

## About

With this Privacy Policy, we would like to inform you about the nature, scope and purpose of the collection and processing of your personal data when you use our mobile app or our website [www.vivid.money](http://www.vivid.money), operated by Vivid Money GmbH (“Vivid”, “we”, “us”).

## Responsible authority

The controller responsible for the collection and processing of your personal data in accordance with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (“GDPR”) is:

Vivid Money GmbH  
Karl-Marx-Straße 97-99  
12043 Berlin, Germany  
Commercial Register HRB 209049 B

If you have any concerns, requests or questions about your data, or think that some of our privacy practices are not addressed in this Privacy Policy, please contact our Data Protection Officer at [dpo@vivid.money](mailto:dpo@vivid.money).

Where we process your personal data jointly with a cooperation partner, please refer to the cooperation partner’s Data Protection Information for details on how the partner processes your personal data.

## Why we process your personal data (legal basis)

### 1. Contract

When you download our app, you have an opportunity to open a current account with our partner bank solarisBank AG (“solarisBank”). Certain personal data are necessary for entering into this agreement and for subsequent delivery of the services included. These data are processed by us, solarisBank and any other third parties who help us provide you with financial services. The lawful basis for this processing is Art. 6 (1)(b) of the GDPR - processing which is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract.

Please note that for many of our financial services and features, without the necessary personal data we will not be able to fulfil our contractual obligations, and therefore we will likely have to refuse entering into, or terminate a business relationship with you.

## 2. Legitimate interests

Sometimes we need to collect and process your personal data to safeguard our legitimate interests or the legitimate interests of third parties. In these cases we also process your data lawfully according to Article 6 (1)(f) of the GDPR. Examples of such processing include:

- Ensuring IT security
- Preventing criminal activity, such as fraud
- Push notifications or messages relating to your existing or new services and offers
- User experience analytics and optimization
- Personalization of services and tariff options
- Defense of and against legal claims

## 3. Consent

If you gave us consent to process your personal data for one or more specific purposes:

- Allowing us to show other clients that you use our bank
- Adding a photo avatar and allowing us to show it to other clients (if you chose to become visible as a client)
- To access contacts on your device
- To place cookies on your device

These data are processed according to Article 6(1)(a) of the GDPR. You can withdraw your consent at any time, by removing the photo, or by accessing the settings in the application or your device to unselect these features. However, keep in mind that the processing which took place before withdrawal remains lawful.

## 4. Legal obligation

In cases where we or our partners are required to comply with any applicable laws, your personal data is processed according to Article 6(1)(c) of the GDPR - processing is necessary for compliance with a legal obligation to which the controller is subject.

Some examples of processing here include verification of your identity and age, prevention of money laundering and fraud, and tax reporting obligations.

## When we process your personal data

### ***Account opening.***

In order for you to enter into an agreement with solarisBank to open an account on your behalf, we collect the following personal data:

- Email
- Phone number
- Country of citizenship
- Country of residency
- Full name
- Date of birth
- Gender
- Whether you're a US tax resident
- Employment status
- Working area
- Address (where we can send your new bank card)
- Login credentials
- Internal client ID (we assign when you become a client)
- Device ID (also we assign)

***Identity verification.***

In order to open an account for you with solarisBank, it is necessary to verify your identity. To accomplish this, we ask you to undergo a video identification procedure through a third party service provider. You may also need to provide a copy of your government-issued ID.

***Card issue and delivery.***

Once you've opened your bank account, you may wish to order a card. To make and deliver one to you, we process and transfer to solarisBank and our service providers your name, address, phone number, email, device ID and the information about the bank account the card is tied to. If it is a virtual card, we process all of the data mentioned above, except your address.

***Transfers and payments.***

When you start using your account and bank cards, in addition to some of the personal data provided for opening of your account, we process the following:

- Transfers to and from your account (e.g. internal and external account numbers, IBAN (for external transfers), recipient name and/or phone number, amount, currency, date, client ID)
- Card transactions (e.g. merchant, amount, currency, location, date, method of payment, client ID)

Please note that when you complete a funds transfer to another person using their phone number, we must show the recipient's name and account number in your monthly or yearly statement, or any other bank document reflecting executed transfers to and from your account.

***Money requests.***

If you send a money request to another person or split a bill with your friends or family (up to 10 persons, and only those who allowed themselves to be visible as our clients), we will show your name to the recipient. Your name and account number will also appear in their monthly or yearly statement, or any other bank document reflecting executed transfers to and from their account.

***Pocket sharing.***

The owner of the pocket can share it with up to five other people. The names of these five people (name from client book or client name) and the details of all transactions they execute (e.g. date, merchant, location, amount) are visible to the owner of the pocket and other pocket users. The users are able to see each other and the shared pocket details only if they accept it. They also can see the details of the owner and each other's transactions, as well as the funds available in the account. Neither the owner, nor the users can see each other's card details.

***Google Pay and Apple Pay.***

Adding your card to Google Pay or Apple Pay involves processing your card information and Google or Apple wallet ID by us and our partner bank. Your card information is transferred to our partner's service provider Visa, where it is tokenized (basically, encrypted) and then, together with your address, phone number and the last four digits of the card number, we pass it on to Google or Apple. They will use that encrypted card data to perform transactions whenever you pay using your mobile phone.

