Vivid Group Privacy Notice

In this Privacy Notice (**"Notice"**) we describe how the companies of the Vivid Group (collectively **"Vivid", "we", "us"**) collect, process, share, and protect your personal data when you use our products, content, features, technologies, or functions, as well as any related websites and applications offered to you by Vivid Group. It also contains information about your rights with respect to your personal data and how you may exercise them.

About

We provide different Vivid products and services to you. The Vivid company providing the relevant product to you is also responsible for processing your personal data in the context of your use of this product, and is known as the "controller" of your personal data for the respective processing activity. In the digital banking offering available to individuals, Vivid Money GmbH acts as a joint controller with Solaris SE.

You can find detailed information about which Vivid companies are providing you with services below and in the Vivid Money App or the Vivid Website in context of the service or pocket that you are dealing with.

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 Notice, please contact our Privacy Team at privacy@vivid.money or our Data Protection Officer at dpo@vivid.money.

Here is the list of Vivid Group companies that may provide services to you:

Vivid Money GmbH
Zimmerstrasse 78,
10117 Berlin, Germany

Vivid Money GmbH provides to you general and joint services on your Vivid Money App (such as cross functional monthly statements or cost overviews) and may, subject to your marketing settings, send you marketing about the products available on the Vivid Money app.

In cooperation with Solaris SE, Vivid Money GmbH offers a digital current account to individuals. Solaris SE is a credit institution with a German banking license and Vivid Money GmbH leverages Solaris SE infrastructure to offer a direct banking solution under its own brand, and serves as a technology platform. Vivid Money GmbH, which does not have its own banking license and does not provide any banking services in its own name to customers, provides the Vivid Money App, and related infrastructure, the Vivid Money Website, from which the customer

can access the services provided by Solaris SE, as well as customer service, overviews and cashback relating to payments on Solaris SE accounts.

Vivid Money S.A.
Rue Glesener 21,
1631 Luxembourg, Luxembourg

Vivid Money S.A. is an electronic money institution regulated by the Commission de Surveillance du Secteur Financier, Luxembourg under register number W00000015, and authorized to provide payment services related to issuance, circulation and redemption of electronic money and issuance of payment instruments to customers in the European Economic Area.

Vivid Money S.A. provides electronic money accounts and commercial cards, as well as payment facilitation services relating to acquiring of card transactions, to consumers ("Retail Customers"), companies and sole-traders ("Business Customers").

Please note that data protection laws do not apply to information relating to companies, but they do protect information about natural persons. As such, Vivid Money S.A. will process and be the controller of personal data relating to a freelancer, sole trader or proprietor account, or the authorized persons appointed by the Business Customers. If you are a team member or a customer of the company holding a Vivid Business Customer Account, they are the controller of your personal data, and any inquiries should be directed to them.

Vivid Money B.V.
Strawinskylaan 4117
1077 ZX Amsterdam, the Netherlands

Vivid Money B.V. is licensed as an investment firm by the Dutch Authority for the Financial Markets (AFM). It offers the brokerage of transactions for the purchase and sale of financial instruments, including in the context of foreign exchange products, on the Vivid Money App.

Vivid Digital S.r.l.
Viale Andrea Doria 7,
20124 Milan, Italy

Vivid Digital S.r.l. is a virtual asset services provider (VASP) registered with the Italian OAM (*Organismo Agenti e Mediatori*), the Bank of Spain (*Banco de España)* and the French AMF (*Autorité des Marchés Financiers*) that provides services relating to virtual assets to customers in these jurisdictions.

Joint controllers for the Digital Banking offering with Solaris (relates to Retail and Freelancer offering)

Please note that for offering digital bank accounts, Vivid Money GmbH works closely with Solaris SE, 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 GmbH acts as the technology platform. We operate the banking app, provide customer service and, together with Solaris, manage the customer deposits. Vivid Money GmbH 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 Vivid Money GmbH. In order to conclude and execute the respective contracts and to provide our services, Vivid Money GmbH and Solaris need to collect your personal data who 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 Vivid Money GmbH's 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's 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.

