Data Processing Addendum

Preamble

The parties have concluded a contract under which Heyflow provides services for the Customer.

In providing the services, Heyflow, as a Processor (Article 4 No. 8 GDPR), may process personal data (Article 4 No. 1 GDPR) on behalf of the Customer as a Controller (Article 4 No. 7 GDPR). References to 'GDPR' in this DPA shall be interpreted to include, where applicable, the UK GDPR (as defined in the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019), and the UK Data Protection Act 2018.

1. Definitions

1.1 **For the purposes of this Contract, the definitions of Article 4 of the GDPR shall apply, unless otherwise specified below.**

1.2 **For the purposes of this Processing Addendum, the following different and/or additional definitions shall apply:**

1.2.1 A "flow" is a web-based, interactive inquiry form that the Customer can independently configure using the Heyflow software, assuming full responsibility for its customization.

1.2.2 "End User" refers to the individual that actually uses/fills out the flow that is designed and published by the Customer.

1.2.3 "EU" or "Union" means the European Union.

1.2.4 "EEA" means the European Economic Area.

1.2.5 "Third country" means any country outside the EEA.

1.2.6 "Contract" refers to the mandating business agreement between Heyflow and Customer that is based on Heyflow's Terms and Conditions.

1.2.7 "Member State" means a Member State of the EU and/or a Contracting State to the EEA.

1.2.8 "Parties" (or individually a "Party") are the Customer and Heyflow.

1.2.9 "Services" means the services to be provided by Heyflow to the Customer under the Contract, as described in Heyflow's Terms and Conditions.

1.2.10 "Safe third countries" means all third countries to which an adequacy decision of the European Commission pursuant to Article 45 (3) of the GDPR applies.

1.2.11 "Standard Contractual Clauses (Processors)" means the standard contractual clauses annexed to European Commission Decision 2021/914 of 4 June 2021 (Ref. C(2021) 3972, OJ EU No. L 199/31 of 07.06.2021) on standard contractual clauses for transfers of personal data to third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council (Module 2).

1.2.12 "Sub-processor" means any other processor used by a Processor pursuant to Article 28(2) and (4) of the GDPR.

1.2.13 "Affiliated Company" means a company (a) owned or controlled by the Customer or Heyflow, (b) owned or controlled by the Customer or Heyflow, or (c) under common control or ownership with the Customer or Heyflow. Control means the ability to directly or indirectly exercise a controlling influence over a company, either through voting rights, contractually, or otherwise.

1.2.14 "CCPA" means the California Consumer Privacy Act, including any amendments or implementing regulations, which (a) grants California residents certain rights regarding their personal information, (b) imposes obligations on businesses that collect, use, or share such information, and (c) provides consumers with the right to access, delete, or opt out of the sale of their personal data.

2. Scope of application, parties and their respective roles

2.1 This Data Processing Addendum applies to the processing of personal data by Heyflow in the provision of the Services.

2.2 Heyflow provides the Customer with a software toolkit for creating flows. In principle, the Customer is responsible for designing these flows using the modular system. Heyflow cannot universally restrict the types of data collected through a flow. However, Heyflow offers an optional feature that prevents the storage of end users' personal data. The proper use of this feature is the responsibility of the Customer.

2.3 In the event of any contradictions between this Data Processing Addendum and other agreements concluded by the parties, particularly the main contract, the provisions of this Data Processing Addendum shall take precedence.

3. Processing details

The subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, as well as the place of processing are set out in Annex 1 to this Data Processing Addendum.

4. Responsibilities and rights of the Customer

4.1 Right to issue instructions

4.1.1 The Controller reserves the right to instruct the Processor on how to process personal data under this Data Processing Addendum.

4.1.2 The provisions of this Data Processing Agreement, especially those outlined in Section 3 for processing details, constitute general instructions for processing Personal Data as necessary for providing the Services, in accordance with both this Data Processing Agreement and the Main Agreement.

4.1.3 The Customer is authorized to issue individual instructions in text form or through corresponding settings in the software builder.

4.2 Right to access and to carry out audits, including inspections

4.2.1 The Customer has the right to request all information necessary to demonstrate compliance with Article 28 of the GDPR and to conduct verifications, including inspections, at the Processor's premises, either directly or through an auditor appointed by the Controller.

