UptimeEye Data Processing Agreement

pursuant to Art. 28 GDPR · Version 1.2 · 15 November 2026

between

the Customer of the Service, i.e. the legal entity or natural person that holds the UptimeEye account or is named in the signature block below (the "**Controller**")

and

LaunchX GmbH, Lärchenstraße 12, 84032 Landshut, Germany, registered with the Amtsgericht Landshut under HRB 14838, represented by its managing directors, operator of UptimeEye (the "**Processor**", "**we**")

1. Subject matter and scope

1.1 This Data Processing Agreement ("**DPA**") governs the processing of personal data by the Processor on behalf of the Controller in connection with the UptimeEye service at uptimeeye.com, including its web app, mobile and desktop apps, API and MCP server (the "**Service**"), as provided under the UptimeEye Terms and Conditions (the "**Main Agreement**").

1.2 This DPA applies to every plan of the Service, including the Free plan, regardless of whether a paid subscription exists.

1.3 The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are described in **Annex 1**.

1.4 This DPA does not cover data for which the Processor is itself controller, in particular the account data of the users who sign up for and sign in to the Service (name, email address, sign-in and session data), billing data, and the Processor's own website analytics. That processing is described in the UptimeEye Privacy Policy.

1.5 The term of this DPA corresponds to the term of the Main Agreement. Provisions that by their nature continue after termination (in particular sections 10 and 11) remain in force until all personal data processed on behalf of the Controller has been deleted or returned.

1.6 This DPA forms part of the Main Agreement and applies to every Customer that uses the Service, from the start of use, without a separate signature. A Customer may additionally sign this DPA and send it to contact@uptimeeye.com; the Processor then returns a countersigned copy. The version published at uptimeeye.com/trust applies; the Processor informs Customers of material changes in advance by email.

2. Instructions

2.1 The Processor processes personal data only on documented instructions from the Controller, including with regard to transfers to a third country, unless required to do so by Union or

Member State law. In that case the Processor informs the Controller of that legal requirement before processing, unless the law prohibits this.

2.2 The Main Agreement, this DPA, and the Controller's configuration and use of the Service (for example the monitors, scheduled tasks, notification channels and log sources it sets up) constitute the Controller's complete instructions at the time of signing. Further instructions must be given in writing or in text form (email to contact@uptimeeye.com) and must be within the scope of the Service.

2.3 The Processor informs the Controller without undue delay if it considers that an instruction infringes the GDPR or other data protection provisions. The Processor may suspend execution of the instruction until the Controller confirms or changes it.

3. Confidentiality

The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4. Security of processing

4.1 The Processor implements the technical and organisational measures described in **Annex 2** to ensure a level of security appropriate to the risk (Art. 32 GDPR).

4.2 The measures are subject to technical progress. The Processor may implement alternative adequate measures, provided the level of security of the measures in Annex 2 is not reduced.

5. Sub-processors

5.1 The Controller grants general authorisation for the Processor to engage sub-processors. The sub-processors engaged at the time of signing are listed in **Annex 3**; the current list is published at uptimeeye.com/trust.

5.2 The Processor informs the Controller of any intended addition or replacement of a sub-processor at least **14** days in advance, by email to the account owner or by updating the list at uptimeeye.com/trust together with an email notice. The Controller may object on reasonable data-protection grounds within that period. If the parties cannot resolve the objection, the Controller may terminate the affected part of the Service. Fees already paid for the remaining term of a paid subscription are refunded pro rata.

5.3 The Processor imposes on each sub-processor, by contract, data protection obligations that offer at least the same level of protection as this DPA. The Processor remains liable to the Controller for the performance of the sub-processor's obligations.

5.4 Providers of purely ancillary services (for example telecommunications, or the operating-system push services of Apple and Google that deliver notifications to a device the user registered themselves) are not sub-processors within the meaning of this section, insofar as they do not process the Controller's data on the Processor's behalf.

