Privacy and Cookie Policy

This Privacy Policy explains how **finmid GmbH** processes your personal data when you visit our website, contact us, apply for a job, or use our Platform. It provides information on what data we process, how we process it, and the rights you have under applicable data protection laws such as the General Data Protection Regulation (GDPR).

A. General Information on the Handling of Personal Data

This section provides general information on how we process personal data. Details for specific scenarios are outlined in subsequent sections.

1. Controller

The controller for the processing of your personal data within the meaning of the General Data Protection Regulation (GDPR) is

finmid GmbH

c/o WeWork

Dircksenstr. 3

10179 Berlin

privacy@finmid.com

For certain activities carried out on the Platform, such as payment processing and transaction handling, finmid may act as a **data processor** on behalf of its customers. Further details on this distinction are outlined in the sections below.

2. Data Protection Officer

Our appointed data protection officer is:

Kertos GmbH

Nymphenburger Str. 86

80636 Munich

Germany

You can reach our data protection officer by e-mailing dsb@kertos.io.

3. Cooperation with Third Parties / Data Recipients

In some cases, we use external service providers and partners to process your data, such as for the hosting of our website or Platform. We carefully select them before working with them. The partners are either bound by our instructions within the scope of data processing on our behalf as the data controller, or have made other agreements with us regarding data protection, for example because we process the data as joint controllers. We also work with partners who are professionally bound to confidentiality, such as tax advisors, lawyers and other service providers. You can find more detailed information about the service providers we use in the respective processing activity below.

Within our company, only those persons have access to your personal data who need it for the purposes stated in each case.

4. Data Transfers to Third Countries

We use some services whose providers are located in third countries (outside the European Union or the European Economic Area) or process personal data there, i.e. countries where the level of data protection does not correspond to that of the European Union. Where this is the case and the European Commission has not issued an adequacy decision (Art. 45 GDPR) for these countries, we have taken appropriate measures to ensure an adequate level of data protection for any data transfers. These include but are not limited to the standard contractual clauses of the European Union.

Where this is not possible, we base the transfer of data on the derogations under Art. 49 GDPR, in particular your explicit consent or the necessity of the transfer for the performance of the contract or for taking steps prior to entering into a contract.

Where a data transfer to a third country is planned and no adequacy decision or appropriate safeguards are in place, it is possible and there is a risk that authorities in the relevant third country (e.g., intelligence agencies) may gain access to the transferred data in order to record and analyze it, and that enforceability of your rights as a data subject cannot be guaranteed. You will also be informed of this when we obtain your consent via the consent banner.

5. Storage Period

In principle, we only store personal data for as long as necessary to fulfil the purposes for which we have collected the data. We then erase the data without undue delay, unless we still require the data until the end of the statutory limitation period for documentation purposes for claims under civil law or due to statutory retention obligations.

For documentation purposes, we are required to keep contract data for another six years after the end of the year in which the business relationship with you ends. After the

standard statutory period of limitation, any claims become statute-barred at this point in time at the earliest.

Even after that, we are still required to store some of your data for accounting reasons. We are required to do so because of statutory documentation requirements, in particular under the German Commercial Code and the Fiscal Code. The periods specified therein for retaining documents range from two to ten years. Where applicable, we will inform you of the length of time for which the data will be stored in the following sections relating to individual processing.

6. Your Rights as a Data Subject when Data is Processed

You have the following rights as a data subject:

- Right to withdraw consent
- Right to object to the processing of your personal data (Art. 21 GDPR)
- Right of access to personal data concerning you which we process(Art. 15 GDPR)
- Right to rectification of inaccurate personal data concerning you which we have stored (Art. 16 GDPR)
- Right to erasure of your personal data (Art. 17 GDPR)
- Right to restriction of the processing of your personal data (Art. 18 GDPR)
- Right to data portability (Art. 20 GDPR)
- Right to lodge a complaint with a supervisory authority (Art. 77 GDPR)

In order to establish your rights described here, you can contact us at any time using the contact details provided. This also applies if you wish to receive copies of safeguards in order to prove an adequate level of data protection. Subject to the respective legal requirements, we will comply with your data protection request.

