GRAPHPILOT

WE FLY THE COMPLEXITY SO YOU DON'T HAVE TO

GRAPHPILOT LEGAL TEXTS

Privacy Policy

Information on the processing of personal data under Art. 13 and 14 GDPR

Provider	GraphPilot UG (haftungsbeschränkt) Arcadiastraße 18 40472 Düsseldorf Germany
Version	1.0
Language	English (translation for information) The German version is binding.
Date	**30 October 2026**

1. Data Controller (hereinafter: “we”)

GraphPilot UG (haftungsbeschränkt)
Arcadiastraße 18
40472 Düsseldorf

represented by the managing director:
Mr. Kay Schecker, contact information as above

Contact Form: https://graphpilot.io/contact
Email: info@graphpilot.io

For more details about us, please see our legal notice (imprint): https://graphpilot.io/legal/imprint.

2. Personal Data, Purposes of Processing, and Legal Bases

Personal data refers to any information relating to an identified or identifiable natural person. We process personal data to the extent necessary to provide the website, the customer portal, the command-line application, and the GraphPilot platform; to manage user accounts and organizations; to provide and manage services and their configuration; to provide analyses of queries, errors, and runtime data (“Insights”); to process subscriptions and billing, to handle inquiries, and to ensure the security and stability of our platform.

Depending on the specific purpose of processing, the processing is carried out on the basis of Art. 6(1)(b) of the GDPR to fulfill the user agreement or to take pre-contractual measures, on the basis of Art. 6(1)(f) GDPR to safeguard our legitimate interests in the secure, stable, and functional operation of GraphPilot, or, where necessary, on the basis of your consent pursuant to Art. 6(1)(a) GDPR.

To the extent that we process personal data transmitted via a service set up by a customer, in particular requests from the customer’s end users and responses from the customer’s backend, we process this data on behalf of the customer and in accordance with the data processing agreement concluded with the customer. In this case, the customer is the data controller under data protection law.

The specific details regarding the processing of your personal data are set forth in the following provisions:

3. Hosting, Database, Access Data, and Technical Logs

Cloudflare Inc.

We use the services of Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA (hereinafter “Cloudflare”) for the hosting and technical delivery of our website, documentation, and customer portal. In particular, Cloudflare processes technically necessary connection and access data generated when using the website, documentation, and customer portal. We also use Cloudflare for bot protection on forms via Cloudflare Turnstile. To the extent that Cloudflare processes personal data on our behalf, this is done on the basis of a data processing agreement in accordance with Article 28 of the GDPR. To the extent that personal data is transferred to Cloudflare in the United States or other third countries, or is accessed from there, the transfer is based on the European Commission’s adequacy decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. Cloudflare, Inc. is certified under the EU-U.S. Data Privacy Framework.

Google Cloud EMEA Ltd.

To provide GraphPilot, we use the services of Google Cloud EMEA Ltd., 70 Sir John Rogerson’s Quay, Dublin 2, Ireland (hereinafter “Google Cloud”). In particular, Google Cloud provides the platform API, background tasks, database, file storage, technical logs, access data and key management, and telemetry data storage. The platform API, database, and technical logs are operated in the europe-west1 region (Belgium); the telemetry data storage and backups are stored

within the EU. We also use Google Cloud's services to back up the data stored in GraphPilot. Telemetry data is not included in the database backups; it is retained in the telemetry data storage within the EU for a maximum of 90 days.

To the extent that Google Cloud processes personal data on our behalf, this is done on the basis of a data processing agreement in accordance with Article 28 of the GDPR. To the extent that personal data is transferred to Google LLC in the United States or accessed from there, the transfer is based on the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework in accordance with Article 45 of the GDPR. Google LLC is certified under the EU-U.S. Data Privacy Framework.

Fastly, Inc.

To operate the services set up by our customers and the platform API, we also use the services of Fastly, Inc., 475 Brannan Street, Suite 300, San Francisco, CA 94107, USA (hereinafter "Fastly"). Fastly operates the globally distributed edge network through which the GraphPilot proxy receives and checks requests, caches them where applicable, and forwards them to the respective customer's backend. In particular, the IP address, technical connection data, and, to the extent permitted by the customer's configuration, cached responses may be processed. Processing may take place at edge locations worldwide. To the extent that Fastly processes personal data on our behalf, this is done on the basis of a data processing agreement in accordance with Article 28 of the GDPR. To the extent that personal data is transferred to Fastly in the United States or other third countries, or is accessed from there, the transfer is based on the European Commission's Adequacy Decision for the EU-US Data Privacy Framework pursuant to Article 45 of the GDPR, as well as, supplementarily, on the EU Standard Contractual Clauses pursuant to Article 46(2)(c) of the GDPR. Fastly, Inc. is certified under the EU-U.S. Data Privacy Framework.

