Data Processing Addendum

Status: August 2026

Preamble

The parties have concluded a contract under which Heyflow provides services for the Customer. This Data Processing Addendum (the "Addendum") governs Heyflow's processing of personal data in connection with those services.

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 Data Processing Addendum, the definitions of Article 4 of the GDPR shall apply, unless otherwise specified below.

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

1.2.1 Funnel: A web-based interactive form used to capture preferences or interests in specific products and services.

1.2.2 Customer: Any individual or entity utilizing Heyflow's Services, acting as Controller (Article 4(7) GDPR) with respect to personal data processed under this Data Processing Addendum.

1.2.3 End User: Refers to an individual who interacts with or uses a Funnel provided by a Heyflow customer as part of that customer's communication or services.

1.2.4 Visit: An instance in which an End User accesses a Funnel.

1.2.5 Response: A Response is defined as information provided by an End User and actively submitted through a Funnel. Each submission is counted as one response.

1.2.6 Partial Submits: An optional functionality which, when activated for a Funnel, causes multiple submissions made by the same End User within a single Funnel session to be combined and counted as a single Response, rather than being counted separately.

1.2.7 Response Handler: An optional integration which a Customer may configure and activate and which, when active, forwards Responses to the configured target system.

1.2.8 Sensitive Tag: A selectable setting within the Heyflow application which, when activated, is designed to route the relevant Responses for forwarding to the Response Handler rather than for storage within Heyflow's systems, subject to the exceptions described in Annex 2.

1.2.9 First-in First-out (FIFO): A procedure under which additional or stored responses are processed or forwarded in the order of their original receipt.

1.2.10 Consumption-Based Pricing: A billing model under which a Customer's use of a metered resource (Responses, Visits/Traffic, or Heyflow Credits) in excess of the volume included in the Customer's Plan or additionally purchased Bundles within a given Contract Period is billed automatically at the applicable per-unit rate, in accordance with Heyflow's Terms and Conditions, unless additional Bundles are purchased.

1.2.11 EU or Union: Means the European Union.

1.2.12 EEA: Means the European Economic Area.

1.2.13 Third country: Any country outside the EEA.

1.2.14 Service Contract: The paid contractual agreement between Heyflow and a Customer for the use of Heyflow's services, whether entered into directly or following a Trial Period.

1.2.15 Member State: A Member State of the EU and/or a Contracting State to the EEA.

1.2.16 Parties (or individually a "Party"): Are the Customer and Heyflow.

1.2.17 Services: Services to be provided by Heyflow to the Customer under the Service Contract, as described in Heyflow’s Terms and Conditions.

1.2.18 Safe third countries: All third countries to which an adequacy decision of the European Commission pursuant to Article 45 (3) of the GDPR applies.

1.2.19 Standard Contractual Clauses (Processors): 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 and/or Module 3, as applicable to the relevant transfer).

1.2.20 Sub-processor: Any other processor used by a Processor pursuant to Article 28(2) and (4) of the GDPR.

1.2.21 Affiliated Company: 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.

1.2.22 CCPA: 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.

1.2.23 Programmatic Interface: Any interface, other than the standard Heyflow web application GUI, through which a Customer or a tool acting on the Customer's instruction may access, configure, or manage the Customer's Heyflow account, including an Application Programming Interface (API), a Command Line Interface (CLI), and an MCP Integration.

1.2.24 MCP Integration: A Programmatic Interface established via the Model Context Protocol (MCP) or a functionally equivalent protocol, through which a third-party AI assistant (e.g., Claude or ChatGPT), operated by the Customer under the Customer's own arrangement with the relevant provider, may access the Customer's Heyflow account to view, create, edit, publish, or otherwise manage Funnels on the Customer's instruction.

1.2.25 AI Output: Content, design, structure, conditional logic, routing, and other configuration of a Funnel that is generated, suggested, or modified using Heyflow's own AI assistant, or a third-party AI assistant accessed via an MCP Integration or other Programmatic Interface.

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 Funnels. In principle, the Customer is responsible for designing these Funnels using the modular system. Heyflow cannot universally restrict the types of data collected through a Funnel. However, Heyflow offers an optional feature — the Sensitive Tag functionality described in Annex 2 — that is designed to limit storage of End Users' personal data, subject to the exceptions described there. 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 Service Contract, the provisions of this Data Processing Addendum shall take precedence.

2.4 Where the Customer processes Protected Health Information ("PHI") within the meaning of the U.S. Health Insurance Portability and Accountability Act ("HIPAA") using the Services, a separate Business Associate Agreement ("BAA") entered into between the Customer and Heyflow shall apply to such processing. In the event of any conflict between this Data Processing Addendum and the BAA with respect to the processing of PHI, the BAA shall take precedence.