6. Transfers to third countries

6.1 Personal data processed on behalf of the Controller is stored in the European Union (Germany). Some sub-processors in Annex 3 process data in the United States or other third countries.

6.2 The Processor transfers personal data to a third country only if the requirements of Chapter V GDPR are met, in particular on the basis of an adequacy decision (for the United States: the EU-U.S. Data Privacy Framework, for recipients certified under it) or of the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, Module 3 (processor to processor), concluded with the sub-processor. Annex 3 states the transfer mechanism for each sub-processor.

6.3 Monitors that the Controller assigns only to the probe location eu-central-1, and scheduled tasks (heartbeats), are processed exclusively in Germany, except for the email alert delivery listed in Annex 3.

7. Assistance

7.1 Taking into account the nature of the processing, the Processor assists the Controller with appropriate technical and organisational measures in responding to requests from data subjects exercising their rights under Chapter III GDPR. Most data can be viewed, exported, changed and deleted directly in the Service. If a data subject contacts the Processor directly, the Processor forwards the request to the Controller without undue delay and does not respond on its own unless instructed.

7.2 The Processor assists the Controller in ensuring compliance with Articles 32 to 36 GDPR (security, notification of personal data breaches, data protection impact assessments, prior consultation), taking into account the nature of processing and the information available to the Processor.

8. Personal data breaches

8.1 The Processor notifies the Controller without undue delay, and in any case within **48** hours, after becoming aware of a personal data breach affecting personal data processed on behalf of the Controller.

8.2 The notification contains, as far as available, the information listed in Art. 33(3) GDPR. Where not all information is available at once, it is provided in phases without undue further delay.

8.3 The Processor takes the measures necessary to contain the breach and to mitigate its possible adverse effects, and documents the breach.

9. Audits and information

9.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with Art. 28 GDPR and this DPA.

9.2 The Processor allows for and contributes to audits, including inspections, by the Controller or an independent auditor mandated by the Controller who is bound to confidentiality. Audits are generally carried out by written questionnaire. On-site inspections require at least **30** days' notice, take place during normal business hours without disrupting operations, and are limited to once per calendar year unless there is a concrete indication of a breach. Each party bears its own costs.

10. Deletion and return

10.1 After the end of the provision of services, the Processor deletes all personal data processed on behalf of the Controller, unless Union or Member State law requires storage. Before that, the Controller can export its data via the Service or the API, or request a copy by email.

10.2 Deletion from the production systems takes place within **30** days after the end of the Main Agreement or after the Controller's deletion request. Copies in encrypted backups are overwritten in the regular backup cycle and are deleted at the latest **90** days after deletion from the production systems. Until then they are not used for any purpose other than disaster recovery.

10.3 The retention periods applying during the term are listed in Annex 1, section 5.

11. Liability

11.1 The liability of the parties towards data subjects is governed by Art. 82 GDPR.

11.2 In the relationship between the parties, the liability provisions of the Main Agreement apply, to the extent permitted by law. Liability for intent and gross negligence, and for injury to life, body or health, remains unlimited.

12. Final provisions

12.1 In the event of a conflict, this DPA takes precedence over the Main Agreement with regard to data protection.

12.2 Changes and amendments to this DPA must be made in writing or in text form.

12.3 Should individual provisions of this DPA be invalid, the validity of the remaining provisions remains unaffected.

12.4 This DPA is governed by German law. Place of jurisdiction is Landshut, Germany, to the extent permitted by law.

For the Controller	**For the Processor**
Legal name[1]: _____	LaunchX GmbH
Trading as (optional): _____	UptimeEye
Address: _____	Lärchenstraße 12, 84032 Landshut, Germany
Register / registration no. (if any): _____	Amtsgericht Landshut, HRB 14838

For the Controller	For the Processor
UptimeEye workspace: _____	
Signatory, function: _____	Manuel Müller, Managing Director
Place, date: _____	Place, date: Landshut, _____
Signature: _____	Signature: _____

[1] The registered legal entity that operates the service for which UptimeEye is used. If the business is run by a sole trader or a partnership without a registered name, enter the full name(s) of the owner(s), and the trade name under “Trading as”.

