



Privacy Policy – Platform

(Last updated: July 2025)

Sunhat GmbH (hereinafter "we" "us" "our") is pleased that you are visiting our platform <https://sunhat.app/> (hereinafter "platform"). Data protection and data security when using our platform are very important to us. We would therefore like to take this opportunity to inform you about the personal data we collect from you when you visit our platform and the purposes for which it is used.

Our guiding principle is to collect only what we need and that we will solely process this information to provide you with the service you signed up / requested for.

§ 1 Responsible / Controller

The controller within the meaning of the General Data Protection Regulation (hereinafter "GDPR") for the data processing of personal data on our platform is

Sunhat GmbH
Escher Str. 25A
50773 Cologne
Germany

You can contact our data protection team at our postal address and via E-Mail at privacy@sunhat.app

§ 2 Data Protection Officer

Our appointed data protection officer is:

Kertos GmbH
Brienner Str. 41
80333 München
Deutschland
E-Mail: dsb@kertos.io

§ 3 What is personal data?

Personal data is any information relating to an identified or identifiable natural person. This includes, for example, information such as your name, age, address, telephone number, date of birth, email address or IP address. Information for which we cannot (or can only with disproportionate effort) establish a link to your person, e.g. by anonymising the information, is not personal data. The processing of personal data (e.g. the collection, retrieval, use, storage or transmission) always requires a legal basis such as your consent.

1) Provision and use of the platform / server log files

a) Scope and purpose of data processing

We collect and use our users' personal data only insofar as this is technically necessary to provide a functional platform and our content and services or information.

When you access and use our platform, we collect the personal data that your browser automatically transmits to our server. This information is temporarily stored in a so-called log file.



The following information is collected without any action on your part and stored until it is automatically deleted:

- IP address of the requesting computer,
- Date and time of access,
- Name and URL of the retrieved file,
- Website from which the access is made (referrer URL),
- the browser used and, if applicable, the operating system of your computer and the name of your access provider.

We process the aforementioned data for the following purposes:

- Ensuring a smooth connection to the platform
- Ensuring the convenient use of our platform
- For IT-Security purposes

b) Legal basis

Art. 6 para. 1 lit. f GDPR serves as the legal basis. The processing of the aforementioned data is necessary for the provision of the platform and to enable secure and convenient use and thus serves to safeguard a legitimate interest of our company.

c) Storage period and data erasure

As soon as the aforementioned data is no longer required to display the platform, it is deleted (latest within 30 days). The collection of data for the provision of the platform and the storage of data in log files is absolutely necessary for the operation of the platform. Consequently, the user has no option to object. Further storage will take place in individual cases if this is required by law.

2) Data collection and processing in the context of the platform usage (in the role as data processor)

a) Scope of data processing

- Surname
- First name
- Address (postal address)
- Email address
- Telephone numbers
- Customer behavior data
- Image data
- Contract data
- Data provided by the user in the platform (e.g. internal policies)
- Contract/billing data (bank/credit card information, payment terms, invoice data, dunning data, correspondence/correspondence)
- System data (login, passwords, log data, IP address, user ID)

Special categories of personal data (e.g. health data, data on racial/ethnic origin) are not processed as part of the data processing relationship.



b) Legal basis and purpose

We collect and process this data exclusively for the purpose of contract performance, e.g. for the purpose of financial accounting. We also process personal data in our IT systems and IT applications.

In the context of establishing and executing contracts, the legal basis is Art. 6 para. 1 sentence 1 lit. b GDPR.

c) Storage period and data erasure

The data will be deleted as soon as it is no longer required for the purpose of its processing. In addition, there may be statutory retention obligations, for example commercial or tax retention obligations under the German Commercial Code (HGB) or the German Fiscal Code (AO). If such retention obligations exist, we will block or delete your data at the end of these retention obligations.

3) Use of Usage and Content Data for Development and Optimization Purposes (as Data Controller)

a) Scope of Data Processing

In addition to processing usage data (e.g., log data, usage duration, interaction information), we may also process content data provided by you (e.g., uploaded documents, comments, input fields) for the purpose of continuously developing and optimizing our platform and, in particular, the AI-based functions underlying it.

b) Legal Basis and Purpose

The legal basis for this processing is our legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR, in order to ensure the highest possible product and service quality as well as a reliable and secure operation of our offering.

Wherever possible, such data will be aggregated or anonymized so that it can no longer be traced back to individual data subjects. Automated decision-making (profiling) as defined in Art. 22 GDPR does not take place in this context.

You have the right to object to this processing at any time on grounds relating to your particular situation. Following your objection, we will no longer process your personal data for these purposes unless we can demonstrate compelling legitimate grounds for the processing.