What personal data do we collect?

1. Information you provide to us when you:

- register to use the Vivid Mobile App;
- open accounts and use our products and services;
- give us access to your other bank accounts (e.g. for Open Banking);
- correspond or speak with us e.g. via chat, email, phone;
- connect with us on social media;
- fill out forms or respond to surveys.

Depending on the type of Vivid products and services you use, the following personal data may be collected and processed:

- your login credentials;
- identification data, e.g. name, place and date of birth, nationality;
- contact details, e.g. residence address, email address, mobile number, delivery address for your Vivid card. As appropriate, we will use these data for communicating with you on topics such as customer service issues and other business and service related matters;
- copies of identification documents (e.g. passport), photos, video and audio recordings and any other information you provide for identification purposes to prove you are eligible to use our services and products;
- country of residence, tax residency, and tax identification number;
- details of accounts, debit or credit cards you use to add or transfer funds to your Vivid account, including account number, IBAN, BIC, card number, expiration date and CVC/CVV code, transaction amounts;
- information about the other participants in the transactions executed using Vivid mobile app, website or paylink, such as bank account or external crypto wallet details, email or phone number of the participant involved in person-to-person transfer through paylink;
- in the context of Business Customer services, information about the company's directors, shareholders, employees, customers or business partners, if we are legally required to ask for this information (e.g. as part of know-your-customer checks or for compliance with anti-money laundering laws requiring us to verify your company's sources of funds);
- information regarding your employment and income in the course of application for Business, Investment or Crypto oriented services;
- information about other people (e.g. authorized account user, spouse or family members) when you wish to add them to your account, and we must ask for this data in order to comply with our know-your-customer obligations, anti-money laundering and other laws, and to assist with fraud monitoring. In this case, we have to assume that you have their permission to share this information with us;
- information you provide when you communicate with us via chat, email, phone, online, etc;
- data and content shared by you when participating in online discussions, surveys or promotions, including those you post on our social media and community pages;
- photo (if you choose to upload one).

2. Information we automatically collect and process when you use our products and services

Depending on the type of Vivid products and services you use, we may collect and process the following personal data:

- personal data retrieved from your identification documents;

- information about your device, how and when you access our mobile application, trading terminal and any other web based products or services, e.g. the IP address of the device, your login information, type of device, unique device identifier such as IMEI number or MAC address (if available), whether your device uses a VPN, device language, time zone setting, operating system/platform and browser type, mobile network information, software version, Vivid mobile application version, information about pages you look at, page response times, download errors, page interaction information, date and time, how long you stay on certain pages, services viewed or searched for;
- information about your use of Vivid products and services, i.e. data relating to your transactions (e.g. payments into and out of the account, card or financial instrument purchases), including date, time, amount, currency, type and amount of financial instrument or digital asset, type and amount of currency, price, fees, exchange rate, beneficiary details, details of the merchant or ATMs associated with the transaction, IP address of sender and receiver, sender and receiver's name and registration information, messages sent or received with the payment, details of device used to make the payment and the payment method used;
- information about the notifications that have been sent to your email address or mobile device, including date and time, type and category of notification, delivery channel and location (country level), and in some cases information about whether the message was delivered/opened;
- information stored on your device (if you have given us permission), e.g contacts in your phone book, photos, videos or other digital content. In the case of your phone book, we have to assume that you have your contacts' permission to share this information with us;
- if you switch on a location services, we will track the location of your device using GPS technology;
- cookies and similar technologies we use to recognise you, remember your preferences and tailor the content we provide to you;
- risk rating information, e.g. transactional behavior and underwriting information;
- investigations and public information data, e.g. due diligence checks, sanctions and anti-money laundering checks;
- information we need to support our regulatory obligations, e.g. information about transaction details, detection of any suspicious or unusual activity.