4.2.2 To demonstrate compliance with its obligations, Heyflow may submit current certificates, reports or extracts from reports from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditor, quality auditor) or a corresponding certification by an IT security or data protection audit (e.g. in accordance with the BSI basic protection).

4.2.3 If, after properly reviewing the information provided by Heyflow, the Customer has a well-founded belief that the information is insufficient to demonstrate compliance with the obligations set out in Article 28 of the GDPR, or that Heyflow has violated its obligations under Article 28 of the GDPR or these data processing terms, the Customer has the right to carry out audits – including inspections – at Heyflow, either personally or through an appointed auditor.

4.2.4 The Customer shall provide Heyflow with at least two (2) weeks' advance notice prior to conducting an audit, including any inspection.

4.2.5 Heyflow may refuse inspections outside normal business hours.

4.2.6 Access to Heyflow's premises shall only take place in the constant presence of a Heyflow representative. This representative is authorized to make decisions regarding the course of the inspection, insofar as necessary to avoid disruptions to business operations and to uphold confidentiality obligations towards third parties.

4.2.7 Heyflow permits the conduct of regular audits – including inspections – no more than once per calendar year. Additional audits – including inspections – are only permitted by Heyflow if the Customer can demonstrate a compelling reason.

4.2.8 The audit and inspection rights regulated herein are subject to the condition that the Customer treats Heyflow's trade and business secrets, which become known to the Customer during an audit – including inspections – as strictly confidential. Heyflow does not permit the Customer to record any of Heyflow's trade and business secrets that become known during such an audit – including inspections – unless this is absolutely necessary for the exercise of the audit right.

5. Responsibilities of Heyflow

5.1 Processing on documented instructions of the Customer

5.1.1 Heyflow processes the personal data that is subject to data processing on behalf of the Customer only on the basis of documented instructions from the Customer – including with regard to the transfer of personal data to a third country or an international organization – unless Heyflow is required to process the data under Union, Member State or United Kingdom law to which Heyflow is subject. In such a case, Heyflow will inform the Customer of these legal requirements prior to processing, unless the relevant law prohibits such notification for reasons of important public interest.

5.1.2 Heyflow ensures that any person under its authority who has access to the personal data covered by this Data Processing Addendum processes such data solely on the Customer's instructions, unless processing is required under Union, Member-State or United Kingdom law.

5.1.3 The Customer shall inform Heyflow without delay if they believe that an instruction violates the GDPR, the UK GDPR, or other applicable data protection regulations of the Union, its Member States, or the United Kingdom. Heyflow is entitled to suspend the execution of the respective instruction until it has been confirmed or amended by the Customer.

5.2 Confidentiality of Authorized Personnel Processing Personal Data

5.2.1 Heyflow ensures that persons authorized to process personal data under the Data Processing Addendum have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality.

5.3 Processing Security

5.3.1 Heyflow shall implement all necessary measures as required by Article 32 of the GDPR.

5.3.2 Specific measures are detailed in Annex 2 of this Processing Agreement.

5.3.3 The technical and organizational measures are subject to technological progress and further development. Therefore, Heyflow is authorized to implement additional or alternative measures to those listed in Annex 2 of these data processing provisions, provided that the security level of the previously established measures is not compromised.

5.3.4 If Heyflow becomes aware of a breach concerning the protection of personal data under the Data Processing Addendum, it shall notify the Customer without undue delay.

5.3.5 The Customer shall bear the costs associated with fulfilling its obligations arising from a personal data breach, as well as any reasonable support costs incurred by Heyflow, unless the breach results from a culpable violation of this Data Processing Addendum or of the Controller's documented instructions by the Processor.

5.4 Appointment of an Additional Processor

5.4.1 Heyflow shall comply with the following conditions set out in Article 28(2) and (4) of the GDPR for the engagement of an additional Processor:

a) Heyflow shall promptly inform the Customer of any intended changes concerning the engagement or replacement of sub-processors, thereby allowing the Customer to raise objections, if necessary.

b) If Heyflow engages an additional sub-processor to carry out specific processing activities on behalf of the Customer, it shall impose on that sub-processor the same data protection obligations as those set out in this Data Processing Addendum, by way of a contract or other legal act pursuant to Article 28 of the GDPR. In particular, the sub-processor must provide sufficient guarantees to implement appropriate technical and organizational measures to ensure that the processing complies with the requirements of the GDPR.

c) If the additional subprocessor fails to fulfill its data protection obligations, Heyflow shall be liable to the Customer for the compliance with the obligations of that other sub-processor.