§ 4 Recipients of personal data

Within our company, only those persons have access to your personal data who need it for the purposes stated in each case. Your personal data will only be passed on to external recipients if we are legally authorized to do so or if we have your consent. Below you will find an overview of the relevant recipients:

- Processors: Group companies or external service providers, for example in the areas of technical infrastructure and processing, maintenance and payment processing, which are carefully selected and checked. The processors may only use the data in accordance with our instructions.
- Public authorities: Authorities and state institutions, such as tax authorities, public prosecutors or courts, to which we (have to) transfer personal data, e.g. to fulfil legal obligations or to protect legitimate interests



Specifically, we use the following service providers for the purpose of the proper provision of our platform:

Subprocessor	Address	Service provided	Int. Data Transfer
AWS (via Render Services, Inc.)	38 Avenue John F. Kennedy, L-1855, Luxemburg	Database hosting	n/a
Pendo.io, Inc.	418 South Dawson Street Raleigh, NC 27601 United States	Analytics	Adequacy decision of the EU-Commission (EU-US Data Privacy Framework certified)
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107 USA	Hosting of the frontend, CDN	Adequacy decision of the EU-Commission (EU-US Data Privacy Framework certified)
Digital Ocean, LLC	101 Avenue OF The Americas FL 10 New York, NY 10013	Media Hosting	Adequacy decision of the EU-Commission (EU-US Data Privacy Framework certified)
Twilio Ireland Limited (Sendgrid)	25 – 28 North Wall Quay, Dublin 1, D01 H104 Ireland	Email Delivery Service	n/a
Functional Software, Inc. (Sentry)	45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Error Tracking	Adequacy decision of the EU-Commission (EU-US Data Privacy Framework certified)
ComDocks GmbH	Schopenstehl 13 c/o The Office Group 20095 Hamburg	Data Import	n/a
Intercom R&D Unlimited Company	124 St Stephen's Green, Dublin 2, Co. Dublin, D02 N960, Ireland	Help Center, Chat, Customer Service	n/a
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay,	AI-powered response and text generation &	Adequacy decision of the EU-



	Dublin 2, Ireland	document processing	Commission (EU-US Data Privacy Framework certified)
Mistral AI 952 418 325	15, rue des Halles 75001, Paris France	OCR, KI-gestützte Antwort- und Textgenerierung	n/a
PostHog Inc	2261 Market Street #4008 San Francisco, California 94114 United States	Product Analysis	Adequacy decision of the EU-Commission (EU-US Data Privacy Framework certified)
Langfuse GmbH	Gethsemanestr. 4, 10437, Berlin,	LLM Observability, Prompt Management, Evaluation	n/a

§ 5 International data transfer

We process your data mainly within the European Union (EU) and the European Economic Area (EEA). However, some of our service providers may be based outside the EEA in so-called "third countries". The General Data Protection Regulation places high demands on the transfer of personal data to third countries. All our data recipients must fulfil these requirements. Before we transfer your data to a service provider in a third country, each service provider is first checked for its level of data protection. A service provider is only selected if it can demonstrate an adequate level of data protection outside the EEA. Regardless of whether our service providers are based within the EEA or in third countries, each service provider must conclude an order processing agreement with us. Service providers outside the EEA must fulfil additional requirements. In accordance with Art. 44 ff. GDPR, personal data may be transferred to service providers who fulfil at least one of the following requirements:

- The European Commission has decided that the third country guarantees an adequate level of protection (e.g. Israel and Canada).
- Standard contractual clauses have been included in our contract with the data recipient (including any additional measures if necessary).
- Further appropriate safeguards pursuant to Art. 46 GDPR provided (e.g. Binding Corporate Rules).
- In special exceptional cases in accordance with Art. 49 GDPR

§ 6 Tracking

a. Scope and Purpose of Data Processing

Our platform uses various tracking technologies. These include, among others, the placement of cookies, the creation of a unique identifier by combining different device and browser information (device fingerprinting), as well as the use of so-called "universal IDs." For the purposes of this privacy policy, the term "cookies" is used as a generic reference to all such tracking technologies.

Cookies are data records that are stored on your computer when you visit our platform,



enabling your browser to be recognized on subsequent visits. Cookies store information such as your language settings, the duration of your visit to our website, or entries you make while using our platform.

There are different types of cookies. Session cookies are temporary and are stored in the user's web browser until the browser window is closed, at which point they are deleted. Persistent cookies are used for repeated visits and remain stored in the user's browser for a predefined period. First-party cookies are set by the platform you visit and can only be accessed by that platform. Third-party cookies are set by organizations other than the operator of the platform you are visiting.

A further distinction is made between technically necessary cookies, functional cookies, and advertising cookies. Technically necessary cookies are essential to ensure basic functions of the platform (e.g., saving language preferences). Functional cookies collect information about user behaviour and whether error messages are received. Advertising cookies, on the other hand, are used to provide users with tailored advertising.

b. Legal Basis

The legal basis for processing personal data by means of technically necessary cookies is Article 6(1)(f) GDPR, as we have a legitimate interest in providing a user-friendly presentation of our platform. If you have provided your consent to the use of functional and advertising cookies via a notice provided on our platform ("cookie banner"), the lawfulness of this processing is also based on Article 6(1)(a) GDPR.

c. Retention Period and Erasure of Data

Once the data transmitted to us via cookies is no longer necessary for the purposes described above, this information will be deleted. Further storage may take place in individual cases where this is required by law.