3. Information we receive from others:

Depending on the type of Vivid products and services you use, the following personal data may be collected and processed:

- information we receive from other Vivid Group companies, e.g. when your KYC data is internally shared, if you decide and where required to register for additional Vivid products or services, or information about the standing of your other Vivid product accounts (e.g. in the course of a credit application or for defense from legal claims);
- in the context of Business Customer services, if a company that holds a Vivid Business account and nominates you as account administrator or team member, your employer will

give us information about you, e.g. your name, business contact details, employment status, salary and tax information;
- depending on which Vivid products and services you use, we may collect and process personal data from third parties, e.g. financial or credit institutions, credit reference agencies, public registers and similar database providers, as well as authorized account users, fraud prevention agencies and other partners who help us to provide our services;
- information about your transactions from merchants and third party financial institutions (in the context of Open Banking);
- in certain cases we may collect information about you if you make it publicly available online, including, but not limited to public company registers and social media;
- information to help us verify your identity.

We do not 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, data concerning health or data concerning sex life or sexual orientation.
However, there may be circumstances where your transaction data reveals this type of 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 all payment information is kept confidential, and forbid our staff to extract data which belongs to special categories.

Why we process your personal data (purpose and legal basis)

In order to collect and process your personal data, we have to have a valid legal basis. It can be one of the following:

1. Contract

When you apply for and use our products and services, we must collect and process certain personal data, because they are necessary to fulfill our contractual and pre-contractual obligations. For example, we rely on this legal basis to process data when you make payments into and out of your account, make purchases with your Vivid cards, buy or sell financial instruments or digital assets, or require customer service assistance.

Please note that for many of our financial 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 if you refuse to provide us with this information.

2. Legal obligation

In certain cases, we and/or our partners are required to collect, process and store your personal data in order to comply with applicable laws. Some examples of data processing under this legal basis include:

- verification of your identity and age when you apply to use our products and services;
- checks and monitoring relating to prevention of money laundering and fraud;
- tax reporting obligations;
- providing information to fiscal criminal authorities in the context of fiscal criminal proceedings or to prosecution in accordance with official orders;
- compliance check of the receiving crypto wallet, as required by applicable laws implementing the FATF guidelines applying to virtual assets service providers in general and Crypto to Crypto transactions in particular.

3. Legitimate interests

Sometimes we need to collect and process your personal data to safeguard our legitimate interests. Some examples may include:

- developing and improving measures to prevent duplicate account creation, abuse of our services and criminal or suspicious activity such as fraud;
- measures for safeguarding our network and ensuring information security;
- risk management;
- personalizing marketing messages, push notifications and in-app banners in order to offer you services and products that might be interesting to you (if allowed by law). This may include analyzing how you use our products, services and transactions;
- helping you balance your expenses and control your budget by providing subscription protection;
- helping you save money and understand your spending behavior by providing insights about your short and long term spending, and how you use our products and services;
- optimization of your user experience and personalization of services and tariff options by analyzing how you use our products and services;
- preparing anonymous statistical reports that can be shared internally and externally (you cannot be identified from anonymous data);
- data transmission within the Vivid Group for account management, any operations requested by you, to conduct internal administrative activities, and improve our products and services;
- processing of inquiries from authorities, lawyers, collection agencies in the course of legal prosecution and enforcement of legal claims in the context of legal proceedings.

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 to participate in this program and 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.

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, and you will have further options relating to cookies that are not required for the use of our services. You can find more information about them in our Cookie Notice (https://vivid.money/en-eu/cookie-notice/).

4. Consent

If you give us consent, you allow us to process your personal data for purposes such as showing other Vivid customers that you are also our customer, sending you marketing messages about our products and services, adding a photo avatar and showing it to other customers (e.g. in their contact lists, shared banking activities, referral links), or accessing your phone contacts or other system settings on your device.

You can withdraw your consent at any time and without giving any reasons, for example by removing your photo, adjusting your marketing or visibility preferences in your Vivid Money App settings or on your device, or by contacting us. However, keep in mind that any processing which took place prior to the withdrawal of the consent remains lawful.

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 consent, a Vivid icon will appear next to your photo in other customers' contact lists within the Vivid Money 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 withdrawn directly in your device's settings at any time.