We will keep your inquiries regarding the establishment of rights under data protection law, and our responses to these, for a period of up to three years for documentation purposes and, where necessary in individual cases, beyond this period if we need to establish, exercise or defend legal claims. The legal basis is Art. 6(1) Sentence 1(f) GDPR, based on our interest in defending ourselves against any civil-law claims under Art. 82 GDPR, avoiding administrative fines under Art. 83 GDPR and fulfilling our accountability under Art. 5 Sentence 2 GDPR.

You have the right to withdraw the consent you gave us at any time. As a result of this, we will cease the data processing based on this consent with future effect. This withdrawal

of your consent will not affect the lawfulness of the processing carried out on the basis of the consent prior to the withdrawal.

Insofar as we process your data on the basis of legitimate interests, you have the right to object to the processing of your data at any time for reasons arising from your particular situation. If your objection is to data processing for direct marketing purposes, you have a general right of objection, which we will implement without requiring you to give reasons.

If you would like to make use of your right of withdrawal or objection, it is sufficient to simply notify us using the contact details provided above.

Finally, you have the right to lodge a complaint with a data protection supervisory authority. You can assert this right, for example, by contacting a supervisory authority in the Member State of your habitual residence, your place of work or the place of the alleged infringement. The competent supervisory authority in Berlin, where we are headquartered, is: Berlin Commissioner for Data Protection and Freedom of Information, Alt-Moabit 59-61, 10555 Berlin; tel.: +49 30 13889-0, e-mail: mailbox@datenschutz-berlin.de

7. Automated Decision-Making

We do not use automated decision-making or profiling.

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. Provision of Personal Data

As a visitor to our website or user of our platform, you are generally not obligated to provide personal data. However, certain functionalities of our services may rely on the collection of data (e.g., connection data for displaying the site correctly or processing requests via contact forms). If you choose not to provide this information, it may limit or impair your ability to fully use certain features of the website or Platform.

10. Changes to this Privacy Statement

We will update this privacy statement from time to time, for example if we adapt our services or if there are changes to the legal or regulatory requirements.

B. Data Processing when you are a user of our Platform

Differentiation Between Controller and Processor Roles

When processing personal data on our Platform (https://platform.finmid.com), finmid may act either as a Data Controller or a Data Processor, depending on the specific processing activities:

Finmid as a Data Controller:
Finmid determines the purposes and means of processing for activities that directly relate to user account management, analytics, and customer support. For these processes, finmid is responsible for compliance with the GDPR and other relevant data protection regulations.

Finmid as a Data Processor:
Finmid processes data on behalf of its customers in connection with services provided through the Platform, such as managing financial transactions, generating invoices, and handling payout data. In this role, finmid follows the instructions of the Data Controller (our customer) and provides the technical infrastructure necessary for processing.

Why is this distinction important?
The GDPR sets different obligations for data controllers and processors. As a controller, finmid ensures transparency and accountability for its independent processing activities, while as a processor, finmid adheres to the instructions of the controller and takes measures to safeguard the data it processes on their behalf. This section provides clarity about these roles and the associated processing activities.

1. Introduction

This section explains how we process your personal data when using our Platform.

2. Provision of the Platform

Every time you visit our Platform, your browser automatically collects and transmits connection data to enable you to visit the site. This connection data comprises what is known as HTTP header information, including the user agent, and includes in particular:

- IP address of the requesting device
- Method (e.g., GET, POST), date and time of the request
- Address of the requested website and path of the requested file

- The previously visited website/file (HTTP referrer)
- Information about the browser used and the operating system
- Version of the HTTP protocol, HTTP status code, size of the file delivered
- Request information such as language, type of content, coding of content, character sets.

It is absolutely necessary to process this connection data to make it possible to visit the website, to guarantee the long-term functionality and security of our systems, and for the general administrative maintenance of our site.

The legal basis for the processing of data is Art. 6(1) Sentence 1(f) GDPR.

The data will be erased as soon as it is no longer required for achieving the purpose of its collection. In the case of recording the data to provide the website, this is the case when the respective session has ended.

3. Hosting with AWS and CDN CloudFront

We host our Platform with Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, 1855 Luxembourg ("AWS"). When you visit our Platform, your personal data is processed on AWS servers. Personal data may also be transferred to the parent company of AWS in the USA. The transfer of data to the USA is based on the adequacy decision of the European Commission for the USA (Amazon.com, Inc. is certified according to the EU-US-DPF) and the EU standard contractual clauses. You can find details here in the AWS Data Processing Addendum.

