Data Processing Agreement

Version 1.0, effective 19 November 2026. For accounts created before that date, it takes effect on 19 December 2026, together with the Terms.

This Data Processing Agreement ("DPA") forms part of the Terms of Service (the "Terms") between UPTRACE DEV S.R.L. ("Uptrace", "we") and the customer that uses Uptrace Cloud ("Customer", "you"). It applies to personal data that Uptrace processes for the Customer when it provides the Services.

You can accept this DPA in either of two ways:

1. **As part of the Terms.** The DPA applies automatically to every Uptrace Cloud account. You do not need to do anything.
2. **As a signed copy.** If you need a countersigned copy, an owner of your organization can sign this DPA in Uptrace Cloud, on the organization's settings page, and download the copy Uptrace countersigns at once. You can also download the DPA as a PDF, fill in and sign the Customer block in the Signatures section, and email it to support@uptrace.dev. We will return a countersigned copy. A signed copy does not change the text of this DPA.

1. Definitions

Terms used but not defined in this DPA, such as "controller", "processor", "data subject", "personal data", "processing" and "supervisory authority", have the meanings given in the GDPR.

1. **"Data Protection Laws"** means all laws that apply to the processing of Customer Personal Data under this DPA, including the GDPR, the UK GDPR and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection ("FADP"), and US state privacy laws such as the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA").
2. **"GDPR"** means Regulation (EU) 2016/679.

3. **"Customer Personal Data"** means personal data that the Customer, or users acting for the Customer, submit to the Services and that Uptrace processes on the Customer's behalf. This includes personal data contained in telemetry (traces, spans, logs, events, metrics and profiles) and in the content the Customer creates in the Services, such as dashboards, alerts and notification settings.
4. **"Services"** means Uptrace Cloud, the hosted Uptrace service at uptrace.dev, including its user interface, APIs and ingestion endpoints.
5. **"Subprocessor"** means any third party that Uptrace engages to process Customer Personal Data.
6. **"Security Incident"** means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data. It does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as pings, port scans, denial-of-service attacks, failed sign-in attempts and blocked attacks. Nor does it include access to, or disclosure of, Customer Personal Data with the Customer's credentials, such as API tokens, DSNs and user passwords, that were disclosed or compromised outside the Services, or through the Customer's own single sign-on or identity provider (Section 7.1), unless Uptrace's breach of Section 5 or Annex II caused it. If Uptrace becomes aware of such access, it tells the Customer without undue delay and assists as Section 10.4 provides.
7. **"SCCs"** means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
8. **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, issued by the UK Information Commissioner under section 119A of the UK Data Protection Act 2018.

2. Scope and roles

1. The Customer is the controller of Customer Personal Data, and Uptrace is its processor. Where the Customer processes Customer Personal Data as a processor for its own clients, Uptrace is a subprocessor, and the Customer is responsible for obtaining any authorisations its controller requires.

2. Uptrace is an independent controller, not a processor, for the personal data it needs to run the Customer's account: names and email addresses of users, sign-in data, billing records and support correspondence. Our Privacy Policy describes that processing.
3. Annex I describes the subject matter, nature, purpose and duration of the processing, and the types of personal data and data subjects.
4. The Customer is responsible for the lawfulness of the Customer Personal Data it sends to the Services, including having a legal basis and giving any notices to data subjects. The Services are built for operational telemetry. The Customer must not send the prohibited data listed in Section 4.2 of the Terms, which include special categories of personal data (GDPR Art. 9) and data relating to criminal convictions (GDPR Art. 10), and must keep such data out, for example with transform pipelines. Uptrace has no obligations for such data beyond the measures in Annex II.
5. This DPA does not apply to self-hosted software, including the Licensed Software defined in the Terms. The Customer operates it on its own infrastructure, and Uptrace processes no Customer Personal Data in it. The Customer removes personal data from the material it sends with a support request about the Licensed Software. If such material contains personal data anyway, this DPA applies to that personal data as Customer Personal Data.
6. The Customer indemnifies Uptrace, as Section 12 of the Terms provides, against claims of data subjects and other third parties, investigations and proceedings of public authorities, and the resulting losses, damages, fines to the extent the law allows them to be indemnified, costs and reasonable legal fees, to the extent they arise from Customer Personal Data that the Customer had no right to send to the Services. That includes data sent without a legal basis, data whose subjects were not given the notices Section 2.4 requires, and data that Section 4.2 of the Terms prohibits. Section 11.3 of the Terms excludes this obligation from the limitations of liability.