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 behavior.

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 analyzes 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.

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).

How we use your personal data for marketing purposes

When you sign up for our services, if it is permitted under applicable national law, we may send you information about Vivid products, services, offers and promotions by post, email, push notification or text message. Where national law requires us to get your consent to send marketing messages, we will do so. If you decide at any time that you no longer wish to receive marketing messages from us, you can always object or opt out by way of changing your marketing preferences.

When you have opted into receiving marketing messages from us, and you open any such e-mail, push or other text messages, we may use technologies, usually web beacons or tracking pixels, in order to track your opening of the message and clicking on links in it. We may also analyze your user behavior by processing data related to your transactions, withdrawals, balance, payments and such, and use this information for structuring personalized marketing campaigns. The purpose is to provide you with marketing based on your interests and to analyze the success of a campaign. If you do not want to be tracked in messages for marketing purposes or that we analyze your behavior for marketing purposes, you can always object by way of changing your marketing settings.

We may also collect and use for marketing purposes your personal information and contact details from publicly available sources, such as websites, online registers or directories. When we do this, we make sure that the information provided to us has been collected and shared

lawfully, that we have a legitimate interest in collecting and using it, and it is balanced against your right to privacy.

Automated decisions

In some cases, the way we analyze your personal data relating to our products and services may involve automated decisions. This means that we will process your personal data using software to evaluate your personal financial circumstances and other factors in order to predict risks or outcomes. This type of data processing can also be called profiling. We do this to make sure that your eligibility for our services and their continued use are determined based on the most accurate and up to date information, and to protect your interests and keep your funds secure. For example, automated methods may be used to make decisions about you in the following situations:

- anti-money laundering and sanctions checks;
- identity and address checks;
- monitoring your account for fraud and other financial crime, either to prevent instances of fraud, or to prevent you from becoming a victim of fraud;
- screening people who may be classed as ‘politically exposed’ (for example, if you are a government minister);
- assessments required by the regulators and relevant authorities to make sure we meet our regulatory obligations (for example, making decisions about those at risk of becoming financially vulnerable).

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. You can contact us to ask to review an automated decision by sending an email to privacy@vivid.money.

When we share or disclose your personal data

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 data connected with your account:

- Vivid Group companies - e.g. when you request to sign up for other Vivid products and services quickly and easily, to prevent fraud and abuse of our services or other Vivid customers, to ensure and improve availability and connectivity of our products and services;

- Our partnering bank and Vivid Money GmbH joint controller Solaris - to provide you with the banking products on our Vivid Money App;
- Companies that make and deliver your cards;
- Payment service providers;
- Mobile payment providers like Google and Apple Pay;
- Other Vivid customers or companies who pay money into your account and to whom you transfer money, share pockets, or split the bill, grant access rights through our functionality (Business Customers), or where you request money from them (in this case we may share your name and phone number as it appears in your account);
- Cloud computing and storage providers like Amazon Web Services;
- Analytics and business intelligence platforms;
- Companies that help us send you service related and marketing messages;
- Providers of software we may use for customer support and issue tracking;
- Companies that help us with customer and operations support;
- 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 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.

In relation to the virtual currency services provided by Vivid Digital S.r.l., it is required to provide the data about the transactions carried out on the territory of the Italian Republic to OAM (Organismo Agenti e Mediatori). OAM processes this data legitimately on the basis of the relevant legislation, but it doesn't have direct contact with you, i.e. the 'Interested Subjects'. As such, you can access the information about how OAM processes your personal data on its website, in a publicly accessible area.

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.

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 - this information is provided within this Privacy Notice.

- 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.
- 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.
- 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.

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 adopted by the European Commission. If you would like to

receive more information about the transfers or safeguards, please contact us at privacy@vivid.money.

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 and regulations, 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.

Security of your information

To help protect the privacy of personal data you provide through the use of our mobile app or websites, 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 Notice

As our organisation and services change from time to time, this Privacy Notice 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 Notice 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 Notice that is in effect and any changes that may have been made to it.

Effective date: 1 March 2024