We also use AWS's CloudFront content delivery network ("CDN") on our site. A CDN is an online service used primarily to deliver large media files (such as graphics, page content or scripts) through a network of regionally distributed servers connected over the Internet. It makes duplicates of a site's data available on multiple AWS servers around the world. These servers, which are located in non-EU countries, are only accessed if the site is accessed from a network in a non-EU country. This means that if the site is accessed from Germany or the EU, the site is loaded from servers in Germany / the EU. Only if the site is visited from outside the EU, will the content be served from the nearest server outside the EU. Some of the images and files embedded in this site are then loaded from the CloudFront CDN when the page is requested. Through this request, information about your use of our Platform (such as your IP address) is transferred to and stored on AWS servers in other EU countries. This happens the moment you enter our Platform.

The use of AWS and the CloudFront CDN is in the interest of increased website reliability, increased protection against data loss, and improved loading speed of this site. This constitutes a legitimate interest within the meaning of Art. 6(1) Sentence 1(f) GDPR.

The data will be erased after it is no longer needed to provide the website or comply with legal requirements.

To learn more about AWS's privacy practices, please visit: https://aws.amazon.com/de/compliance/gdpr-center/

4. Authentication and Login

When logging into the Platform, we collect and process:

- Login credentials (e.g., email and password, stored securely in encrypted form)
- Session data to maintain your authentication and user session throughout your use of the Platform.

The legal basis for this data processing is Art. 6(1) Sentence 1(b) GDPR, as it is necessary to perform the contract and provide the Platform's functionalities.

5. Payment and transaction data

When you process transactions on the Platform, we collect the following data:

- Payment details, such as Payment ID, buyer information, total amount, and due dates.
- Invoice-specific details such as invoice number, creation date, due date, and payment status.
- Buyer and seller contact information, including names and identifiers used in the system.
- Transaction completion details, including timestamps when payments are successfully completed.The legal basis for this data processing is Art. 6(1) Sentence 1(b) GDPR, as this is necessary for the execution of payment-related service.

The legal basis for this data processing is Art. 6(1) Sentence 1(b) GDPR, as this is necessary for the execution of payment-related services.

6. Customer Support

When providing customer support for Platform users, we process:

- User identification data (e.g., name, email address)
- Details related to inquiries, such as payment or invoice issues
- Platform usage logs to resolve technical issues or disputes

The legal basis is Art. 6(1)(b) GDPR and Art. 6(1)(f) GDPR (legitimate interest in resolving issues and improving services).

7. Invoice Management
The platform processes and presents:

- Payout data related to sellers, including payout details and completion status.
- Structured invoice details visible to the user, such as total amounts, amounts paid, and remaining balances.
- Buyer-seller relationship data, enabling transparency for both parties in the transaction.

The legal basis for this data processing is Art. 6(1) Sentence 1(b) GDPR, as it enables the proper functioning of payment and invoice management features within the platform.

8. Analytics with PostHog

We use PostHog, an analytics tool provided by PostHog Inc, 2261 Market Street #4008 San Francisco, CA 94114.

PostHog may process data outside of the EU. For any data transfers to the USA, we rely on Posthog's active certification under the EU-U.S. Data Privacy Framework.

Legal Basis: The use of PostHog is based on your explicit consent under Art. 6 para. 1 lit. a GDPR. This consent is obtained via the consent banner when you visit the platform for the first time.

You can revoke your consent at any time by visiting the cookie preferences in the settings menu of the platform.

C. Cookie Policy

1. General

We use the tools necessary for Platform operation on the basis of our legitimate interest in accordance with Art. 6 para. 1 lit. f GDPR to provide the basic functions of our Platform. In certain cases, these tools may also be necessary for the performance of a contract or in order to take steps prior to entering into a contract, in which case the processing is carried out in accordance with Art. 6 para. 1 lit. b GDPR. Access to and storage of information in the end device is absolutely necessary in these cases and takes place on the basis of the implementation laws of the ePrivacy Directive of the EU member states, in Germany pursuant to Section 25(2) TDDDG.

