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, operated by Vivid Money GmbH (“Vivid Money”, “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
Kemperplatz 1
10785 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.

Joint controllers

Additionally, please note that we work closely with Solaris SE (formerly Solarisbank AG), Cuvrystraße 53, 10997 Berlin, Germany (“Solaris”), in order to provide you with our banking products. Solaris may operate through a local branch in your country. As a licensed credit institution, Solaris operates the necessary infrastructure for the banking services, and Vivid Money acts as the technology platform. We operate the banking app, provide customer service and, together with Solaris, manage the customer deposits. We and Solaris jointly determine the purposes and means of processing your personal data on the basis of a joint controller agreement within the meaning of Article 26 GDPR.

In essence, you conclude a payment services framework agreement with Solaris, as well as a Contract of Use with us. In order to conclude and execute the respective contracts and to provide our services, we and Solaris need to collect your personal data. We and the bank act as joint controllers of this data, meaning that in general any collection, processing and use of personal data with regards to the provision of banking services is within the responsibility of the bank and with regards to the Contract of Use is within our responsibility.

Among other things, the joint controller agreement specifies that you can assert all rights relating to processing of your data against us and Solaris.

If you'd like to receive more detailed information regarding our and Solaris' respective obligations, please contact us at privacy@vivid.money.

Please refer to https://vivid.money/en-de/legal-documents/ where you can find in your language and country the information on how Solaris 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 Solaris. Certain personal data are necessary for entering into this agreement and for subsequent delivery of the services included. These data are processed by us, Solaris 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 a 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 (we collect device and session data for this purpose)
- Push notifications or messages relating to your existing or new services and offers
- User experience analytics and optimization
- Personalization of services and tariff options
- Defence 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 partner bank
- Adding a photo avatar and allowing us to show it to other clients, for example in their contact lists, shared banking activities, or referral links (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, for example 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.

Fraud prevention and anti money laundering checks, SEON

When you register via our Vivid Money mobile application to use the banking services provided by Solaris *[defined as Solaris SE, Cuvrystraße 53, 10997 Berlin, Germany]* or one of Solaris' local branches in Spain or Italy or France), and on an ongoing basis while you use such services, Solaris will perform a risk assessment for fraud prevention and anti-money laundering purposes. For such purposes, Solaris uses SEON Technologies Kft. (Rákóczi út 42. 7. em., Budapest 1072, Hungary) as a service provider under a data processing agreement with Solaris in accordance with Art. 28 GDPR.

In order to perform the risk assessment, we collect and transfer to Solaris the following browser data, device data, traffic data and location data from your device: IP address including type (e.g. commercial, mobile line, university) and whether it is listed as harmful, TOR value, VPN, proxy, number of accessories attached to your device, whether your phone is muted or not, device system's volume, country code and name of carrier (a) associated with the SIM card and (b) the device is currently using, device model type and unique identifier, system uptime, iCloud token, version and name of device given by the user in iOS settings, when the device last booted in UNIX time format and UTC time zone, country code and ID associated with device, cookie session ID, and browser details / settings including scrolling behaviour.

Solaris may add additional information and will then transfer such data to SEON along with your email address, name and phone number for performance of a risk analysis regarding potential fraudulent or other illicit activities.

SEON analyses this personal data based on a mathematically-statistically recognised and proven procedure and will provide Solaris with a fraud risk score. As part of the analysis, SEON may perform email analysis, social media lookup or address profiling.

