

About

Vivid Digital S.r.l. (hereinafter “Vivid Digital”) is part of the Vivid Group of companies (hereinafter “Vivid Group”) who offers its services and products related to buying and selling cryptocurrencies and other digital assets via Vivid mobile application (“Vivid app”) and the website www.vivid.money.

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 by Vivid Digital affiliated companies and its partners, as well as the rights you have with regard to your personal data.

Regarding the terms used in this Privacy Policy, such as “processing” or “controller”, we refer to the definitions of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (hereinafter “GDPR”).

Responsible authority

The controller responsible for the collection and processing of your personal data in accordance with the GDPR is Vivid Digital S.r.l. with registered address at Via dell'Annunciata, 23/4, 20121 Milan, Italy, registered in the Chamber of Commerce of Milan under REI number MI-2640474.

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 or our Privacy Team at privacy@vivid.money.

Why we process your personal data (purposes and legal bases)

1. Contract (Art 6(1) lit. b GDPR)

When you sign up to use our services, it is necessary for us to collect and process certain personal data for the performance of our contract with you or in order to take steps at your request prior to entering into this contract. These data are processed by us, our affiliated companies and any other third parties who help us facilitate the provision of the services. Specific examples of such processing include:

- crypto pocket opening and management;
- execution of your orders;
- customer service and support requests;
- service notifications and emails;
- analysis and improvement of the website and mobile app's performance and the general user experience;

- ensuring security of the website and mobile application (e.g. prevention of fraud and identity theft).

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

2. Legal obligation (Art 6(1) lit. c GDPR)

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 such processing include:

- contract management, accounting and invoicing;
- compliance and risk management;
- Know-Your-Customer measures like capturing of ID copies, authentication process (verification of identity);
- monitoring for prevention of fraud, misuse, money laundering and terrorist financing;
- providing information to fiscal criminal authorities in the context of fiscal criminal proceedings or to prosecution in accordance with official orders.

3. Legitimate interests (Art 6(1) lit. f GDPR)

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:

- preventing criminal activity, such as fraud (device and session data is collected 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;
- data transmission within the Vivid Group for internal administrative purposes;
- measures for safeguarding our network and information security;
- processing inquiries from authorities, lawyers, collection agencies in the course of legal prosecution and enforcement of legal claims in the context of legal proceedings;
- market research, business management and continuing development of services and products;
- processing statistical data, performance data and market research data via the website, the Vivid App or social media platforms.

4. Consent (Art 6(1) lit. a GDPR)

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 services;
- Adding a photo avatar and allowing us to show it to other customers, for example in their contact lists, shared banking activities, or referral links (if you chose to become visible as a customer);
- To access contacts on your device or use other device permissions (e.g. camera, microphone) if necessary;
- To place cookies on your device
- direct marketing and advertising (e.g. customer satisfaction surveys, newsletters, sweepstakes and other advertising communications).

Please note that 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 options. However, keep in mind that the processing which took place before withdrawal remains lawful.

When we process your personal data

Crypto pocket creation.

In order to enter into an agreement with us and create a crypto pocket in your Vivid app, you need to have an existing account with Solarisbank AG. When we create your crypto pocket, we do not ask you to provide us with personal data again, but with your permission, re-use the data you have previously provided in order to enter into a contractual relationship with Vivid Money GmbH and Solarisbank AG. The legal basis for this data processing is Art. 6 (1) lit. b GDPR (processing is necessary for the performance of a contract or steps taken at the request of the data subject prior to entering into a contract).

Identity verification.

In order to facilitate the opening of an account allowing you to use our products and services related to buying and selling cryptocurrencies, it is necessary that you undergo an identification procedure according to the applicable laws and regulations against money laundering and terrorist financing.

For the purpose of identification, we process the personal data you provide or already have provided via Vivid Money GMBH/Solarisbank AG for verification (e.g. photos of you and your ID document, name, date of birth, address, e-mail address, telephone number, desired language, document info - number, issue date, expiration date). This data remains stored by us to fulfill statutory anti money laundering and fraud prevention obligations, and is deleted once applicable retention periods expire.

The legal basis for this data processing is Art. 6 (1) lit. b and c GDPR (processing is necessary for the performance of a contract or steps taken at the request of the data subject prior to entering into a contract and legal obligation).

Orders and transactions.

For the execution of your orders and transactions, we also need to process your personal data: e.g. type and amount of coin, type and amount of currency, price, fees, information about the date and time of the transaction, information about your tariff. The legal basis for this data processing is Art. 6 (1) lit. b GDPR (processing is necessary for the performance of a contract).

Recurring investments.

If you decide to create a savings plan pocket and use our recurring investment service, we will collect and process your personal data, such as information about the rules you set for your plan (e.g. day and time of month when you want us to buy or sell cryptocurrencies for you, amount, status), information relating to the execution of your rules (e.g. status, date and time), and information about the corresponding order. The legal basis for this data processing is Art. 6 (1) lit. b GDPR (processing is necessary for the performance of a contract).

Crypto withdrawals.

When you send crypto to an external wallet, we process data necessary for execution of the transaction on our end, as well as information about this wallet. We also do a compliance check of the receiving wallet (performed by a third party service provider), as required by the FATF guidelines applying to virtual assets service providers in general and Crypto to Crypto transactions in particular.

These data are processed in accordance with Art. 6 (1) lit. b and c GDPR (processing is necessary for the performance of a contract or steps taken at the request of the data subject prior to entering into a contract and legal obligation).

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.

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.

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 services, sometimes we have to share your personal data with affiliated companies, 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 and regulations, which do not allow them to use your data for any other purpose without notifying you or asking for your consent.

Data transfers within the Vivid Group.

Within the Vivid Group, only those teams and employees will receive your personal data who need it to fulfill the contractual and legal obligations and our legitimate interests. We transfer personal data for the purpose of our daily business operations like account management and other operations requested by you, as well as to conduct internal administrative activities and improve our products and services.

Data transfers to service providers.

For certain outsourced activities, we also transmit your personal data to service providers who perform services for us such as video authentication services (e.g. Provider), cloud computing services (Amazon Web Services Inc.), customer support (Intercom, Frontapp), improvement of our website, performance of contracts, account management, accounting, invoicing,

examination of defective or suspicious business cases (Group-IB, Castle), application management and sending out emails and notifications. These service providers are contractually bound to only use or disclose your data to the extent necessary to perform services for us or to comply with legal requirements, as well as to ensure the confidentiality and security of your personal data that they process on our behalf.

Data transfer to public bodies and institutions.

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.

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 do 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 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 www.vivid.money or in the Vivid 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.