When using our website, documentation, customer portal, command-line application, and platform, technically necessary connection and access data may be processed. This may include, in particular, the IP address, date and time of access, the page or interface accessed, the amount of data transferred, HTTP status codes, the referrer URL, browser type and version, operating system, and information about the Internet service provider. To a limited extent, technical error, security, and system logs may be generated. These may contain the data mentioned above to the extent necessary for error analysis, for detecting and fending off abusive access, and for ensuring the security and stability of our information technology systems.

The processing of access data and technical logs is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure, stable, and functional provision of GraphPilot, as well as in the prevention of attacks and misuse. To the extent that the processing concerns data transmitted via a customer's API, it is carried out on behalf of the respective customer based on the data processing agreement concluded with that customer in accordance with Article 28 of the GDPR.

ClickHouse, Inc.

To analyze telemetry data in the "Insights" section, we use the services of ClickHouse, Inc., 20807 Stevens Creek Boulevard, Suite 310, Cupertino, CA 95014, USA (hereinafter "ClickHouse"). The analytics database is hosted in the europe-west4 region (Netherlands). ClickHouse Cloud performs backups of the analytics database every 24 hours. A backup is discarded 30 days after the most recent backup in its backup chain. Deleted data may therefore remain in backups for several days after it has been deleted from the production system. Access by ClickHouse support from countries outside the European Union cannot be completely ruled out. In particular, telemetry data regarding requests, errors, runtimes, and usage volumes is processed in the analytics database. To the extent that ClickHouse processes personal data on our behalf, this is done on the basis of a data processing agreement in accordance with Article 28 of the GDPR. To the extent that personal data is transferred to ClickHouse in the United States or accessed from there, the transfer is based on the European Commission's Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. ClickHouse, Inc. is certified under the EU-U.S. Data Privacy Framework.

Grafana Cloud

For operational monitoring, we use Grafana Cloud, operated by Raintank Inc. d/b/a Grafana Labs, 165 Broadway, 23rd Floor, New York, NY 10006, USA. In doing so, we process metrics regarding the number of requests per organization, service, and hour. Request records are not processed. This processing is carried out to ensure the stability, security, and functionality of GraphPilot based on Article 6(1)(f) of the GDPR. The transfer is based on the European Commission's Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. Grafana Labs is certified under the EU-U.S. Data Privacy Framework.

4. Cookies

To the extent that we use cookies or similar technologies on our website, in our documentation, or in the customer portal, these serve the technically necessary provision of GraphPilot, in particular for login, session management, application security, the storage of user settings, and the processing of orders. To the extent that the storage of or access to information on your device is strictly necessary for these purposes, this is done pursuant to Section 25(2) no. 2 TDDDG. To the extent that personal data is processed in this context, such processing is carried out in accordance with Section 2 of this Privacy Policy. If you object to audience measurement (Section 8), a note is stored in your browser's local storage at your request that switches off measurement for this browser; this is done pursuant to Section 25(2) no. 2 TDDDG.

In particular, the customer portal uses a session cookie for login, cookies to store settings for the display of the customer portal, and local storage for user-specific settings, such as the most recently selected service, the time zone, filter templates, the column layout, and the history of your own cache invalidations. During the ordering process, technically necessary cookies from the payment service provider Stripe may also be used, in particular for fraud prevention.

Details regarding the services we use for audience measurement and usage analysis, as well as the respective legal bases, can be found in Section 8 of this Privacy Policy.

5. User Account

A user account is required to use GraphPilot. When you register and set up a user account, we process, in particular, your name, your business email address, your affiliation with an organization, your role and permissions, as well as login and profile data. We also process evidence of acceptance of the Terms of Use and the Data Processing Agreement (AVV) and of the confirmation that GraphPilot is used as a business and not as a consumer, in particular the version of the Terms of Use and the AVV accepted in each case, the version of the confirmed text, the time and process of acceptance (creation of an organization or order), the access channel (customer portal, command-line application, or platform API), the user and organization IDs, as well as the email address stored with the identity provider and, if available, the user's name. Depending on the selected login method, this may also include a password hash, one-time codes, a profile picture, a language setting, and information regarding logins and sessions, in particular the time, login method, IP address, and browser identifier. User accounts may be assigned to multiple organizations.

To the extent that user accounts are created for employees or other users of an organization, we process the data provided by the organization for this purpose. In this case, this data originates from the organization to which the user is assigned.

To verify business status, we may process the VAT identification number, the company name, and other business data required for billing. If a VAT identification number is provided, we may verify its validity. The processing is carried out to establish and execute the user relationship based on Art. 6(1)(b) of the GDPR, as well as to prevent use by consumers based on Art. 6(1)(f) of the GDPR.