d. Configuring Browser Settings

Most browsers are configured to accept cookies by default. However, you may set your browser to accept only certain cookies or to reject all cookies. Please note that if you disable cookies via your browser settings, you may not be able to use all functions of our platform. You can also use your browser settings to delete cookies already stored or to view the storage period. It is also possible to configure your browser to notify you before cookies are stored. As browsers may differ in their respective functions, please refer to the help menu of your browser for information on configuration options.

e. Cookielist

NAME	Provider	Purpose	Duration
intercom-device-id-tscm3zvq	Intercom, Inc.	Storage of ID for user identification	1 week
intercom-device-id-tscm3zvq	Intercom, Inc.	Storage of ID for session recognition	1 week
pendo_cd	Pendo.io, Inc.	Tracking user interactions for analysis and optimization of the user experience	Session
pendo_tabId	Pendo.io, Inc.	Storage of a unique tab ID to distinguish multiple open sessions of the same user	Session
sentryReplaySession	Sentry	Capturing session data for error analysis and improvement of application stability	Session



sidebarState	Sunhat	Storage of the current state of the sidebar for personalization of the user interface	Unlimited
sidebarWidth:v2	Sunhat	Storage of the sidebar width to restore individual view settings	Unlimited
sun-locale	Sunhat	Storage of the user's preferred language to tailor content to language preferences	Unlimited

§ 7 Intercom

We use the service Intercom, provided by Intercom R&D Unlimited Company, 18-21 St. Stephen's Green, Dublin 2, Ireland, and Intercom, Inc., 55 2nd Street, 4th Floor, San Francisco, CA 94105, USA ("Intercom"), to identify logged-in users and manage sessions within our platform. This enables a personalized user experience and the storage of relevant session data.

When using Intercom, the following categories of personal data are processed:

- Your IP address
- Date and time of login
- Browser type and operating system
- User ID or email address (if registered)
- Session information (e.g. duration and interactions)

The processing of this data is carried out on the basis of Article 6(1)(f) GDPR, as we have a legitimate interest in the secure and efficient management of user accounts and the provision of a personalized platform experience. Processing is also based on Article 6(1)(b) GDPR insofar as it is necessary for the performance of the contract with you (provision of the website).

Intercom may transfer personal data to the USA or other third countries. For data transfers to the USA, there is an adequacy decision by the European Commission (EU-U.S. Data Privacy Framework). Intercom is certified under this framework, so such transfers are based on Article 45 GDPR. In addition, Standard Contractual Clauses (SCCs) have been implemented to ensure an adequate level of data protection.

For further information on data protection at Intercom, please visit:
<https://www.intercom.com/legal/privacy>.

§ 8 Data security and security measures

We undertake to treat your personal data confidentially. In order to prevent manipulation, loss or misuse of your data stored by us, we take extensive technical and organizational security precautions, which are regularly reviewed and adapted to technological progress. However, we would like to point out that due to the structure of the Internet, it is possible that the rules of data protection and the above-mentioned security measures may not be observed by other persons or institutions outside our area of responsibility. In particular, unencrypted data - e.g. when sent by e-mail - may be read by third parties. We have no technical influence on this. It is your responsibility as a user to protect the data you provide against misuse by means of encryption or in any other way.

§ 9 Obligation to provide personal data

There is no contractual or legal requirement to provide personal data and there is no



obligation to do so. If you do not provide your data, it may not be possible to fulfil the contract.

§ 10 Storage of the data

The personal data of the data subject will be deleted or blocked as soon as the purpose of storage no longer applies. Data may also be stored if this has been provided for by the European or national legislator in EU regulations, laws or other provisions to which the controller is subject. The data will also be blocked or erased if a storage period prescribed by the aforementioned standards expires, unless there is a need for further storage of the data for the conclusion or fulfilment of a contract.

§ 11 Data subject rights

You have the following legal rights vis-à-vis us with regard to your personal data:

Right of access

You have the right to request confirmation as to whether we are processing personal data concerning you. If this is the case, you have the right to information about this personal data and to further information, e.g. the processing purposes, the recipients and the planned duration of storage or the criteria for determining the duration.

Right to rectification

You have the right to request the rectification of inaccurate data without undue delay. Taking into account the purposes of the processing, you have the right to request the completion of incomplete data.

Right to erasure ("right to be forgotten")

You have the right to erasure if the processing is not necessary. This is the case, for example, if your data is no longer required for the original purposes, if you have revoked your declaration of consent under data protection law or if the data has been processed unlawfully.

Right to restriction of processing

You have the right to restrict processing, e.g. if you believe that the personal data is incorrect.

Right to data portability

You have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format.

Right to object

You have the right to object at any time, on grounds relating to your particular situation, to the processing of certain personal data concerning you. In the case of direct advertising, you as the data subject have the right to object at any time to the processing of personal data concerning you for the purpose of such advertising; this also applies to profiling insofar as it is associated with such direct advertising.

Right to withdraw your consent under data protection law

You can revoke your consent to the processing of your personal data at any time with effect for the future. However, this does not affect the legality of the processing carried out up to the point of revocation.

Without prejudice to these rights, you have the right to lodge a complaint with a supervisory authority at any time if you believe that the processing of your personal data violates data protection regulations.