5.4.2 Heyflow engages the sub-processors listed in Annex 3 of this Data Processing Addendum for the purposes of commissioned data processing.

5.4.3 If the Customer demonstrates to Heyflow that a planned change regarding the engagement or replacement of sub-processors is unreasonable – taking all relevant circumstances and the interests of both parties into account – and submits an objection in text form within two (2) weeks of being informed by Heyflow of the change, Heyflow may, at its discretion, either:

a) continue the processing without the planned change, either by itself or through another additional processor engaged by Heyflow with the Customer's approval, or

b) take all necessary measures to eliminate the reason for the Customer's objection, inform the Customer accordingly, and grant a renewed right of objection, and then proceed with the planned change if either (i) the new objection period expires without a renewed objection from the Customer, or (ii) Heyflow has implemented only those measures proposed by the Customer.

If a legitimate reason for objection exists and Heyflow does not take steps to eliminate the objection, the Customer will be granted the right to terminate the contractual relationship with immediate effect within 14 days after the objection period ends.

5.5 **Assistance to the Customer in Fulfilling Their Obligation to Respond to Data Subject Requests**

5.5.1 Heyflow supports the Customer, considering the nature of the processing, by implementing appropriate technical and organizational measures to assist in fulfilling their obligation to respond to requests for the exercise of data subjects' rights as outlined in Chapter III of the GDPR.

5.6 Assisting the Customer in GDPR Compliance Obligations

5.6.1 Taking into account the nature of the processing and the information available to Heyflow, Heyflow assists the Customer in complying with the obligations set out in Articles 32 to 36 of the GDPR concerning personal data that is subject to commissioned processing.

5.7 Deletion or return of the Personal Data to the Customer after completion of the provision of the Processing Services.

5.7.1 Upon completion of the provision of services, Heyflow shall, at the Customer's choice, either delete all personal data subject to the Data Processing Addendum or return it to the Customer and delete any existing copies, unless retention is required by Union or Member State law.

6. Transfer of personal data to third countries

6.1 Before transferring the processing to a third country, Heyflow will inform the Customer in text form (e.g., via email). The Customer may object to the change within three weeks of receiving the information from Heyflow, either in writing or in text form (e.g., via email), providing a justification. The transfer of processing to a third country may only take place if the specific conditions for the transfer to a third country in accordance with Articles 44 et seq. of the GDPR are met.

7. Liability

The liability of the parties shall be subject to the relevant statutory regulations.

8. Term and Termination

The duration of the data processing is determined by the term of the main contract. After the termination of the main contract, Heyflow is no longer bound by these provisions in relation to the Customer.

Annexes:

Annex 1: Processing details

Annex 2: Technical and organizational measures taken by the contract processor

Annex 3: Sub-processors of consumer data

Annex 1: Processing Details

Subject of processing	The subject matter of the processing is the provision of services by Heyflow. Heyflow develops software for the creation and delivery of interactive flows, which the Customer can use, for example, for customer support or for acquiring customers or employees.
Processing duration	The processing duration aligns with the service provision period and concludes upon the deletion of the Customer account created at Heyflow.
Nature and purpose of the processing	Heyflow provides the Customer with a software tool for building web-based interactive inquiry forms, known as “flows.” These flows are used to digitally capture consumer preferences and product interests. Customers can also connect their flows to third-party services, such as advertising platforms or Customer relationship management systems, via technical interfaces. These integrations are managed within the Heyflow web application, and any related data processing is carried out by Heyflow based on explicit in-app instructions.
Type of personal data	The data collected by the Customer depends on their use of the Heyflow software tool, particularly the specification of input fields. There is no universal limitation on the type of data that the Customer can collect. However, personal data like name, address, email, and phone number is often collected at the Customer's request. Form-specific data is only collected when the end user initiates data transmission by clicking the 'send' button. Additionally, a consent function can be integrated via the Heyflow app.
Data subjects	As described, data subjects cannot be universally restricted by Heyflow due to the modular character of the Heyflow app. Generally, data is collected from potential or actual prospective buyers of the Customer or potential or actual employees.