2.5 With respect to personal information of California residents processed under this Data Processing Addendum, Heyflow acts as a "Service Provider" within the meaning of the California Consumer Privacy Act ("CCPA"). Heyflow shall not sell or share such personal information and shall process it solely for the Business Purposes specified by the Customer and for no other purpose.

2.6 Except as otherwise provided in Sections 5.4 (engagement of sub-processors) and 6 (transfers to third countries), amendments to this Data Processing Addendum are subject to the amendment and objection procedure set out in Heyflow's Terms and Conditions.

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 Addendum, 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 Addendum and the Service Contract.

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 the Data Processing Addendum, 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 Heyflow shall inform the Customer without delay if, in its opinion, an instruction given by the Customer infringes 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.

5.1.4 Heyflow shall not use Responses (personal data submitted by End Users through a Funnel) to train, fine-tune, evaluate, or otherwise develop or improve any artificial intelligence or machine learning model, whether operated by Heyflow or by a third party.

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 Data Processing Addendum.

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 the Data Processing Addendum, 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.

This process also governs any resulting transfer of processing to a third country (see Section 6.1).

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.

5.8 **External Data Protection Service Provider**

5.8.1 Heyflow relies on the services of the external data protection service provider PROLIANCE GmbH (www.datenschutzexperte.de), Dominik Fünkner, Leopoldstr. 21, 80802 München, refer to datenschutzbeauftragter@datenschutzexperte.de for questions and matters relating to data protection.

6. Transfer of personal data to third countries

6.1 Personal data may only be transferred to a third country if the specific conditions for such a transfer under Articles 44 et seq. of the GDPR are met, in particular through the use of Standard Contractual Clauses (Processors) or an applicable adequacy decision pursuant to Article 45 GDPR. For personal data transfers from the United Kingdom to third countries, the Standard Contractual Clauses (Processors), as supplemented by the UK International Data Transfer Addendum issued by the UK Information Commissioner, shall apply. Where the transfer is to a sub-processor engaged by Heyflow (as opposed to a transfer from the Customer as controller to Heyflow as processor), Module Three (processor to processor) of the Standard Contractual Clauses (Processors) applies.

6.2 Where a transfer of processing to a third country results from the engagement or replacement of a sub-processor, the notification and objection procedure set out in Section 5.4 shall apply, and no separate notification or objection right shall arise under this Section 6. Where a transfer of processing to a third country arises other than through the engagement or replacement of a sub-processor, Heyflow will inform the Customer in text form (e.g., via email) in advance, and the Customer may object within two (2) weeks of receiving such information, in writing or in text form, providing a justification. Section 5.4.3(a)–(b) shall apply mutatis mutandis to any such objection.

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 Service Contract. After the termination of the Service Contract, Heyflow is no longer bound by these provisions in relation to the Customer.

Annexes:

Annex 1: Processing details

Annex 2: Technical and Organisational Measures of Heyflow

Annex 3: Sub-Processors of End User 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 Funnels. Funnels are individually modifiable by the Customer, but are typically used to capture End User preferences, product interests, or job applications.
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 and operating Funnels. Customers can connect their Funnels 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. Heyflow may also use third-party AI providers internally (see Annex 3) to power Heyflow's own AI assistant and other features generating AI Output, and to help deliver parts of the Service more generally, including in connection with requests received via the MCP Integration or another Programmatic Interface.
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. The transmission of form-specific data depends on how the Customer has configured the relevant Funnel, including which building blocks — such as the "Submit" button, the Stripe payment block, or another configurable building block — are configured to trigger data transmission. 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 SOC 2 Type II certified (covering the Security and Confidentiality Trust Services Criteria, independently audited), and are regularly audited both internally and externally. Heyflow provides an up-to-date overview of its current compliance status, including current certification periods and reports, 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 (Art. 32(1)(b) GDPR)

IT Infrastructure
For the hosting of its product offering, Heyflow relies on leading, state-of-the-art cloud infrastructure. This solution promises a high level of physical and network security. The servers rented by Heyflow are located exclusively in the European Union. The servers themselves are hosted with Google Cloud Platform, which 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/offerings.

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.

Separation 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.

End User data transmitted between users or Customers and Heyflow's public production endpoints is encrypted in transit using TLS 1.2 or TLS 1.3. These endpoints use restricted modern cipher suites; the cipher suite and key-exchange mechanism are negotiated for each connection, with forward secrecy provided where supported. When Heyflow sends End User data by email, the connection is encrypted using TLS. Email delivery to the Customer's receiving mail server uses TLS where the receiving server supports it.

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.