We process the data collected in connection with the user account to enable registration, login, administration of the user account and organizations, rights management, and the use of GraphPilot's features. To the extent that we process data of the contracting party or its contacts, this is done on the basis of Article 6(1)(b) of the GDPR, insofar as the processing is necessary for the performance of the user agreement. To the extent that we process data of additional

users added by an organization, the processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest consists in providing and managing the platform covered by the contract for the respective customer.

To the extent that the processing serves to ensure the security of the user account (in particular, the confirmation of the email address, the reset of passwords, and the prevention of unauthorized access), it is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure and functional provision of GraphPilot.

User accounts are authenticated and managed using WorkOS, a service provided by WorkOS, Inc., San Francisco, USA. To the extent that personal data is transferred to WorkOS in the United States or accessed from there, the transfer is based on the EU Standard Contractual Clauses pursuant to Article 46(2)(c) of the GDPR.

If you log in using a GitHub account, GitHub processes the data required as part of the login process. GitHub, Inc. is headquartered in the United States. To the extent that personal data is transferred to the United States or accessed from there, the transfer is based on the European Commission's Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. GitHub, Inc. is certified under the EU-U.S. Data Privacy Framework.

Where used, we also use WorkOS Radar to detect and prevent fraudulent or abusive login and registration attempts. In particular, IP addresses, browser identifiers, and email addresses may be processed in this context. Processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in preventing unauthorized access, fraudulent registrations, and other misuse of GraphPilot. The above information regarding WorkOS applies accordingly to processing by WorkOS and transfers to the United States.

6. Contact via Email, Contact Form, Support, and Sales

If you send us inquiries via email or the contact form, we process your information, including the contact details you provide, to handle your inquiry and in the event of follow-up questions. The legal basis is Article 6(1)(b) of the GDPR, insofar as the inquiry relates to the initiation or performance of a contractual relationship. In all other cases, processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest consists in processing the inquiries directed to us.

Contact Form

Messages sent via the contact form on the website or in the customer portal are processed via the GraphPilot platform hosted on Google Cloud and delivered to the Zoho mailbox via Resend. In particular, the following data is processed: name, email address, and the content of the message; in the case of a message from the customer portal, the organization and service identifiers are also processed.

Cloudflare Turnstile is used to protect against automated requests. Messages are not stored by Cloudflare. Proof of consent, including the IP address or browser identifier, is not stored.

The information in Sections 3 and 6 of this Privacy Policy also applies to processing by Google Cloud, Resend, Zoho, and Cloudflare.

Email and Support

To receive and process emails sent to the email addresses under our domains, in particular to info@graphpilot.io, we use the services of Zoho Corporation GmbH, Trinkausstraße 7, 40213 Düsseldorf, Germany (hereinafter "Zoho"). We also use Zoho to process support requests via Zoho Desk. To the extent that Zoho processes personal data on our behalf, this is done on the basis of a data processing agreement in accordance with Article 28 of the GDPR. Processing generally takes place in data centers within the European Union. However, access by Zoho's U.S. parent company or other subprocessors cannot be completely ruled out. To the extent that personal data is transferred to a third country or accessed from there, the transfer is based on the EU Standard Contractual Clauses pursuant to Article 46(2)(c) of the GDPR.

System Emails

To send system emails related to GraphPilot, we use the Resend service provided by Plus Five Five, Inc., 2261 Market Street #5039, San Francisco, CA 94114, USA (hereinafter “Resend”). In particular, we use Resend to send emails regarding the registration and management of user accounts, invitations, invoices, alerts, responses to inquiries, and other communications necessary for the use of GraphPilot. When sending emails, Resend processes, in particular, the recipient’s email address, sender information, the content of the email, and technical sending and delivery data.

Resend processes data in the United States. The transfer is based on the European Commission’s Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. Plus Five Five, Inc. is certified under the EU-U.S. Data Privacy Framework. Additionally, a data processing agreement has been entered into in accordance with Article 28 of the GDPR.

To the extent that we process email data to fulfill the contractual relationship with the contracting party or its contacts, this is done on the basis of Article 6(1)(b) of the GDPR. To the extent that we send system emails to other users within an organization, the processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure and functional provision of GraphPilot.

To the extent that emails contain content derived from data transmitted via the customer API, the processing is carried out on behalf of the respective customer. In this regard, the customer is the data controller under data protection law.

To the extent that we process technical sending and delivery data to ensure delivery, for error analysis, to prevent misuse, or to ensure the operation of GraphPilot, this is done on the basis of Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure, reliable, and traceable provision of GraphPilot’s email functions.

Sales and Customer Service

We also use Zoho CRM to manage sales contacts and provide customer support. In doing so, we process, in particular, the name, company, job title, business email address, phone number, meeting notes, quotes, and the history of communication with prospects and customers. This processing is carried out to implement pre-contractual measures and to fulfill the contractual relationship based on Article 6(1)(b) of the GDPR, as well as, in other respects, based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in maintaining business relationships and processing sales inquiries. The above information regarding Zoho applies accordingly to processing carried out by Zoho.