More information

SEON's technology makes it possible to identify and assess the risk of fraudulent and illegal activities. In particular, the following types of personal data can be processed:

IP address (including type, such as commercial / organisation / library / landline / mobile line / school, college, university / data centre, web hosting / reserved / military / content delivery network / government / search engine spider), email address (including whether it exists), score value relating to email address, registered or disposable Boolean, IP country code, IP status, geographic latitude, geographic longitude, TOR value, whether an IP address is listed as harmful or not, VPN, web proxy, public proxy, number of spam lists in which the IP address has been found, history of requests for re-qualification of the IP address based on previous evaluations in SEON, social network account details (if an account is registered on (social network) networks with the email account, e.g., g., if an account is registered with the email account, e.g., g., g. e.g. g. Facebook, Google, Apple, Twitter, Microsoft, eBay, Yahoo, Instagram), details of data breaches if the email has been compromised, history of requests relating to the email address (based on previous assessments in SEON), phone number, number of accessories connected to the device, whether the phone is muted or not, system volume of the device on a scale from 0 to 100, whether the phone is currently charging, current battery level of the device on a scale from 0 to 100. The country code

associated with the SIM card, the phone number of the device, the phone number of the device, the phone number of the device and the phone number of the device, the country code associated with the SIM card, the name of the operator associated with the SIM card, the unique identifier of the user's device based on the SEON algorithm, the model type of the device, the unique device identifier, the iCloud ubiquity token registered on the device, the version and name of the device provided by the user in iOS settings, the last time the device was started in UNIX time format and UTC time zone, the network currently used by the device, and the country code associated with the device.

SEON may collect additional information about the user's (social media) accounts, such as avatar URL, name or date of registration. If publicly available, this may also include domain analysis, account existence, gender, age (depending on the profile), language settings, relationship status, place of work and profile activity assessment.

For device fingerprinting: cookie hash (ID of browser cookie session), browser hash (ID of browser environment using all data collected from browser/operating system/device and network), device hash (ID of device hardware environment via canvas and html5 based fingerprinting):

- Parameters collected from browsers: cookie hash, browser hash, device hash / unique device identifier, browser time zone and IP, OS detection, user agent information, private browsing detection, OS / browser languages, device screen size / browser / windows, installed fonts and generated hash, installed plugins and generated hash, battery level, GPU information, cursor, scrolling behaviour, browser features: flash / java, etc., canvas device fingerprint, audio fingerprint, WebRTC IPs, DNS: Geo + ISP, TCP/IP fingerprint, passive SSL/TLS hand-shake analysis.

- Parameters collected from IOS devices: hash / unique device identifier, accessory info, audio info, battery info, CPU info, advertising identifier (ADID), device name, device orientation, unique device identifier (UDID), iCloud ubiquity token, iOS version data, jailbreak status, emulator detection, kernel info, boot information, network configuration, PCB data, memory information, proximity sensor data, local language, local time zone, screen brightness, screen resolution, system uptime, storage information, MAC address, WIFI SSID, TCP/IP fingerprint, passive SSL/TLS protocol analysis.

- Parameters collected from Android devices: device hash/unique device identifier, Android ID, Android version data, au-dio information, battery information, build information, carrier information, CPU information, device name, storage information, emulator detection, root status, kernel information, boot information, network configuration, PCB data, memory information, proximity sensor data, local language, local time zone, screen brightness, screen resolution, system uptime, MAC address, WIFI SSID, TCP/IP fingerprint, passive SSL/TLS protocol scan.

Based on the analysis and risk score, you will be able to complete your registration, be rejected as a new customer, or may be guided through an extended registration process. The decision-making process is automated. If you want to challenge the automated decision and want to have a human review of this automated decision, you can get in touch with us by contacting privacy@vivid.money. Once you have given your consent and are onboarded, Solaris will continuously collect the above data and perform additional risk analysis via SEON for ongoing fraud risk assessment.

The legal basis for the device analysis and of the processing is your consent (as applicable, Art. 25 TTDSG, *Art. 122 Italian Privacy Code – as applicable to Customers whose accounts are characterized by Italian IBANs,* Art. 6 (1) lit. a, Art. 22 (2) lit. a GDPR and other relevant data protection provision applicable to your jurisdiction).