Annex 2: Technical and Organisational Measures of Heyflow

Organizations that collect, process or use personal data themselves or on their behalf must take the technical and organizational measures necessary to ensure that the provisions of the data protection laws are implemented. Measures are only necessary if their cost is proportionate to the intended purpose of protection.

The technical and organizational measures of Heyflow GmbH's overall organization are ISO 27001 certified and are regularly audited both internally and externally. Heyflow provides an up-to-date overview of its current compliance status in the publicly accessible Heyflow Trust Center at https://trust.heyflow.com/.

The measures described in this document primarily relate to end-user data—that is, information collected through the use of Heyflow's services and products.

Heyflow, hereinafter also referred to as "we" or "us", fulfills this requirement through the following measures:

1. Confidentiality according to Art. 32 para. 1 lit. GDPR

IT Infrastructure
Heyflow has outsourced the server hosting of its product offering to the leading cloud infrastructure providers. This solution promises a high level of physical and network security. The servers rented by Heyflow are located exclusively in the European Union. Google Cloud Platform regularly undergoes rigorous security audits and is certified according to ISO 27001, ISO 27002, ISO 27017, ISO 27018 and SOC 2/3, among others. The physical, environmental and infrastructural security precautions have been confirmed by independent bodies as part of the ISO 27001 and SOC 2 Type 2 certifications. The corresponding certificates can be viewed at https://cloud.google.com/security/compliance/compliance-reports-manager.

Internal processes and measures
To prevent the unauthorized use of data processing systems (computers), several rules are also taken into account. Firstly, the use of strong passwords must be guaranteed. In addition, all authentication is name-based; group users are not permitted for data processing systems. Within the company, the rule of manual desktop locking also applies, which requires all employees to lock their computer manually, even if they only leave their workplace for a short time. Furthermore, automatic desktop locks must be activated on computers to prevent misuse in the event of an employee's unplanned absence. Each computer can only be unlocked via one access point. The username and password must match.

All computers are equipped with the latest operating systems and are updated within 14 days of any new software release. To meet this requirement, Heyflow uses virtual remote management of employees' devices. This ensures that all computers in use within the company are up to date with the latest technology. When accessing customer-critical interfaces, all employees are required to use a virtual private network (VPN) to ensure a secure connection and data transfer.

Privileged access to production infrastructure is protected by Multi-Factor Authentication (MFA), and system utility access is restricted to authorized personnel only. Passwords are stored and shared using secure vault systems (e.g. 1Password and Google Passwords) in accordance with company guidelines.

Role concept
Heyflow follows a certified role concept for the administration of authorizations within the company. The role concept makes the use of each user and resource clearly traceable. Each role is assigned a substitute to avoid failures. The role concept is intended to make business processes, responsibilities and authorizations clearly traceable, particularly regarding personnel growth within the company. All employees go through a structured onboarding process including training and enablement on data privacy and security.

User access provisioning and deprovisioning are documented through an internal system (CakeWalk), and all permissions must be formally approved. Reviews of access rights – including for privileged and service accounts – are conducted at least once a year. Deprovisioning must occur within 48 business hours after contract termination or role change.

Disconnection control
Heyflow ensures separation control by applying the role concept. Furthermore, the services provided by Heyflow are made available in separate virtual folders so that a logical separation of the systems can be guaranteed. Depending on the selected service, the applications are also provided as dedicated applications (as Google Cloud Platform projects), which ensures increased separation of data processing.

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

Data transfer and storage
The role concept is used within the company to control the transfer of data. In principle, no personal data of end users is passed on within the company. In justified exceptional cases, data is transferred in recorded form and deleted as quickly as possible. Data is never passed on to third parties without a written request to do so.

The transfer of end user data to the Customer is encrypted. This includes the transfer of data by e-mail with a valid TLS/SSL certificate (TLS version 1.1 and higher) via SMTP. Any data sent via the services provided by Heyflow (“In Transit”) is encrypted with a SHA-256 (with RSA encryption) TLS (version 1.1 and up) certificate. Any data stored by Heyflow (“At Rest”) is encrypted with the Advanced Encryption Standard (AES) algorithm, AES-256.