7. Usage Data, Activity Log, and Support

Usage Data

When using GraphPilot, we process data regarding the use of the customer portal, the command-line application, and the platform. This includes, in particular, information on features used, user actions, the timing and methods of logins, session data, the assignment of actions to users or API keys, as well as log data on security events and errors.

To the extent that we process this data to provide GraphPilot, to manage user accounts, organizations, services, and configurations, and to administer the user relationship, the processing is based on Article 6(1)(b) of the GDPR. To the extent that we process data of additional users added or invited by an organization, such processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest consists in providing and managing the platform covered by the contract for the respective customer.

To the extent that we process usage data for our own purposes (in particular for error analysis, to ensure IT security, and to prevent unauthorized access), this is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure and functional operation of GraphPilot.

Activity Log and API Keys

We log write operations in the customer portal and via the platform API. The activity log contains, in particular, information regarding which user, API key, support access, or system process performed an action, the time at which the action took place, the action performed, and the object affected. For users, the email address stored with the identity provider and, if available, the name may be processed. The activity log does not contain the content of requests, secrets (such as credentials or keys), or IP addresses.

For API keys, we process, in particular, their names, a truncated value, the owner, the permissions, and the times of creation, use, and deletion.

This processing is carried out for the performance of the user agreement pursuant to Art. 6(1)(b) of the GDPR, as well as to ensure the security of GraphPilot, to investigate misuse and fraud, and to provide evidence of actions pursuant to Art. 6(1)(f) of the GDPR. Our legitimate interest lies in the secure, traceable, and functional provision of GraphPilot.

Whether and to what extent activity logs can be viewed in the customer portal or via the platform API depends on the roles and permissions within the respective organization.

Authorized GraphPilot employees who are bound by confidentiality obligations may view activity logs to the extent necessary for support, security, the investigation of misuse or fraud, and the enforcement or defense of legal claims. In this regard, processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure, traceable, and functional provision of GraphPilot.

Support Access and Support Notes

To the extent necessary to process a support request, authorized GraphPilot employees who are bound by confidentiality obligations may access the functions used by the customer on behalf of a user. Every instance of support access is logged; in particular, the following information is stored: the person accessing the system, the affected customer, and the time of access, as well as the reason provided in the case of write access.

GraphPilot employees may maintain internal support notes in free text for billing accounts to the extent necessary to handle support, billing, or customer issues. Processing is based on Article 6(1)(b) of the GDPR and Article 6(1)(f) of the GDPR. Our legitimate interest lies in the traceable and efficient handling of customer inquiries. The notes are deleted along with the respective billing account.

Background Tasks

To perform background tasks, particularly in connection with billing, emails, alerts, and the delivery of configurations, we use the services of Inngest, Inc., San Francisco, USA (hereinafter “Inngest”). In particular, event data from Stripe and WorkOS may be processed, which may include names, email addresses, billing addresses, VAT identification numbers, masked payment method details, billing data, invitations, organization names, and domains. Processing is carried out, to the extent necessary for the performance of the user agreement, on the basis of Article 6(1)(b) of the GDPR, and, in all other respects, to ensure the secure and functional operation of GraphPilot on the basis of Article 6(1)(f) of the GDPR. To the extent that personal data is transferred to Inngest in the United States or accessed from there, the transfer is based on the EU Standard Contractual Clauses pursuant to Article 46(2)(c) of the GDPR.

To the extent that data from end users of the customer API is processed when using the services set up by a customer (in particular, telemetry data regarding requests, errors, runtime, and service usage), such processing is carried out on behalf of the respective customer. In this regard, the customer is the data controller under data protection law.

8. Consent Management and Web Analytics

Consent Management

On our website, in the documentation, and in the customer portal, we use the CCM19 service provided by Papoo Software & Media GmbH, Auguststraße 4, 53229 Bonn, Germany, to manage your consents. CCM19 stores your choices to give, refuse or withdraw consent. Processing is carried out, to the extent necessary for storing your consent, on the basis of Art. 6(1)(c) of the GDPR in conjunction with Art. 7(1) of the GDPR and Section 25(2) no. 2 TDDDG. You may withdraw any consent you have given at any time with effect for the future via the consent management settings, which are accessible in the footer of the website (Art. 7(3) of the GDPR). Audience measurement with Plausible is not controlled through the consent management; the right to object described in the following section applies to it.