7. If Uptrace becomes aware that a project receives data that Section 4.2 of the Terms prohibits, the Customer instructs Uptrace to delete that data, or to keep it from being displayed and queried until it expires. Where the data puts data subjects or the Services at risk, or the Customer does not stop sending it after notice, the Customer also instructs Uptrace to suspend ingestion for that project until the Customer stops sending it. Uptrace tells the account owner first where it can, and limits the action to the data and the project concerned. Uptrace has no duty to look for such data.

3. Customer instructions

1. Uptrace processes Customer Personal Data only on the Customer's documented instructions, unless Union or Member State law to which Uptrace is subject requires otherwise. In that case, Uptrace informs the Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.
2. The Customer's instructions are:
    - the Terms and this DPA;
    - the Customer's configuration of the Services, including projects, retention periods, transform pipelines, ingestion settings, alerts, notification channels and other integrations, and a project administrator's acceptance of the data notice for optional AI features;
    - any other written instructions the Customer gives and Uptrace accepts.
3. Uptrace informs the Customer without delay if, in its opinion, an instruction infringes Data Protection Laws, and may suspend carrying out that instruction until the Customer confirms or changes it. Uptrace is not obliged to carry out a legal review of the Customer's instructions.
4. Uptrace does not sell Customer Personal Data, does not use it to train AI models that are used for, or made available to, anyone other than the Customer, and does not use it for advertising or for any purpose other than providing, securing and supporting the Services, and as Section 3.5 provides.

5. The Customer instructs Uptrace to create anonymised, aggregated statistics from Customer Personal Data, such as data volumes, cardinality and performance figures, that do not identify the Customer, its users or any data subject, and to use them to operate and improve the Services. These statistics are not Customer Personal Data.

4. Confidentiality and personnel access

1. Uptrace ensures that every person authorised to process Customer Personal Data is bound by a duty of confidentiality, by contract or by law.
2. Uptrace personnel access Customer Personal Data only when that is needed:
    - to provide support the Customer asks for, and only with the Customer's consent;
    - to keep the Services running, for example when an automated process fails, and then only to the minimum extent needed;
    - to investigate a Security Incident, abuse or a breach of the Terms;
    - to comply with law, as described in Section 9.

5. Security

1. Uptrace implements and maintains the technical and organisational measures in Annex II to protect Customer Personal Data, as GDPR Art. 32 requires.
2. Uptrace may update these measures as technology and threats change, provided an update does not reduce the overall level of protection.
3. The Customer is responsible for using the security features the Services provide, such as roles and permissions, single sign-on, two-factor authentication and the protection of its API tokens and DSNs, and for incidents that result from their compromise (Section 1.6).

6. Subprocessors

1. The Customer gives Uptrace a general written authorisation to engage Subprocessors. Annex III lists the Subprocessors authorised on the effective date. The AI model providers it lists are used only while they are the default AI model provider (Section 7.3).
2. Uptrace notifies the Customer at least 30 days before it adds or replaces a Subprocessor, by email to the account owner and by updating Annex III on this page, except as Section 6.5 provides. The Customer is responsible for keeping the account owner's email address current.
3. The Customer may object to a new Subprocessor on reasonable data protection grounds by writing to support@uptrace.dev within that 30-day period, stating the specific grounds. The parties will discuss the objection in good faith, and Uptrace may propose a change to the Services or their configuration that avoids the Subprocessor for the Customer. If they cannot resolve it, the Customer may terminate the affected Services before the change takes effect, as Section 17.4 provides.
4. Uptrace imposes on each Subprocessor, by written contract, data protection obligations that offer at least the same level of protection as this DPA. Uptrace remains fully liable to the Customer for the performance of each Subprocessor's obligations, subject to Section 16.
5. Where Uptrace must replace a Subprocessor urgently because the security or continuity of the Services requires it, Uptrace may engage the replacement before the 30-day period ends. It notifies the Customer as soon as reasonably possible, and the Customer may object as Section 6.3 provides, with the period counted from that notice.