Additionally, encryption policies are aligned with current NIST guidelines (e.g., NIST SP 800-57). Confidential company or Customer data in transit or at rest is encrypted using algorithms such as AES-256 and SCRYPT, based on data classification and lifecycle stage. Any storage of data on portable media is strictly prohibited unless encrypted and explicitly approved.

In principle, no personal data is transmitted to Heyflow or its sub-processors until the end user either submits their data via the “Submit” button or initiates a payment via the Stripe payment block, both of which are available to and configurable by the Customer within the Heyflow application.

When a heyflow is accessed and during navigation within a Heyflow, non-personal information is transmitted to heyflow. This information is necessary for processing behavioral data displayed in the analytics dashboard within the Heyflow application and for supporting error tracing and observability. The transmitted data includes, for example, the Heyflow identification number (Heyflow ID), the accessed URL, screen size, browser identifier, and debug logs. The IP address of the end user is expressly neither processed nor stored by Heyflow.

In addition to storing end user responses within its system, Heyflow provides interfaces to external services and platforms, such as Slack, HubSpot, and Salesforce, to which end user data may be transmitted, provided the Customer has explicitly configured and activated the integration. Heyflow always transmits end user data via secure connections (HTTPS/TLS); however, it assumes no responsibility for the processing or storage of such data within third-party systems.

Software development and changes

Programmatic changes to the services provided by Heyflow are logged using the versioning technology git and can thus be traced. For this purpose, the responsible developer must be clearly authenticated and registered in advance for the corresponding changes. Activities within the cloud infrastructure are logged and can be traced (see 1).

Code development follows a secure, structured release process, including staged environments (development, staging, production), automated regression testing, peer review, and manual QA testing before deployment. Developers receive regular secure coding training to mitigate OWASP Top 10 threats. In addition, Heyflow conducts annual penetration tests to identify and address potential security vulnerabilities in the application.

Changing and deleting end user data

End user data is processed automatically and encrypted using dedicated developed software systems. It is not possible for the end user to change or delete their sent data via this interface. Authorized Heyflow employees have access to the cloud infrastructure via which data can be entered, changed and deleted. For input control, the role concept is used within Heyflow according to which rights to enter, change and delete data are assigned.

Data protection-relevant additional functions of Heyflow as a software tool

Heyflow offers the functionality to mark sensitive questions as such, whereby these are only processed for forwarding to the Customer and are not stored in the Heyflow system (“sensitive tag”). Heyflow generally recommends that all Customers make use of this functionality for personal data.

Another feature that helps our customers comply with data protection regulations is the automatic deletion of outdated end-user responses. Heyflow users can enable this feature in their flow settings.

When using the restore function, which persists the end user's entries over subsequent visits, an additional field is created in the localStorage, in which the entries are stored in the end user's browser. Similarly, when using Heyflow's cookie consent manager, a field is created in the localStorage that stores the end user's privacy settings over subsequent visits. If our customer is using our A/B Testing Functionality, a cookie will be set on the end user's device so that the next time they visit the same flow they receive the same version of that flow. We don't use PII for this assignment.

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

Heyflow has outsourced the server hosting of its product offering to the leading cloud infrastructure providers. The above-mentioned providers regularly undergo strict security audits and are certified according to ISO 27001, ISO 27002, ISO 27017, ISO 27018 and SOC 2/3, among others. Availability is further ensured by a documented deployment process involving pre-release checklists, rollback strategies, and continuous monitoring.

To ensure high performance and global availability of flows for End Users, Heyflow also utilizes a Content Delivery Network (CDN). This CDN serves static assets – such as images, scripts, and stylesheets – from a distributed network of edge servers, delivering them from locations closest to the End User. Strategically located international servers can also improve the loading speed and responsiveness of flows.

These CDN edge locations and performance-optimized servers are used exclusively for acceleration purposes and do not store or process End User Data submitted via forms. They are separated from data storage components and solely intended to optimize the frontend performance of the flows.

Any processing of personal data involving routing or caching by CDN providers or global performance nodes is carried out in full compliance with applicable data protection laws (e.g., the GDPR).

Where such data routing occurs outside the European Union, Heyflow ensures that appropriate legal safeguards are in place, including the use of Standard Contractual Clauses (SCCs).

For personal data transfers from the United Kingdom to third countries, such transfers are subject to the Standard Contractual Clauses (Processors), supplemented by the UK International Data Transfer Addendum issued by the UK Information Commissioner.