Audience Measurement with Plausible Analytics

On the website and in the documentation, reach is evaluated statistically with Plausible Analytics provided by Plausible Insights OÜ, Västriku tn 2, 50403 Tartu, Estonia (hereinafter “Plausible”). Plausible sets no cookies and, unless you object, stores nothing on your device. When a page is opened, the following are processed: the page address (without query parameters other than campaign tags), the referring page, browser, operating system and device type (derived from the browser identifier), the approximate location (country, region, city, derived from the IP address), and usage details such as time on page and scroll depth. The IP address and browser identifier are not stored; together with a random value that changes daily, they are used to form an identifier that only groups visits on the same day. The random value is deleted every 24 hours. The data is transmitted to Plausible through a forwarding service at a graphpilot.io address run on Cloudflare; the information in Section 3 of this Privacy Policy also applies to processing by Cloudflare.

The legal basis is Art. 6(1)(f) of the GDPR. The legitimate interest lies in statistically evaluating the reach and use of the website and the documentation and in improving these offerings. Plausible processes the data on our behalf on the basis of a data processing agreement pursuant to Art. 28 of the GDPR; the data is stored within the European Union.

Objection: You may object to audience measurement at any time (Art. 21(1) of the GDPR). The toggle in the Privacy Policy on the website (https://graphpilot.io/legal/privacy) or in the footer of the documentation stores a note in your browser that switches off measurement of the respective website for this browser. The note contains no personal data. If you delete your browser’s site data, the note is removed and measurement resumes.

9. Routed Data and Telemetry Data

In connection with the use of GraphPilot, we process data that is transmitted via the services set up by our customers. These include, in particular:

Request and telemetry data: End-user IP address, timestamp, request ID, information about the device, browser, location, network, and Internet service provider, selected request and response headers, path, hostname, status codes, response times, size information, cache status, request bodies, error messages from the customer’s backend, and object identifiers, to the extent that these are used as cache keys. The storage of the end user’s IP address depends on the customer’s settings. The customer can specify whether IP addresses are stored in full, truncated, or not at all. GraphQL variables are never stored in plain text, but only as pseudonymous hash values. By default, credentials in headers and Vary values are not stored in plain text, but only as pseudonymous hash values. The customer can explicitly configure storage of these data in plain text.

Cached data: complete responses from the customer’s backend, including their content and headers, to the extent that the customer permits this in its caching rules or the customer’s backend permits this in the response headers. Non-public responses are stored separately by user, organization, or role, in accordance with the customer’s configuration.

This data is processed on behalf of the respective customer using GraphPilot. The customer is the data controller under data protection law and determines the legal basis for the processing. GraphPilot processes this data exclusively in accordance with the data processing agreement concluded with the customer.

Depending on the subscribed plan, telemetry data is generally stored for a period of one, seven, 30, or at most 90 days. Responses from the customer’s backend are cached only until the expiration of the validity period specified by the

customer, until they are invalidated, or until the respective service is deleted. Details regarding the retention periods are set forth in the data processing agreement.

10. Communication, Alert, and Notification Data

In connection with the use of GraphPilot, we process data related to invitations, system emails, alerts, notifications in the customer portal, and alert channels. This includes, in particular, the email addresses of additional recipients, any webhook URLs used, the content of the respective notification, the time of sending, and information regarding delivery and processing.

If an additional email address is added as an alert channel, this address first receives a confirmation email. Alerts are sent to the address only after the link in this email has been confirmed; an address that is not confirmed within seven days is removed. Every email to such an address contains a link with which the recipient can remove the address without logging in. The status of the confirmation and its time are stored, as well as hash values of the links, not the links themselves. Processing is carried out on the basis of Art. 6(1)(f) of the GDPR; the legitimate interest lies in sending alerts only to recipients who have confirmed them and in preventing misuse of alert delivery.

Processing is carried out, to the extent necessary for the provision of the agreed-upon functions and the performance of the user agreement, on the basis of Art. 6(1)(b) of the GDPR. To the extent that we process data of additional recipients added by an organization, the processing is carried out on the basis of Art. 6(1)(f) of the GDPR. Our legitimate interest lies in the secure, traceable, and functional provision of GraphPilot.

11. Contract and Billing Data

In connection with the conclusion and performance of contracts regarding GraphPilot, we process the data of our contractual partners and their contacts. This includes, in particular, name, company name, business address, business contact and communication details, VAT identification number, contract data, subscribed plans, contract terms, terminations, usage volumes, as well as billing and payment data. To provide evidence of the conclusion of the contract and the inclusion of the Terms of Use and the Data Processing Agreement (AVV), we also process the evidence of acceptance in accordance with Section 16 of this Privacy Policy. The processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in defending against and enforcing legal claims.

The processing is carried out for the purpose of initiating, concluding, and executing the contractual relationship on the basis of Article 6(1)(b) of the GDPR. To the extent that we process contract and billing data to fulfill statutory retention and documentation obligations, this is done on the basis of Article 6(1)(c) of the GDPR.