7. Customer-enabled integrations and AI features

1. Some features send data to a service that the Customer chooses and configures, such as notification channels (email, Slack, Telegram, webhooks, PagerDuty and others), issue trackers, the Customer's own SAML or OIDC identity provider, the Customer's own AI model provider, and AI clients connected to the Uptrace MCP server. Uptrace sends data to these services on the Customer's instruction. They are not Uptrace Subprocessors, and the Customer is responsible for its relationship with them.
2. AI features, such as the assistant and incident analysis, are optional and off by default. A project administrator turns them on for a project by accepting an in-app data notice that describes the data sent to the AI model provider. Accepting the notice is the Customer's instruction to process that data with the AI model provider that Uptrace uses by default. That provider is one of the AI model providers listed in Annex III, which are Subprocessors. The Customer is responsible for ensuring that its project administrators are authorised to give this instruction.
3. Uptrace may change the default AI model provider to another provider listed in Annex III without a new acceptance of the notice, and tells the Customer on request which provider is in use. Adding a provider that Annex III does not list is a change of Subprocessor under Section 6.
4. Uptrace does not send data to an AI model provider for a project whose administrator has not accepted the notice. The Customer can withdraw its instruction at any time by turning the AI features off, or can use its own AI model provider instead under Section 7.1.
5. The AI model providers may process data outside the European Economic Area, in the countries Annex III states. The Customer decides, for each project, whether that processing is appropriate for the personal data in the project's telemetry.

8. International transfers

1. Uptrace is established in the Republic of Moldova. Customer Personal Data is stored and processed on servers in Germany and Finland. Uptrace personnel may access it from Moldova, and that access is a transfer of personal data to a third country.
2. Where the GDPR applies to a transfer of Customer Personal Data from the Customer to Uptrace, the SCCs are incorporated into this DPA by reference and apply as follows:
    - Module Two (controller to processor) applies where the Customer is a controller, and Module Three (processor to processor) applies where the Customer is a processor;
    - the Customer is the data exporter and Uptrace is the data importer;
    - Clause 7 (docking clause) is included;
    - in Clause 9(a), Option 2 (general written authorisation) applies, and the time period for prior notice is the one set out in Section 6.2;
    - the optional language in Clause 11(a) does not apply;
    - in Clause 13, the competent supervisory authority is the one determined under Clause 13(a) and Annex I.C;
    - in Clause 17, Option 1 applies, and the SCCs are governed by the law of Germany;
    - in Clause 18(b), disputes are resolved by the courts of Germany;
    - Annexes I, II and III of this DPA serve as Annexes I, II and III of the SCCs.
3. Where the UK GDPR applies to the transfer, the UK Addendum is incorporated into this DPA by reference and amends the SCCs as set out in it. Tables 1 to 3 of the UK Addendum are completed with the information in Section 8.2 and Annexes I to III. For Table 4, either party may end the UK Addendum as set out in its Section 19.

4. Where the FADP applies to the transfer, the SCCs apply with these changes: references to the GDPR are read as references to the FADP; the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for transfers governed by the FADP; and the term "Member State" is not read so as to exclude data subjects in Switzerland from suing for their rights in their place of habitual residence.
5. If Uptrace transfers Customer Personal Data to a Subprocessor in a third country that does not benefit from an adequacy decision, it does so under the SCCs (Module Three) or another transfer mechanism permitted by Data Protection Laws.
6. If the SCCs and any other part of this DPA or the Terms conflict, the SCCs prevail.

