs by the user (prompts), which may contain personal data; generated text outputs
Place of processing:	USA (Google Cloud / AWS data centres)
Data protection contractual relationship:	Data Processing Addendum (DPA) concluded with Anthropic. Standard Contractual Clauses pursuant to (EU) 2021/914 agreed. Zero data retention (API inputs are not stored for training).

A5.4 OpenAI (Codex) – AI service

Name:	OpenAI (Codex)
Address:	OpenAI, L.L.C., 3180 18th Street, San Francisco, CA 94110, USA
Description of the processing:	Provision of AI-supported language models (Codex) for automated code generation and text processing within the optional AI features of the Processor.
Categories of data concerned:	Text inputs by the user (prompts), which may contain personal data; generated text outputs
Place of processing:	USA (Microsoft Azure data centres)
Data protection contractual relationship:	Data Processing Addendum (DPA) concluded with OpenAI. An adequacy decision (the Data Privacy Framework) is in place and the provider is certified accordingly. Standard Contractual Clauses agreed. Zero data retention (API inputs are not stored for training).

A5.5 Google (Gemini) – AI service

Name:	Google (Gemini)
Address:	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland
Description of the processing:	Provision of AI-supported language models (Gemini) for processing text inputs and generating text outputs within the optional AI features of the Processor.
Categories of data concerned:	Text inputs by the user (prompts), which may contain

	personal data; generated text outputs
Place of processing:	EU/EEA (Google Cloud data centres, including Ireland, the Netherlands and Finland); USA where applicable
Data protection contractual relationship:	Google Cloud Data Processing Addendum (DPA) concluded. EU data centres available. For third-country transfers: adequacy decision (Data Privacy Framework) and Standard Contractual Clauses agreed.

A5.6 Firecrawl (SideGuide Technologies, Inc.)

Name:	Firecrawl (SideGuide Technologies, Inc.)
Address:	SideGuide Technologies, Inc. d/b/a Firecrawl, 800 Haight Street, San Francisco, CA, USA
Description of the processing:	Provision of a web scraping and data extraction API for preparing web content for AI-supported features within the optional AI services of the Processor. Firecrawl extracts publicly accessible web content and converts it into structured data.
Categories of data concerned:	URLs and web content of publicly accessible websites; where applicable, personal data contained on those pages (e.g. imprint details, contact information)
Place of processing:	USA (cloud infrastructure)
Data protection contractual relationship:	Use in accordance with the Firecrawl Terms of Service. Only publicly accessible web content is processed. Standard Contractual Clauses agreed for third-country transfers.

Note: the sub-processor A5.7 listed below is used exclusively where the Controller evaluates its test results using Varify Realtime Tracking. This service is optional and must be activated in the Controller's account. Without activation, no data processing by this sub-processor takes place.

A5.7 ClickHouse

Name:	ClickHouse
Address:	ClickHouse, Inc., 650 Castro St, Ste. 120 Unit 92426, Mountain View, California 94041, USA
Description of the processing:	Use as an analytical database for storing the event data collected within Varify Realtime Tracking. Test results are evaluated in the Varify application, not at ClickHouse. The service is optional and is used exclusively where the Controller activates Realtime Tracking in its account.

Categories of data concerned:	Anonymous ID (UUID, generated in the browser on page load if none exists, held in localStorage and carried across all anonymous events), session ID (held in sessionStorage, regenerated for every new tab and every new session), user agent, browser navigation information, device information derived from the user agent, and the browser time zone. No further data is transmitted. IP addresses are not transmitted to ClickHouse and are therefore not processed there. Transmission of personal data in event properties is not permitted. No ClickHouse tracker is loaded on the Controller's website; there is no direct connection between the data subject's device and ClickHouse.
Place of processing:	ClickHouse Cloud region eu-central-1, Frankfurt am Main, Germany
Data protection contractual relationship:	The ClickHouse Customer Data Processing Addendum applies. The Standard Contractual Clauses are incorporated therein by reference; Module 3 (processor to processor) applies where the Processor itself acts as a processor. In addition, an adequacy decision (the Data Privacy Framework) is in place and the provider is certified accordingly. Storage takes place exclusively within the EU.