Stripe

To process payments, subscriptions, invoices, and taxes, we use the services of Stripe Payments Europe, Limited, and Stripe Technology Europe, Limited, both located at 1 Grand Canal Street Lower, Grand Canal Dock, Dublin 2, Ireland (hereinafter collectively “Stripe”). Stripe processes, in particular, name, address, email address, VAT identification number, payment data, invoice amount, payment status, usage volumes, and technical transaction data. Complete card and account data are processed exclusively by Stripe; we receive only masked information regarding the payment method.

Stripe processes payment data in the context of payment processing as an independent controller. To the extent that Stripe processes personal data in the United States, the transfer is based on the European Commission’s Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. Stripe, Inc. is certified under the EU-U.S. Data Privacy Framework. In addition, the EU Standard Contractual Clauses pursuant to Article 46(2)(c) of the GDPR apply.

In addition, we may transfer contract, billing, and payment data to financial institutions, accounting service providers, and tax advisors to the extent necessary for payment processing, bookkeeping, tax consulting, or to fulfill legal

obligations. Processing is based on Article 6(1)(b) of the GDPR and Article 6(1)(c) of the GDPR.

12. Status Page and Outage Notifications

To provide our public status page at graphpilot.instatus.com and to monitor the availability of our services, we use the services of Instatus, Inc., Beaverton, Oregon, USA (hereinafter “Instatus”). When you access the status page, Instatus processes, in particular, your IP address and technical information about your browser. If you sign up for notifications about outages or maintenance work, Instatus also processes your email address.

This processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in providing transparent information about the operational status of GraphPilot and in monitoring the availability of our services. To the extent that you expressly subscribe to outage notifications, the processing of your email address is additionally based on Article 6(1)(a) of the GDPR. To the extent that personal data is transferred to Instatus in the United States or accessed from there, the transfer is based on the EU Standard Contractual Clauses pursuant to Article 46(2)(c) of the GDPR.

13. Map View in the Customer Portal

In the customer portal, you can explicitly activate the map view for a request by clicking “Load Map.” For this purpose, we use the services of the OpenStreetMap Foundation, St. John’s Innovation Centre, Cowley Road, Cambridge, United Kingdom (hereinafter “OpenStreetMap”). When you activate the map view, your browser establishes a direct connection to OpenStreetMap’s servers. In particular, your IP address and the coordinates required for the map view are processed.

This processing is based on Article 6(1)(b) of the GDPR, to the extent that the map view is provided at your express request within the scope of the user relationship. OpenStreetMap processes the data as an independent controller. Data processing may take place in the United Kingdom and, due to the global delivery of map tiles, in other countries as well. To the extent that the coordinates used for the map view pertain to a customer’s end users, the respective customer remains responsible under data protection law for the lawfulness of the processing of this data.

14. Command-Line Application

We use the services of GitHub, Inc., San Francisco, USA (hereinafter “GitHub”) for the download, installation, and update checks of our command-line application “gpilot.” When downloading the command-line application and when checking for available updates, GitHub may, in particular, process the user’s IP address.

This processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the secure provision, updating, and technical development of the command-line application. To the extent that personal data is transferred to GitHub in the United States or accessed from there, the transfer is based on the European Commission’s Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article 45 of the GDPR. GitHub, Inc. is certified under the EU-U.S. Data Privacy Framework.

15. Appointment Booking

When you book an appointment via our website or documentation, we use the services of Cal.com, Inc., San Francisco, USA (hereinafter “Cal.com”). In doing so, Cal.com processes, in particular, your name, your email address, the selected appointment, and, if applicable, any message you submit.

This processing is carried out to implement pre-contractual measures or to fulfill a contractual relationship based on Article 6(1)(b) of the GDPR. To the extent that the appointment booking is not related to an existing or intended contractual relationship, the processing is based on Article 6(1)(f) of the GDPR. Our legitimate interest lies in the efficient coordination of appointments with prospects and customers.

To the extent that personal data is transferred to Cal.com in the United States or accessed from there, the transfer is based on the European Commission’s Adequacy Decision for the EU-U.S. Data Privacy Framework pursuant to Article

45 of the GDPR. Cal.com, Inc. is certified under the EU-U.S. Data Privacy Framework.