9. Requests from public authorities

1. If a public authority requests access to Customer Personal Data, Uptrace:
    - redirects the authority to the Customer where possible;
    - notifies the Customer promptly, unless the law prohibits notification, in which case Uptrace uses its best efforts to obtain a waiver of that prohibition;
    - assesses the lawfulness of the request and challenges it where there are reasonable grounds to consider it unlawful;
    - discloses only the minimum amount of data the request permits.
2. This Section supplements, and does not limit, Clause 15 of the SCCs.

10. Data subject requests

1. Taking into account the nature of the processing, Uptrace assists the Customer by appropriate technical and organisational measures in responding to requests from data subjects to exercise their rights under Data Protection Laws.

2. The Customer can handle most requests in the Services itself: it can query and export telemetry through the user interface and API, shorten retention periods, and remove attributes before storage with transform pipelines. Where the Customer needs Uptrace to delete specific Customer Personal Data that the Services do not let it delete, the Customer can ask support@uptrace.dev. Where the law allows, Uptrace may meet such a request by letting the data expire at the end of the retention period the Customer configured.
3. If Uptrace receives a request directly from a data subject about Customer Personal Data, it does not respond to it, other than to refer the data subject to the Customer, unless the Customer authorises it to.
4. Uptrace may charge the Customer its reasonable costs for assistance under this Section, and under Sections 1.6, 12 and 13, that goes beyond the self-service features of the Services and the information in Section 13.1.

11. Security Incidents

1. Uptrace notifies the Customer of a Security Incident without undue delay, and where feasible within 72 hours, after confirming it.
2. The notification describes, as far as the information is available:
    - the nature of the Security Incident, including the categories and approximate number of data subjects and records concerned;
    - the likely consequences of the Security Incident;
    - the measures Uptrace has taken or proposes to take to address it and to mitigate its possible adverse effects;
    - a contact point for more information.
3. Where Uptrace cannot provide all the information at once, it provides it in phases without undue delay.
4. Uptrace notifies the account owner by email. Notification is not an acknowledgement of fault or liability. The Customer, as controller, decides whether to notify supervisory authorities and data subjects, and gives those notices itself; Uptrace assists as GDPR Art. 28(3)(f) and Clause 8.6 of the SCCs require.

12. Data protection impact assessments

Taking into account the nature of the processing and the information available to it, Uptrace provides reasonable assistance to the Customer with data protection impact assessments and prior consultations with supervisory authorities that GDPR Arts. 35 and 36 require, to the extent they concern the Services.

13. Audits

1. Uptrace makes available to the Customer the information necessary to demonstrate compliance with this DPA and GDPR Art. 28, including written answers to reasonable security questionnaires and a description of its security measures.
2. Uptrace does not currently hold third-party security certifications such as SOC 2 or ISO/IEC 27001. Its hosting provider's datacenters are ISO/IEC 27001 certified. Once Uptrace holds such a certification, or a report of an independent auditor such as a SOC 2 Type II report, it may meet Section 13.1 by making it available.
3. If the information under Section 13.1 is not enough to demonstrate compliance, or a supervisory authority requires it, the Customer may audit Uptrace, itself or through an independent auditor bound by confidentiality, no more than once in any 12 months, unless a Security Incident or a supervisory authority justifies another audit. The Customer gives at least 30 days' written notice, and the parties agree the scope, timing and duration in advance. Before the audit, the auditor signs a confidentiality agreement with Uptrace. The audit is carried out remotely, unless an on-site audit is needed to verify compliance, and lasts no more than one business day, unless the parties agree otherwise. Audits are carried out during business hours, without unreasonable disruption to Uptrace's operations, and without access to other customers' data. The auditor must not be a competitor of Uptrace. The Customer bears its own costs of the audit and reimburses Uptrace's reasonable costs, as Section 10.4 provides.