The transmission of personal data to Heyflow or its sub-processors depends on how the Customer has configured the relevant Funnel. Each relevant building block — such as the "Submit" button, the Stripe payment block, or another configurable building block — is available to, and must be explicitly configured and activated by, the Customer within the Heyflow application. Personal data is transmitted to Heyflow or its sub-processors only in accordance with such configuration.

When a Funnel is accessed and during navigation, 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.

Heyflow offers an integration ("MCP Integration") that allows the Customer to connect a third-party AI assistant (e.g., Claude or ChatGPT), operated by the Customer under the Customer's own account and arrangement with the relevant provider, to the Customer's Heyflow account in order to view, create, edit, or manage Funnels on the Customer's instruction. Data exchanged directly between the Customer's own AI assistant and its provider in the course of this connection is processed under the Customer's own agreement with that provider; Heyflow is not a party to, and assumes no responsibility for, that processing.

Separately, Heyflow itself uses third-party AI providers to power Heyflow's own AI assistant and other AI-assisted features generating AI Output, and to help deliver parts of the Service more generally, including in connection with requests received via the MCP Integration or another Programmatic Interface. In each case, Heyflow uses its own account and credentials with the relevant provider — the Customer does not connect its own account. The relevant provider(s) are engaged as Heyflow's sub-processor(s) for this purpose and are listed in Annex 3, regardless of whether a specific instance of such processing involves personal data. End User Responses are not currently accessible through the MCP Integration.

Should Heyflow in the future enable retrieval of Responses via the MCP Integration, such retrieval shall be available only to Customers who have separately activated a dedicated account-level setting for this purpose, distinct from activation of the MCP Integration itself.

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 Sensitive Tag functionality, which, when activated, is designed to route the relevant Responses for forwarding to the Customer's configured Response Handler rather than for storage within Heyflow's systems. Where the Customer's Response quota has been exceeded and the Customer is not subject to Consumption-Based Pricing, further Responses — including those marked with a Sensitive Tag — are stored in the Heyflow system notwithstanding the Sensitive Tag setting, and are forwarded on a First-in-First-out (FIFO) basis once additional Response quota has been purchased. Where the Customer is subject to Consumption-Based Pricing, Responses continue to be forwarded and processed as configured, including in accordance with the Sensitive Tag setting, regardless of quota. Heyflow generally recommends that all Customers make use of the Sensitive Tag functionality for personal data and, where not subject to Consumption-Based Pricing, monitor their Response quota accordingly.

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 Funnel 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 Funnel they receive the same version of that Funnel. We don’t use PII for this assignment.

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

Heyflow's server hosting, as described above, is provided by Google Cloud Platform, which regularly undergoes rigorous security audits and is 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 Funnels 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 Funnels.

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 Funnels.

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.

The hosting infrastructure described above – i.e., the servers on which End User Data is stored – is primarily located within Europe, and Heyflow's core hosting operations are centered in this region to ensure consistent alignment with European data protection standards. This statement relates solely to server hosting; the complete list of sub-processors involved in the processing of End User Data, including those located outside the EU/EEA, is set out in Annex 3.

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 email. 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

Anthropic PBC

- **Address:** 548 Market Street, PMB 90375, San Francisco, CA 94104, USA
- **Scope, Nature and Purpose:** Heyflow's internal use of AI models to power Heyflow's own AI assistant and other AI-assisted features generating AI Output (e.g., interpreting instructions, generating or structuring Funnel content), and to help deliver parts of the Service more generally, including but not limited to requests received via the MCP Integration. This entry applies regardless of whether a given instance of such processing involves personal data.
- **Categories of Data Subjects:** End Users and/or Customer users, to the extent personal data is incidentally included in the processed content.
- **Categories of Personal Data:** Varies by feature; primarily Funnel structure/configuration data, which may incidentally include personal data (e.g., placeholder text, test submissions, or account metadata)
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** US, Standard Contractual Clauses apply, Transfer Impact Agreement conducted

OpenAI Ireland Limited

- **Address:** 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
- **Scope, Nature and Purpose:** Heyflow's internal use of AI models to power Heyflow's own AI assistant and other AI-assisted features generating AI Output (e.g., interpreting instructions, generating or structuring Funnel content), and to help deliver parts of the Service more generally, including but not limited to requests received via the MCP

Integration. This entry applies regardless of whether a given instance of such processing involves personal data.
- **Categories of Data Subjects:** End Users and/or Customer users, to the extent personal data is incidentally included in the processed content.
- **Categories of Personal Data:** Varies by feature; primarily Funnel structure/configuration data, which may incidentally include personal data (e.g., placeholder text, test submissions, or account metadata)
- **Duration of the Sub-processing:** Undefined
- **Place of Sub-processing:** EU

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 email 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 Funnel 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

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 Assessment 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