We use all other nonessential (optional) Tools that provide additional functions on the basis of your consent in accordance with Art. 6 para. 1 lit. a GDPR. Access to and storage of information in the end device then takes place on the basis of the implementation laws of the ePrivacy Directive of the EU member states, in Germany pursuant to Section 25(1) TDDDG. Data processing using these tools only takes place if we have received your

consent in advance. We currently use Posthog as an optional tool (see section 6 "Analytics with PostHogs").

If personal data is transferred to third countries, and the European Commission has not issued an adequacy decision (Art. 45 GDPR) for these countries, we have taken appropriate measures to ensure an adequate level of data protection for any data transfers. These include but are not limited to the standard contractual clauses of the European Union.

Where this is not possible, we base the transfer of data on the derogations under Art. 49 GDPR, in particular your explicit consent or the necessity of the transfer for the performance of the contract or for taking steps prior to entering into a contract.

2. Obtaining your consent

We use a necessary tool to obtain and manage your consent. This generates a banner informing you about data processing and giving you the option to consent or reject data processing through the optional tool. This banner appears the first time you login in to our Platform and when you revisit the selection of your preferences to change them or revoke consent.

The data processing is necessary to provide you with the legally required consent management and to comply with our documentation obligations. The legal basis is Art. 6 para. 1 lit. c GDPR and Art. 6 para. 1 lit. f GDPR, justified by our interest in meeting the legal requirements for consent management.

3. Withdraw consent and manage settings

You can revoke your consent for certain tools, i.e. for the storage of and access to information in the end device and the processing of your personal data, at any time with future effect. To do so, please visit the Platform, open the settings menu, and select cookies preference.

4. Implemented Tool: Analytics with PostHog

We use PostHog, an analytics tool provided by PostHog Inc, 2261 Market Street #4008 San Francisco, CA 94114.

PostHog may process data outside of the EU. For any data transfers to the USA, we rely on Posthog’s active certification under the EU-U.S. Data Privacy Framework.

Legal Basis: The use of PostHog is based on your explicit consent under Art. 6 para. 1 lit. a GDPR. This consent is obtained via the consent banner when you visit the platform for the first time.

You can revoke your consent at any time by visiting the cookie preferences in the settings menu of the platform.

5. Cookie List

Technically Necessary Cookies

These cookies are essential for the operation of the platform and cannot be disabled.

NAME	Service	Purpose	Cookie Type	Duration
KEYCLOAK_SESSION	Authentication	Used to manage and persist user authentication sessions via Keycloak.	First-Party	Session
KEYCLOAK_SESSION_LEGACY	Authentication	Legacy session management for authenticated users, ensuring backward compatibility.	First-Party	Session
KEYCLOAK_IDENTITY	Authentication	Stores the identity token for authenticated users to enable secure access.	First-Party	Session
KEYCLOAK_IDENTITY_LEGACY	Authentication	Legacy identity token management for backward compatibility.	First-Party	Session
FINMID_KEYCLOAK_DEVICE	Device Management	Stores device-specific settings to support authentication across multiple devices.	First-Party	Session
FINMID_KEYCLOAK_DEVICE_LEGACY	Device Management	Legacy device-specific settings for compatibility with older configurations.	First-Party	Session

AUTH_SESSION_ID	Authentication	Session management for authenticated users to prevent unauthorized access.	First-Party	Session
AUTH_SESSION_ID_LEGACY	Authentication	Legacy session ID management for backward compatibility.	First-Party	Session
I18nextLng	Language Selection	Set by finmid to indicate user-selected language.	First-Party	1 year
CookieConsent	Consent Management	Stores the user's cookie consent preferences for compliance with GDPR and ePrivacy requirements.	First-Party	1 year

Optional Cookies

This cookie is optional and serves for analytics purposes.

NAME	**Service**	**Purpose**	**Cookie Type**	**Duration**
ph_phc_yAikBwmVcfMeSO4ozsg8nuQVP901j2rQ8oO4Vv69BaQ_posthog	Posthog Analytics	Tracks user interactions and generates session-based analytics for service improvement.	First-Party	1 year

D. Changes to this Privacy and Cookie Policy

We may update this Privacy and Cookie Policy from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. We encourage you to review this Privacy and Cookie Policy periodically to stay informed about how we use cookies.

Last amended: November 2024