4. Information Uptrace provides under this Section, including answers to security questionnaires and audit results, is Uptrace's Confidential Information under Section 14 of the Terms. The Customer uses it only to verify compliance with this DPA, and may disclose it only to its auditors, its advisers and supervisory authorities.
5. Audits do not extend to the facilities or systems of Subprocessors. For a Subprocessor, Uptrace's obligations under this Section are met by the Subprocessor's certifications, audit reports or other information it makes available, such as the ISO/IEC 27001 certification of the hosting provider's datacenters.

14. Return and deletion

1. During the term, the Customer can export Customer Personal Data through the user interface and API of the Services.
2. When the Customer's account is cancelled or terminated, Customer Personal Data becomes inaccessible in the Services. Uptrace deletes it from active systems within 30 days and from backups within 60 days, unless the law to which Uptrace is subject, or an order of a public authority, requires Uptrace to keep it. In that case, Uptrace continues to protect the data as this DPA requires, and processes it only to the extent and for as long as that law or order requires. The Customer exports the Customer Personal Data it wants to keep before it cancels its account (Section 14.1): the data is not available after the account ends, and Uptrace does not return it. This is the Customer's choice of deletion under GDPR Art. 28(3)(g) and Clause 8.5 of the SCCs.
3. On the Customer's written request, Uptrace certifies the deletion in writing.

15. US state privacy laws

To the extent the CCPA or a similar US state privacy law applies, Uptrace is a "service provider" or "processor" for Customer Personal Data. Uptrace does not sell or share Customer Personal Data; does not retain, use or disclose it for any purpose other than the business purposes set out in the Terms and this DPA; does not retain, use or

disclose it outside the direct business relationship with the Customer; and does not combine it with personal data it receives from other sources, except as those laws permit. Uptrace notifies the Customer if it can no longer meet its obligations under those laws.

16. Liability and order of precedence

1. Each party's liability arising out of or related to this DPA is subject to the limitations of liability in the Terms, except as Section 2.6 provides. Liability under this DPA and under the Terms counts towards one aggregate limit, not separate limits. Nothing in this DPA or the Terms limits a party's liability to data subjects under Clause 12 of the SCCs or GDPR Art. 82, or any other liability, to the extent that the SCCs or Data Protection Laws do not allow it to be limited.
2. If the documents conflict on the processing of Customer Personal Data, the following order of precedence applies: first the SCCs and the UK Addendum, then this DPA, then the Terms. On all other matters, the Terms prevail.

17. Term, changes and governing law

1. This DPA takes effect when the Customer accepts the Terms or signs this DPA, whichever comes first. It remains in force for as long as Uptrace processes Customer Personal Data for the Customer, and Sections that by their nature should survive, such as Section 14, survive its end.

2. Uptrace may update this DPA to reflect changes in Data Protection Laws or in the Services, and updates Annex III as described in Section 6. An update does not reduce the protection of Customer Personal Data under this DPA. Uptrace notifies the account owner by email at least 30 days before a new version takes effect. Where a Customer has signed this DPA, the new version applies to that Customer when it takes effect. If the new version materially and adversely affects the Customer's rights under this DPA, the Customer may object in writing before it takes effect, stating how it does so. If the parties cannot resolve the objection, the Customer may terminate the affected Services before the new version takes effect, as Section 17.4 provides. Updates to Annex III under Section 6, and changes Data Protection Laws require, need no new version.
3. This DPA is governed by the law, and subject to the jurisdiction of the courts, that govern the Terms. The SCCs are governed by the law, and disputes under them are resolved by the courts, that Section 8.2 sets out.
4. Termination is the Customer's only remedy for an objection under Section 6.3 or 17.2. On such a termination, fees for usage up to termination remain due, and fees already paid, including any prepayment, are not refunded, as Section 5.9 of the Terms provides. The termination ends, without penalty, any remaining minimum term or commitment in a signed order form for the terminated Services.