Further details regarding sub-processors and cross-border data transfers can be found in Annex 3.

All End User Data submitted through flows created and managed on the Heyflow platform is primarily stored and processed within Europe. The company's core data operations are centered in this region to ensure consistent alignment with European data protection standards.

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

Employees are regularly sensitized to data protection and committed to confidentiality. A data protection impact assessment is carried out as required and in close consultation with the responsible parties. Heyflow users and end users can find the formalized process for requests for information in our privacy policy. We have provided all procedures and regulations on data protection with access for all employees as required or authorized. A review of the effectiveness of the technical protective measures is also carried out every six months under the supervision of the CTO.

Access rights – especially privileged ones – are reviewed at least annually. Job role changes trigger immediate access review and adjustment. Segregation of duties is enforced to prevent unauthorized or undetected misuse.

Critical security incidents and data breaches are documented via a ticketing system and reported immediately to our Customers by telephone or e-mail. In addition, Heyflow communicates important updates through in-app messages and maintains a publicly available status page, which can be accessed at https://status.heyflow.com.

Any obligation to report to supervisory authorities is complied with.

We follow the “privacy by default” concept and only collect the personal data that is necessary for the use of our services. The “privacy by design” principles are also embedded throughout the software lifecycle.

All sub-processors are checked by us in advance regarding the security measures implemented and their documentation. Sub-processors are selected with due diligence (in particular regarding data protection and data security). The conclusion of the necessary agreement on order processing or EU standard contractual clauses is mandatory.

Employees can report suspected or confirmed security violations, including anonymously, via an internal feedback system in line with our whistleblower policy.

Annex 3: Sub-Processors of End User Data

Default Sub-processors

Google Ireland Limited

- **Address:** Gordon House, Barrow Street, Dublin 4, Ireland
- **Scope, Nature and Purpose:** Google Cloud Platform to provide and operate the servers
- **Categories of Data Subjects:** End users
- **Categories of Personal Data:** App data, end user data as defined by Controller
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** EU

Cloudflare, Inc.

- **Address:** 101 Townsend Street, San Francisco, CA 94107, USA
- **Scope, Nature and Purpose:**
  - Content delivery, security, DNS, and abuse prevention
  - Manages SSL certificates and connections for custom domains
  - Processes limited personal data for logging and abuse detection
- **Categories of Data Subjects:** End users
- **Categories of Personal Data***:* IP address, user agent
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** Global

Optional / Feature-based Sub-processors

Amazon Web Services EMEA SARL

- **Address:** 38 Avenue John F. Kennedy, L-1855, Luxembourg
- **Scope, Nature and Purpose:** Sending request data by e-mail to Customer
- **Categories of Data Subjects:** End users
- **Categories of Personal Data:** End user data as defined by Customer
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** EU

Tinybird, Inc.

- **Address:** 41 East 11th Street, 11th Floor, New York, NY 10003, USA
- **Scope, Nature and Purpose:**
  - Real-time data processing to enhance querying and visualization of flow analytics
  - Supports analytics dashboard functionality
- **Categories of Data Subjects:** End users
- **Categories of Personal Data:** IP address
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** EU

tyntec Ltd.

- **Address:** 13th floor, One Angel Court, London EC2R 7HJ, United Kingdom
- **Scope, Nature and Purpose:** Phone number verification (optional functionality)
- **Categories of Data Subjects:** End users
- **Categories of Personal Data:** Phone number (unattributable to other PII)
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** EU / UK

Trestle Solutions, Inc.

- **Address:** 12819 SE 38th St #263, Bellevue, WA 98006, United States
- **Scope, Nature and Purpose:** Phone number verification (optional functionality)
- **Categories of Data Subjects:** End users
- **Categories of Personal Data:** Phone number (unattributable to other PII)
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** US, respective Standard Contractual Clauses included, Transfer Impact Agreement conducted

Sinch Sweden AB

- **Address:** Lindhagensgatan 112, 112 51 Stockholm, Sweden
- **Scope, Nature and Purpose:**
    - Sending one-time passcodes for SMS verification (optional functionality)
- **Categories of Data Subjects:** End users
- **Categories of Personal Data:** Phone number (unattributable to other PII)
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** EU