As a new Customer, while you are free to give your consent, you cannot, unless you are a Customer in Spain, use the banking service provided by Solaris without consenting, because the fraud prevention and anti-money laundering check is necessary for a secure provision of the banking services by Solaris. As a licensed bank, Solaris has a statutory obligation to fight money laundering by setting up a functioning risk management system and internal security measures as well as an ongoing screening of customers' activities (sections 4, 6 and 10 of the

German Anti-Money-Laundering Act, Art. *15, 17, 19 and 25 of the Italian Legislative Decree 231/2007 – as applicable to Customers whose accounts are characterized by Italian IBANs, and other relevant anti money laundering provisions applicable to your jurisdiction*). You can withdraw your consent at any time by email to privacy@vivid.money, but without consent you will not be able to continue using Solaris' services. As a consequence we will need to terminate our relationship with you and also other services available through the Vivid Money mobile application may be affected. Customers in Spain are advised that they can use the banking service provided by Solaris without consent, however you may be required to provide additional information and documentation in order to continue using Solaris banking services without risk of fraud.
Your personal data will be stored until the purposes of processing these data as set forth above have been achieved, and be deleted within 12 months after performance of the risk assessment at the latest, unless statutory retention obligations apply (e.g. under anti-money laundering, commercial or tax law).

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 Solaris to open an account on your behalf, we collect the following personal data including but not limited to: email, phone number, country of citizenship, country of residency, full name, date of birth, gender, whether you're a US tax resident, employment status, address, Vivid client ID (assigned by us) login credentials.

Identity verification
In order to open an account for you with Solaris, 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 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 Solaris 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 on 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.

Open banking payment initiation
When you use open banking, your personal data is transmitted to authorised third party payment service providers. This data includes your Vivid client ID, address (when it is required), IBAN and the name of the bank you're sending your request to. The login and password information which you are asked to provide is not collected or stored by us.

Visibility and access to your phone's contact book
When you join Vivid, or later, when you first use certain Vivid features and joint banking activities such as Shared Pockets, referral links, instant money transfers, or money requests by phone number, we ask for your consent to make you visible as a Vivid user to other customers and/or to access the contact book on your phone via its operating system.

If you give us this permission, a Vivid icon will appear next to your photo in other customers' contact lists within the Vivid app, and in joint bank activities and recommendation links when you interact with other Vivid customers. This means that other Vivid customers who have your phone number in their contact books can identify you as a Vivid user. You can withdraw this consent anytime in your app's profile settings. The second consent, for Vivid to access the phone book on your device, which you give through your phone's operating system, can also be revoked directly 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. Additionally, in order to verify your transactions and correctly calculate your cashback amounts, we have to share with the merchants or our cashback partners some pseudonymised data about your transactions: date/time, operation amount and currency, merchant data (merchant category code, merchant id and merchant name in case of card operations, IBAN and recipient name in case of direct debits), country and city of purchase, acquirer id, terminal id. If you do not wish that we process or share your data for this purpose, you can object at any time. To do so, please contact us at privacy@vivid.money. Please note that we do not sell or share your 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 (https://vivid.money/en-eu/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 analyse 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 customised 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.

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 Solaris
- Companies that make and deliver your cards
- Cloud computing and storage providers like Amazon Web Services
- Analytics and business intelligence platforms like Mode Analytics, Appsflyer, Amplitude
- Companies that help us send you service related and marketing messages like Amazon SNS
- Payment service providers
- Third party payers (people who pay money into your account) and people you transfer money to
- 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 and Apple Pay
- Analytics service providers
- Cashback partners

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 authorise 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.

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.

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 by anti-money laundering or any other applicable laws, or in cases of potential or ongoing court litigation. When the purpose for processing is fulfilled, but we are required to keep the data, it will be restricted and stored in a secure archive until it can be deleted.

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.
- 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 (a list of national and regional data protection authorities is available on this website). 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. 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 organisation 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.

Last updated: 17 July 2023