Signatures

	Customer	Uptrace
Company		UPTRACE DEV S.R.L.
Address		str. Ion Nistor 2, ap. 50, mun. Chișinău, MD-2009, Republic of Moldova
Name		Vladimir Mihailenco
Title		Administrator
Authority	The signatory represents that they are authorised to bind the Customer.	The signatory represents that they are authorised to bind Uptrace.
Date		
Signature		

A copy signed in Uptrace Cloud has both parties' entries written into this table, and a Signature record page at its end states them in full. In a copy signed by hand, each party fills in and signs its own column.

Annex I: Description of processing

A. List of parties

Data exporter: the Customer, as identified in its Uptrace account or in the Signatures section.

- Role: controller, or processor where the Customer processes personal data for its own clients.
- Activities: use of the Services to collect, store and analyse telemetry from the Customer's systems.
- Contact person: the account owner of the Customer's Uptrace organisation, or the signatory above.

Data importer: UPTRACE DEV S.R.L.

- Address: str. Ion Nistor 2, ap. 50, mun. Chișinău, MD-2009, Republic of Moldova.
- Company registration number (IDNO): 1024606007235. VAT number: 0310552.
- Contact person: Vladimir Mihailenco, Administrator, support@uptrace.dev.
- Role: processor, or subprocessor where the Customer is a processor.
- Activities: providing the Services.

B. Description of the transfer

Item	Description
Categories of data subjects	The Customer's end users, employees, contractors and other individuals whose data appears in the telemetry the Customer sends; the Customer's users of the Services.
Categories of personal data	Whatever the Customer chooses to include in telemetry, typically IP addresses, user and session identifiers, user names and email addresses, URLs, request parameters, device and browser data, and free-text log messages. Names and email addresses of people who receive alert notifications.

Item	Description
Sensitive data	None. The Customer must not send special categories of personal data or the other prohibited data in Section 4.2 of the Terms, and must keep them out with transform pipelines or its instrumentation (Section 2.4). The safeguards in Annex II apply to all Customer Personal Data.
Frequency of the transfer	Continuous, for as long as the Customer sends telemetry to the Services.
Nature of the processing	Receiving, buffering, transforming as the Customer configures, storing, indexing, querying, aggregating, displaying, alerting on and deleting telemetry.
Purpose of the processing	Providing the Services to the Customer: application performance monitoring, distributed tracing, metrics, logs, alerting and related features; and answering the Customer's support requests, including about the Licensed Software (Section 2.5).
Retention	For the retention period the Customer configures for each project and signal: 28 days by default, and up to 100 weeks for paid accounts. After cancellation, deletion follows Section 14.
Transfers to Subprocessors	As listed in Annex III, for the purposes and duration stated there.

C. Competent supervisory authority

The supervisory authority determined under Clause 13(a) of the SCCs: where the data exporter is established in an EU Member State, the supervisory authority of that Member State; otherwise, the authority determined under Clause 13(a). For transfers governed by the UK GDPR, the UK Information Commissioner's Office. For transfers governed by the FADP, the Swiss Federal Data Protection and Information Commissioner.

Annex II: Technical and organisational measures

Hosting and physical security

- All servers and storage that hold Customer Personal Data are dedicated servers rented from Hetzner Online GmbH and located in Hetzner datacenters in Germany and Finland.
- Physical security, power, cooling and network redundancy are provided by Hetzner, whose datacenters are ISO/IEC 27001 certified.

Encryption

- Connections from the public internet to the Services, including the user interface, API and ingestion endpoints, are encrypted with TLS.
- Disks and databases that store Customer Personal Data are encrypted at rest.
- Database backups are encrypted.
- User passwords are stored as bcrypt hashes. API tokens are shown masked in the user interface.