Annex 1: Description of the processing

1. Nature and purpose

Providing the UptimeEye service: monitoring the availability and behaviour of websites, APIs and servers specified by the Controller (“monitors”), receiving and evaluating heartbeats from the Controller’s recurring jobs (“scheduled tasks”), receiving, storing and searching log data the Controller sends (“UptimeEye Logs”), alerting the Controller through the notification channels it configures, operating status pages, and storing the related history.

2. Categories of data subjects

- Employees and contractors of the Controller who are named as alert recipients or appear in configurations
- Subscribers of the Controller’s status pages
- End users of the Controller’s systems, insofar as their data is contained in log data or in check responses the Controller has the Service retrieve
- Other persons whose data the Controller enters into the Service

3. Types of personal data

Area	Data
Scheduled tasks (heartbeats)	Timestamp, beat type (start, success, failure), duration if sent, sender IP address, user agent; task configuration (name, schedule, time zone, grace period); run, outage and alert history
Monitors	Configuration (URLs, headers, request bodies, assertions, secure variables), check results (status codes, response times, error messages), check responses where the Controller has them evaluated
Notification channels	Email addresses, chat or webhook targets, PagerDuty keys and similar the Controller enters; content of alerts (name and status of

Area	Data
	the monitor, task or log alert, time)
Status pages	Subscriber email addresses, incident texts
Logs	Log lines the Controller sends, which may contain any personal data the Controller's systems log (for example IP addresses, user identifiers, email addresses)

The Controller does not send special categories of personal data (Art. 9 GDPR), credentials or payment card data in logs, heartbeats or configurations.

4. Location

Production data is stored on servers of Hetzner Online GmbH in Falkenstein, Germany. Encrypted database backups are stored with Amazon Web Services in Frankfurt, Germany. For processing by sub-processors outside the EU, see Annex 3.

5. Retention during the term

Data	Retention
Raw monitor check results	7 days, then deleted automatically; aggregated uptime statistics are kept for the life of the monitor
Heartbeats, run history, outages and alert records of a scheduled task	For the life of the task; deleted together with the task
Log data	Per plan: 3 days (Free), 7 days (Pro), 15 days (Agency); physical storage reclaimed within 31 days
Monitors, tasks, channels, status pages, incidents	Until deleted by the Controller, or until the end of the Main Agreement (section 10)
Encrypted backups	Point-in-time recovery window of 30 days; backup copies are deleted at the latest 90 days after creation

Annex 2: Technical and organisational measures (Art. 32 GDPR)

1. Confidentiality

Physical access control. All systems run in data centres of Hetzner Online GmbH (Germany) and Amazon Web Services (Frankfurt), which are certified under ISO/IEC 27001. The Processor operates no server rooms of its own.

System access control. Administrative access to the server infrastructure is restricted to the managing directors and the automated deployment pipeline and uses SSH keys. Infrastructure is managed as code (Terraform, Kubernetes manifests) and changes go through version control.

A network firewall exposes only the required ports. Secrets are stored encrypted in the cluster (Sealed Secrets) and not in plain text in repositories.

Data access control. Every customer workspace (organisation) is logically isolated, and every request is authorised against the signed-in member's organisation memberships and role. Ingest keys for logs can only write; reading requires a signed-in member. Each organisation's log data is held in a separate tenant. Secure variables are stored encrypted. Sign-in is provided by Clerk; members' passwords are never processed or stored by the Processor.

Separation. Production and test environments are separate (separate databases and deployments).

2. Integrity

Transfer control. All connections to the Service and between the Service and its sub-processors are encrypted with TLS. Backups are transferred to AWS S3 over TLS.

Input control. Every request is authenticated as a signed-in member or an API key of the organisation. Tool calls by AI assistants connected through MCP are logged with the tool name, the organisation and the names of the arguments.