16. Retention Period

We delete your data as follows:

Data Category	Retention Period	Purpose
User account and registration data, including name, business email address, organizational affiliation, roles, and permissions	Until the user account is deleted	Registration, login, rights management, and provision of GraphPilot
Logins and sessions	Until the user logs out, the session is invalidated by the server, or the session automatically expires	Login and Secure Use of GraphPilot
Organizations, services, and configurations, including schemas, deployments, domains, and request documents	Until the respective service, organization, or user account is deleted; upon termination of the entire contractual relationship, retained for up to 30 more days for data handover	Provisioning and management of the platform and services
Platform API telemetry, in particular calls from the customer portal and command-line application	Up to 90 days	Operation, troubleshooting, and security of the Platform API
Platform API cache	Depending on the data category, a few minutes to approximately 37 days; invalidated upon changes	Accelerated data delivery in the customer portal
Platform operation logs	30 days	Troubleshooting, IT security, and detection of malfunctions
Evidence of acceptance of the Terms of Use and the Data Processing Agreement (AVV)	The following are stored: the respective version of the Terms of Use and the Data Processing Agreement (AVV), the acceptance process, the date and time, the access channel (customer portal, command-line application, or platform API), the user's and organization's identifiers, the billing account, confirmation of business status when creating an organization and when placing an order, together with the version of the confirmed text, as well as the email address on file with the identity provider and, if available, the user's name. These records are retained even after a user account or organization is deleted; upon deletion of the billing account, the link to it is removed. Deletion occurs at the end of the third calendar year following the year in which the billing account was deleted.	Proof of the conclusion of the contract and the inclusion of the Terms of Use and the Data Processing Agreement; Art. 6(1)(f) GDPR; Art. 17(3)(e) GDPR

Note regarding the deletion of the billing account	Evidence of acceptance is retained until the end of the third calendar year following the year in which the billing account was deleted.	The records of your acceptance of the Terms of Use (email address, name, date and time, version) will not be deleted. GraphPilot retains them as proof of the conclusion of the contract and deletes them at the end of the third calendar year following the year in which your billing account was deleted.
Activity Log in the Account	Entries visible to customers: Glider 1 day, Jet 30 days, Airliner 180 days, Jumbo 365 days. Entries regarding actions taken by GraphPilot support, as well as entries not visible to the customer: 365 days. Deletion occurs daily. If the organization is deleted, the entries are deleted immediately. If a user is deleted, the entries remain until the respective retention period expires; the name and email address are replaced with “Deleted user.”	Audit trails, rights management, security, support, and prevention of abuse and fraud
API keys	Until the API key or the organization is deleted	Authentication, access control, security, and traceability of access to the platform API
Support access log	365 days; immediately upon deletion of the organization or billing account	Verification and monitoring of support access on behalf of a user
Internal support notes regarding billing accounts	Until the respective billing account is deleted	Processing of support, billing, and customer issues
Blocklist of deleted users and organizations	Hash values of deleted user and organization identifiers: 365 days. Hash value of the email address: 90 days after the last deletion. Deletion requests: until the deletion is complete.	Ensuring that events arriving late do not reassign or restore a deleted user or organization; technical implementation of the deletion
Hostname label of a deleted organization with the organization’s identifier	Indefinitely	Ensuring that the label is not reassigned and that hostnames cannot be taken over (Art. 6(1)(f) of the GDPR)
Data from contact requests	Until the request is fully processed; if the request concerns business correspondence, six years from the end of the calendar year in which the correspondence was generated	Processing of inquiries and communication
Support requests and business correspondence	Six years from the end of the calendar year in which the correspondence was generated, to the extent that statutory retention obligations apply	Support, communication, and compliance with commercial and tax law retention obligations
Sales contacts, quotes, and meeting notes	Until the purpose of processing no longer applies; quotations and business letters, however, for six years from the end of the calendar year in which they were created	Sales and customer service
System emails and technical sending and delivery data	In accordance with the deletion periods of the service provider Resend, to the extent that no statutory retention obligations preclude this	Sending, verification, and technical traceability of emails
Contract data, contract history, and business correspondence	Six years from the end of the calendar year in which the contract ends or the correspondence is generated, unless longer retention is required in individual cases	Contract processing, documentation, and compliance with commercial and tax law retention obligations