Access control in the Services

- Role-based access control at the organisation level (owner, admin, member, viewer, billing manager, collaborator) and at the project level (none, view, edit, admin), with teams and per-user overrides.
- Single sign-on through SAML and OIDC, with an organisation-wide option to require it.
- Time-based one-time password (TOTP) two-factor authentication with recovery codes.
- Rate limiting of sign-up, sign-in and other unauthenticated endpoints.

Personnel access

- Production access is limited to Uptrace personnel who need it to operate the Services.
- Personnel access to a customer's account is used only for the purposes in Section 4.2.
- All personnel are bound by confidentiality obligations.

Tenant isolation

- Customer Personal Data is logically separated by organisation and project. Every query the Services run is scoped to the projects the requesting user or token is authorised for.

Availability and resilience

- Telemetry in ClickHouse is stored in two replicas.
- Incoming telemetry is buffered in Kafka before it is written to storage.
- The PostgreSQL database, which holds accounts, projects, dashboards and alert settings, is backed up regularly. Backups are encrypted.
- Uptrace monitors the Services with Uptrace itself and is alerted to failures.

Data minimisation and deletion

- Customers configure retention per project and signal. A daily retention sweep permanently deletes telemetry older than the configured retention period.
- Customers can delete, rename or keep only selected attributes before telemetry is stored, using transform pipelines.
- Ingestion limits cap the length and number of attributes in each record.

Application security

- Server-side requests to customer-supplied URLs, for example webhooks and source map downloads, are protected against server-side request forgery by default.
- Uptrace fixes security issues reported to it as a priority.

Annex III: Subprocessors

Subprocessor	Purpose	Customer Personal Data processed	Location	Transfer mechanism
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting of all servers and storage	All Customer Personal Data	Germany and Finland	Not a transfer (EEA)
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg (Amazon SES)	Delivery of email, including alert notifications	Recipients' names and email addresses; content of alert emails	Germany (AWS region eu-central-1)	Not a transfer (EEA)
Anthropic, PBC, San Francisco, California, United States (Anthropic API)	AI features, such as the assistant and incident analysis, when it is the default AI model provider (Section 7.2)	Only for projects whose administrator accepted the in-app data notice: alerts, incidents, questions, and the telemetry the AI features read	United States	SCCs, Module Three, in Anthropic's Data Processing Addendum

Subprocessor	Purpose	Customer Personal Data processed	Location	Transfer mechanism
OpenAI OpCo, LLC, 1455 3rd Street, San Francisco, CA 94158, United States (OpenAI API)	AI features, such as the assistant and incident analysis, when it is the default AI model provider (Section 7.2)	Only for projects whose administrator accepted the in-app data notice: alerts, incidents, questions, and the telemetry the AI features read	United States	SCCs, in OpenAI's Data Processing Addendum. OpenAI Ireland Limited processes EEA and Swiss data, and transfers it outside the EEA under SCCs
OpenRouter, Inc., 169 Madison Ave #2404, New York, NY 10016, United States (OpenRouter API)	AI features, such as the assistant and incident analysis, when it is the default AI model provider (Section 7.2). OpenRouter passes each request to the provider that hosts the selected model	Only for projects whose administrator accepted the in-app data notice: alerts, incidents, questions, and the telemetry the AI features read	United States, and the country where the provider that hosts the selected model processes the request	SCCs, in OpenRouter's Data Processing Agreement, which its Terms incorporate

Not Subprocessors. These services receive personal data as independent controllers or at the Customer's own choice, and are not Subprocessors under this DPA:

- Paddle.com Market Limited (United Kingdom) acts as merchant of record and processes payment and billing data as an independent controller.
- Google LLC and GitHub, Inc. receive sign-in data only when a user chooses to sign in with a Google or GitHub account.
- Services the Customer connects under Section 7.1, such as notification channels and issue trackers.
- Gravatar, operated by Automattic Inc. (United States). To show a user's avatar, the viewer's browser sends Gravatar a hash of that user's email address. This is account data that Uptrace controls (Section 2.2), not Customer Personal Data.