***Security trading services.***

If you choose to use our security trading services, in addition to some of the personal data provided for opening a regular account, we and our partners process the following:

- Information about your occupation and employer
- Sources of your wealth
- Net worth and liquid net worth
- Annual net income
- Country where you pay taxes and your tax ID
- Investment account number
- Transaction data (generated during each trade)

Please note that all regulated activities are performed exclusively by our partner solarisBank and the third-party broker Interactive Brokers. Vivid only provides a mobile application and platform environment which enables onboarding and reception and transmission of your orders.

***Phone contacts.***

If you choose to use the feature which allows you to quickly and easily transfer money to contacts in your mobile device's phonebook, or to share your pocket or cashback with friends, we will access your contacts in order to check if the contact you are trying to transfer money to is also our client. Please note that when we access your contacts and do the check, we do not

transfer “raw” phone numbers from your phone - they are processed in such a way that only hashed (irreversibly changed into a unique unrecognizable sets of digits) versions, stored on your device, are used to match the number to an existing client. You can switch off access to contacts in your device’s settings at any time.

***Cashback/Vivid Points Program.***

In the context of our cashback/points program we process your client ID, as well as data about your transactions, including details received from payment processors about the amount, date, time and merchant. We do not sell or share this personal data with third parties for marketing purposes.

***Subscription protection.***

To help you balance your expenses and control your budget, we keep track of all regularly occurring payments that are charged to your account and let you know when one is coming up. That way you can take action in advance, in case there are limited funds in your account and the payment needs to be modified or cancelled. Here we may process such personal data as your client ID, bank account transaction and merchant details, date, amount, currency.

***When you contact us.***

When you contact us via support chat or by any other means, we may process such categories of personal data as your email, phone number, client ID, language, country, as well as any information about the standing of your account or details of your transactions, depending on the issue you are experiencing. We may also collect other information if you choose to share it with us. Please do not share any additional personal data or documents, either concerning yourself or other individuals, unless specifically requested by us.

***When you visit our website.***

When you visit our website, we may automatically collect some personal data from your device. This information may include your IP address, date and time of the request, time zone difference to GMT, browser language and version, operating system version or producer, information about your device, as well as some data about how you interact with our website (e.g. which website you came from, pages visited, links clicked). We do this to keep our website secure and to understand who visits it and which pages they find interesting, so we can improve the site and provide relevant content. Some of this data is collected using cookies. You can find more information about them in our [Cookie Notice](#).

***Analytics.***

We process the personal data you provide us with, as well as the data created as a result of your use of our application, for analytics purposes. For example, we analyze how you interact with the app and make it more intuitive and easier for you to use, or to understand whether our products and services are customized to your needs so we can make changes if necessary,

tweak the rates and conditions, and develop new products and services. In that case these data are stripped of direct identifiers, to provide an additional layer of protection. If you wish to object to this processing, please contact us at [privacy@vivid.money](mailto:privacy@vivid.money).

### ***Direct marketing.***

From time to time we will contact you to tell you about our new products or services which we think may be of interest to you. This type of activity is considered direct marketing, and in this case we rely on your consent or our legitimate interest to process your personal data for this purpose. If you wish to withdraw your consent or object to this processing, you can switch off notifications in your app preference center, or click on the “unsubscribe” link at the bottom of the email you receive from us.

## **Special categories of data**

We do not intentionally ask you to provide information that belongs to a “special” category, like racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning sex life or sexual orientation.

However, there may be circumstances where your transaction data reveals this more sensitive information. For example:

- Payments for medical services or treatments may reveal data concerning your health.
- Making contributions and donations to churches, NGOs, political parties, trade unions etc. may reveal your religious or philosophical beliefs or political affiliation.
- Payments to sex shops or certain night clubs may reveal sensitive information regarding your sex life.

Taking into account this risk, we ensure that the payment information is kept confidential, and forbid our staff to extract data which belongs to special categories.

## **Who we share your personal data with**

In order to provide you with certain functions and services, we have to share your personal data with partners, external third party service providers, related and regulatory entities. They only process your personal data on the basis of data processing agreements and according to strict instructions, which do not allow them to use your data for any other purposes without notifying you or asking for your consent. Here are some of the categories of the parties we may share your data with:

- Our partner bank and joint controller solarisBank
- Companies that make and deliver your cards
- Cloud computing and storage providers like Amazon Web Services
- Analytics and business intelligence platforms like Snowflake, Mode Analytics, Appsflyer, Amplitude

- Companies that help us send you service related and marketing messages
- Providers of software that we use for customer support and issue tracking
- Companies that help us with customer and operations support
- Mobile payment providers like Google Pay
- Investment and trading platforms like Interactive Brokers
- Web analytics services like Google Analytics

We, our partners, service providers and others may also be required to share your personal data with various financial institutions and/or enforcement or court authorities to comply with applicable laws, prevent fraud, enforce an agreement we have with you, or to protect our rights, property or safety, or the rights, property or safety of our employees or agents.