Invoices, invoice data, and accounting documents	Eight years from the end of the calendar year in which the invoice or accounting document is generated	Compliance with tax and commercial law retention obligations
Usage volumes and usage meters	Eight years from the end of the calendar year in which the data was generated, even after an account or organization has been deleted	Billing and billing records
Masked information regarding payment methods, payment status, and billing data on Stripe	In accordance with statutory retention periods and Stripe's deletion schedules	Processing of payments, subscriptions, invoices, and taxes
Telemetry data from customers' services, in particular request records, log lines, and cache invalidations	Depending on the pricing plan, generally one day, seven days, 30 days, or a maximum of 90 days	Provision of insights, troubleshooting, support, and evidence in the event of complaints
Service history after reset by an authorized administrator	Associated request data, cache invalidations, and resolved alert events are deleted early. Billing counters, raw telemetry in the telemetry data store, and backup copies remain stored until the respective retention periods expire.	Premature deletion of service history at the customer's request
Raw telemetry in the telemetry data store	No more than 90 days; even after a service, organization, or account has been deleted	Technical processing and restoration of the analytics database
Raw telemetry in the analytics database	Up to three days; one day for the Glider plan	Technical processing of telemetry data
Backups of the analytics database on ClickHouse Cloud	Backups are created every 24 hours. A backup is discarded 30 days after the most recent backup in its backup chain; therefore, deleted data may remain in backups for a few days longer.	Restoration of the analytics database following technical issues or data loss
Error groups and filter suggestions based on telemetry data	Depending on the plan you've subscribed to: one day for the Glider plan, seven days for the Jet plan, 30 days for the Airliner plan, and individually for the Jumbo plan, up to a maximum of 90 days	Overview and filtering in the Insights section
Operational metrics	Minute-by-minute and hourly values for up to eight days; daily summaries for up to 13 months	Monitoring, Alerts, and Status Display
Cached responses from the customer backend	Until the expiration of the validity period specified by the customer, until invalidation, or until the service is deleted; responses may be evicted from the cache earlier	Acceleration of API requests and reduction of backend load
Edge data of a service, in particular request documents, public keys, and signing keys	As long as the service exists, or until revoked or cleaned up	Operation of the GraphPilot proxy
Client IP addresses at Fastly	Typically up to two working days (Werktage); up to seven days in the event of transmission errors, and potentially longer in the event of security incidents	Operation and security of the edge network
Alert channels, alert rules, and alert events	Until the respective organization or configuration is deleted; recipient addresses until the user account or organization is deleted	Sending and management of alerts

Confirmation of additional alert recipients	Status and time of confirmation until the alert channel is deleted; hash value of the confirmation link until it expires after seven days; hash value of the removal link until it expires after 180 days; in each case no later than the deletion of the alert channel	Proof of confirmation by the recipient, unsubscribing without logging in, protection against misuse
Evidence of consent	Until consent is withdrawn and beyond, as long as this is necessary to prove valid consent	Record-keeping and management of consents
Data from visitors to the status page and subscribers to outage notifications	In accordance with the retention periods of the service provider Instatus; email subscriptions until unsubscription	Provision of the status page and sending of outage notifications
Data from appointment bookings	In accordance with the retention periods of the service provider Cal.com, to the extent that no statutory retention requirements preclude this	Coordination of appointments with prospects and customers
Backups of platform data	35 days	Recovery following data loss and technical malfunctions
Deleted data in backups	Up to 35 days after deletion in the production system	Recovery following data loss and technical malfunctions

We also review at least once a year whether the storage of personal data is still necessary and delete data as soon as the respective purpose no longer applies and there are no legal retention requirements or overriding legitimate interests that preclude further storage.

An authorized administrator can reset the history of a service in the customer portal ahead of schedule. This deletes the associated request data, cache invalidations, and resolved alert events. Billing counters, raw telemetry in the telemetry data store, and backup copies remain stored until the applicable retention periods expire.

17. Rights of Data Subjects

You are not legally obligated to provide your personal data. However, providing such data may be necessary for entering into a contract or for certain platform functions. If you do not provide this data, a contract or a platform function may not be available.

There is no automated decision-making, and no profiling takes place.

The rights of data subjects arise in particular from Articles 15 through 23 and Article 77 of the GDPR, as well as from Sections 32 through 37 of the Federal Data Protection Act (BDSG).

With regard to your personal data, you have the right to

- **access**, Art. 15 GDPR
- **Rectification**, Art. 16 GDPR
- **Erasure**, Art. 17 GDPR
- **Restriction of processing**, Art. 18 GDPR
- **Data portability, Art. 20 GDPR.**

If you have given consent to the processing of personal data, you have the right of

- **withdrawal, Art. 7(3) GDPR**

with effect for the future.

You also have the right to

□ object to the processing of personal data (objection, Art. 21 GDPR)

.
1. You have the right, for reasons arising from your particular situation, to object at any time to the processing of personal data concerning you that is carried out pursuant to Article 6(1)(f) of the GDPR (data processing based on a balancing of interests).
If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or the processing is necessary for the establishment, exercise, or defense of legal claims.
2. In certain cases, we process personal data for direct marketing purposes. If this applies to you, you have the right to object at any time to the processing of your personal data for such marketing purposes.
If you object to processing for direct marketing purposes, we will no longer process your personal data for these purposes.
The objection may be made in any form and should, if possible, be directed
to us; see section 1 above.

If you believe that the processing of your personal data violates data protection law, you always have the

- **right to lodge a complaint**

with the competent supervisory authority, see Art. 77 of the GDPR. Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work, or the location of the alleged infringement, if you believe that the processing of your personal data violates the GDPR.

You can find the contact details of the data protection commissioners of the federal states, the supervisory authorities for the non-public sector, the data protection officers for broadcasting and the churches, the authorities in Europe and in other countries, and the Virtual Data Protection Office here:
https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

The supervisory authority responsible for us is the State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia, Kavalleriestraße 2–4, 40213 Düsseldorf.