3. Availability and resilience

Availability control. The database is backed up continuously to Amazon S3 in Frankfurt (write-ahead log archiving plus a weekly full backup), encrypted at rest (AES-256), with bucket versioning and public access blocked. Backups allow point-in-time recovery within the retention window. Systems are monitored around the clock, including with UptimeEye itself.

Recoverability. The database can be restored to any point in time within the retention window.

4. Procedures for regular review

Data protection management. The managing directors are responsible for data protection. The Processor is not required to appoint a data protection officer (Art. 37 GDPR, § 38 BDSG); privacy enquiries go to contact@uptimeeye.com.

Incident response. Security incidents are assessed without undue delay and the Controller is informed under section 8 of the DPA.

Privacy by default. Optional data flows to third countries (push notifications, the in-app AI assistant, probe locations outside the EU) are switched off until a member actively uses them. Log access for the AI assistant is off until an admin switches it on.

Order control. Sub-processors are selected according to their data protection guarantees, and data processing agreements are concluded with them.

Annex 3: Sub-processors

As of 15 November 2026. The current list is published at uptimeeye.com/trust.

Sub-processor	Purpose	Data	Location	Transfer mechanism
Hetzner Online GmbH, Gunzenhausen, Germany	Hosting of application, database and log storage; check probe location eu-central-1	All data processed on behalf of the Controller	Germany (Falkenstein)	Not applicable (EU)
Amazon Web Services	Encrypted database backups (Amazon S3)	Backup copies of all database data (not log data)	Germany (Frankfurt, eu-central-1)	Not applicable (EU region); AWS GDPR Data Processing Addendum
Amazon Web Services	Check probes at the locations us-east-1, us-west-2, ap-southeast-1, ap-southeast-2, sa-east-1; **only for monitors the Controller assigns to those locations**	Monitor configuration including secure variables, check responses	USA, Singapore, Australia, Brazil	SCCs under the AWS GDPR Data Processing Addendum
Resend (Plus Five Five, Inc.)	Delivery of alert and transactional emails	Recipient email address, alert content (name and status of the monitor, task or log alert, time)	USA	EU-U.S. DPF (incl. UK Extension); SCCs as fallback
Google LLC (Firebase Cloud Messaging)	Push notifications to the mobile and desktop apps; **only for members who turn push on**	Device push token, notification content (name and status of the monitor, task or log alert, organisation name, time, internal IDs); no URLs, no log lines	USA	EU-U.S. DPF (Google LLC); SCCs under the Firebase Data Processing and Security Terms

Sub-processor	Purpose	Data	Location	Transfer mechanism
OpenAI Ireland Ltd. (with OpenAI, L.L.C.)	The in-app AI assistant; **only when members use it**	Chat messages and the configuration and check status the assistant reads; log lines only if an admin switched on Log access; never response bodies, headers or secure variable values	Ireland; USA	OpenAI Data Processing Addendum; SCCs (2021/914) for transfers to the USA

Not sub-processors under this DPA:

- **Clerk, Inc.** (USA) provides sign-in and user management. It processes the account data of members (name, email address, sign-in and session data, workspace name and memberships), for which the Processor is controller (section 1.4). Clerk acts as the Processor's own processor for that data, under Clerk's data processing addendum with EU-U.S. DPF certification (incl. UK Extension and Swiss-U.S. DPF) and SCCs as fallback. Clerk does not process the Controller's monitoring, scheduled-task or log data.
- **Stripe.** For every workspace, including on the Free plan, a Stripe customer record with the workspace name and an internal workspace ID is created. Stripe processes payment data as an independent controller under its own privacy policy (Stripe, LLC is certified under the EU-U.S. DPF).

Changes in version 1.2 (15 November 2026): new section 1.6, the DPA applies to every Customer as part of the Main Agreement, signature optional.

Changes in version 1.1 (15 November 2026): Clerk moved from the sub-processor table to the list of providers that are not sub-processors under this DPA, consistent with section 1.4; signature block extended to name the Controller's legal entity.