Additionally, we may reveal your personal data to third-parties if: (1) you request or authorize it; (2) to address emergencies or acts of God; and (3) to address disputes, claims, or to persons demonstrating provable legal authority to act on your behalf.

If you would like to receive more detailed information regarding third parties we share your personal data with, please contact us at [privacy@vivid.money](mailto:privacy@vivid.money).

## **Data transfers to third countries**

Some of our partners, service providers or other parties we transfer your personal data to may be located in countries throughout the world, including outside the EU or the EEA. Therefore, the data may be sent to countries with different data protection laws than your country of residence. In such cases, to ensure that your personal data receives a comparable level of protection, we provide appropriate safeguards, such as adequacy decisions and frameworks or Standard Contractual Clauses approved by the European Commission. If you would like to receive more information about the transfers or safeguards, please contact us at [privacy@vivid.money](mailto:privacy@vivid.money).

## **Automated decision-making and profiling**

We process your data partially automatically in order to evaluate certain personal aspects (profiling). For example, we use profiling to prevent fraud, combat money laundering, terrorist financing and asset-polluting crimes. Our monitoring model combines information from transaction details, customer profile data and device session data. The approach is based on current fraud trends, best practices from VISA and other sources. These measures serve to protect your interests and keep your deposits secure.

## How long we keep your data

We keep your personal data for as long as it is necessary to achieve the purpose for which it was collected, usually for the duration of our contractual relationship plus any period thereafter as required or permitted by law, or to satisfy any legal obligations. When the data is no longer required, it will normally be deleted, unless we must:

- Satisfy the retention requirements of the Commercial Code (Handelsgesetzbuch), Tax Code (Abgabenordnung), Banking Act (Kreditwesengesetz), Money Laundering Act (Geldwäschegesetz) and Security Trading Act (Wertpapierhandelsgesetz). The retention periods for storage range from two to ten years.
- Preserve evidence under the statute of limitations. According to §§195 ff. of the German Civil Code (BGB), these limitation periods can be up to 30 years, however the regular limitation period is three years.

## Your rights

Data protection laws provide you with rights to help you understand and control how your personal data is used. These are your rights:

- **Right to be informed** about why and how we are processing your personal data - we hope we achieved this by providing you with this Privacy Policy.
- **Right to have access** to your data - you have the right to ask us if we are processing your personal data, why we are doing so, under what lawful basis, the categories of your personal data, whether the data is being sent outside the EU, who we share your data with, how long we keep it, and request a copy of the data we are processing. If you are unable to find sufficient information in our Privacy Policy, please contact us at [privacy@vivid.money](mailto:privacy@vivid.money).
- **Right to object** to some processing - direct marketing, or if processing is based on legitimate interests.
- **Right to have your data deleted** - otherwise known as “right to be forgotten”. You can exercise this right if you withdraw your consent and there is no further legitimate interest in our processing of your data, your objection to processing under legitimate interests outweighs our interests, the processing is no longer necessary, there is a law that requires the data to be deleted, or the processing is unlawful.
- **Right to restrict processing** - if the personal data we are processing is inaccurate, if our processing is unlawful, if the data is no longer necessary for the original purpose of processing but needs to be kept for potential legal claims, or you have objected to processing carried out under legitimate interests and we’re still in the process of determining whether there is an overriding need to continue processing.



- Right to **data portability** - you can ask for your data that we process by using a computer, which you provided to us on the basis of consent or because it was necessary for a contract.
- Right to ask us about **automated decision-making** - you have the right to ask us to explain the logic involved in making any automated decisions and for the decision to be reviewed by a human being, if that decision had an effect on your rights or freedoms.
- Right to **rectification** - if any of your personal data that we hold is inaccurate, you can request to have it corrected.
- You have the **right to lodge a complaint** with the competent data protection authority if you have concerns about how we process your personal data. However, we would appreciate it if you contacted us first and gave us an opportunity to resolve the issue.

If you would like to exercise any of these rights, or find out more about how we process your personal data, please contact us at [privacy@vivid.money](mailto:privacy@vivid.money). Reasonable access to your personal data will be provided at no cost. If access cannot be provided within a reasonable time frame, we will let you know the date when the information will be provided. If for some reason we cannot satisfy your request, we will provide an explanation why.

## Security of your information

To help protect the privacy of personal data you provide through the use of our website or mobile app, we maintain physical, technical and administrative safeguards. We update and test our security technology on an ongoing basis. We restrict access to your personal data to those employees who need to know that information to provide services to you. In addition, we train our employees about the importance of confidentiality and maintaining the privacy and security of your data. We commit to taking appropriate disciplinary measures to enforce our employees' data protection responsibilities.

## Changes and updates to this Privacy Policy

As our organization and services change from time to time, this Privacy Policy may change as well. We reserve the right to amend it at any time, for any reason, without notice to you, other than the posting of the amended Privacy Policy on our website or in the mobile app. We may email periodic reminders of our notices and terms and conditions and will notify you of material changes thereto, but you should check our site or the app to see the Privacy Policy that is in effect and any changes that may have been made to it.