

Personal Customer Privacy Notice

If you are a business, please see our [Business Privacy Notice](#)

This Privacy Notice is effective from 31 March 2025.

Version Number: 3.0. You can find the previous version [here](#).

You can find below the translations of this Notice.

- [German/Deutsch version](#)
- [French/Français version](#)
- [Portuguese/Português version](#)
- [Chinese/中文 version](#)
- [Hebrew/עברית version](#)
- [Bahasa Indonesia version](#)
- [Japanese/日本語 version](#)
- [Filipino version](#)
- [Turkish/Türkçe version](#)
- [Malay/Melayu version](#)
- [Spanish/Español version](#)

Welcome

This privacy notice (“notice”) explains the types of personal data we collect and how we use and share it. It also tells you about your rights and the choices you can make about how we process your personal data.

Wise offers money transfer services, a Wise account and, in some regions, Assets services (our “services”).

This notice applies to all services provided by the Wise group of companies to our personal account customers globally.

If anything in this notice applies to only one of our services or to customers in a particular country, we’ll clearly highlight it. You can also find [country-specific provisions](#) in the appendices below. For US users, our [US Consumer Privacy Notice](#) applies.

1. [Data Controller](#)
2. [Personal data we collect about you](#)
3. [Ways we use your information](#)

- [**4. How we share your personal data**](#)
- [**5. International data transfers**](#)
- [**6. Profiling and automated decision making**](#)
- [**7. Cookies**](#)
- [**8. Data retention**](#)
- [**9. How we protect your personal information**](#)
- [**10. Your rights**](#)
- [**11. Changes to our Privacy Notice**](#)
- [**12. Contact**](#)

Country specific provisions

- [**1. EEA \(European Economic Area\) - disclosure of your personal data**](#)
- [**2. California residents - your rights**](#)
- [**3. India - Data we collect about you and ways we use your information**](#)
- [**4. Japan - To whom we disclose your personal data**](#)
- [**5. UK anti-fraud agency specific provisions**](#)

1. Data controller

In this notice, "we," "our" or "us" refers to the Wise group company providing you with a product or service and responsible for the handling of your personal data (known as the "data controller").

The services provided by the different Wise companies are listed [here](#).

2. Personal data we collect about you

Personal data, or personal information, means any information about an identified or identifiable individual. It can include data that you provide to us (such as your name, address or contact details) and data that we collect about you during your interaction with our services (such as device information, IP address, etc.). It does not include anonymous data, which cannot be linked back to an individual.

We will collect and process personal data about you in the following ways:

2.1 Information you give us

Information we hold about you will often be information you provided to us directly. For example, when you sign up for a Wise service or take part in online discussions or promotions, you provide certain data that's necessary to your experience. This includes:

- Contact details: your name, email address, postal address, and phone number;
- Personal details: date of birth, passport number or other form of identification information including national identification number (such as your CFP in Brazil or MyNumber in Japan), tax residency, tax reference number, proof of address, and proof of residency;
- Financial information: your bank account number, credit or debit card numbers, and financial history;
- Your image in photo or video form: In some jurisdictions we will also collect facial scan data extracted from your photo or video (known as 'biometric data'). Please refer to our [Facial Scan Privacy Notice](#) and section 3 below for more information on how and why we process this data;
- The content of your communications with us: emails, telephone call recordings and online chat messages;
- Information about your personal circumstances: information that could make you susceptible to harm or in need of extra care to meet our regulatory obligations to support vulnerable customers;
- Source of Funds: information regarding the source of funds or source of wealth, which may include a copy of your bank account statements.

If you fail to provide any information which we tell you is needed to meet legal requirements, it might affect our ability to provide our services to you.

You can ensure that your contact details are current, complete and accurate by logging into your account and updating them at any time in account settings.

If you provide personal data about anyone other than yourself, including a payment counterpart, a friend you have recommended, someone you wish to (or have) set up Group Spending with, individuals in your phone book contact list, or any other person who has a relevant relationship with Wise (a "connected person"), you confirm that you have their agreement or are otherwise entitled to provide this information to us. That includes bringing this notice to their attention if legally necessary.

2.2 Information we collect about you from your use of our services:

This includes:

- Transaction data: details of the transactions you carry out when using our services (for example, payments into and out of your account including beneficiary details and the geographic location from which the transaction originates);
- Information about your devices: details of the internet protocol (IP) address used to connect your device to the internet, your login information, browser

type and version, time zone setting, browser plug-in types and versions, operating system and platform, the type of device you use, whether your device uses a virtual private network (VPN), a unique device identifier (for example, your device's IMEI number, the MAC address of the device's wireless network interface, or the mobile phone number used by the device), mobile network information, your mobile operating system, and the type of mobile browser you use;

- Information about how you are using our Websites or App: details of the products you viewed or searched for, page interaction information, and, if you've installed the app, installed applications on your mobile device that have remote access permissions;
- Behavioural biometrics: details of the way you login and interact with our website or app such as typing cadence, keystroke, touch and mouse behavior to support the detection of fraudulent and suspicious attempts to access your Wise Account;
- Information stored on your device: including your contact list if you give us access to your phone book.

2.3 Information we receive from other sources.

This includes:

- Information from financial institutions: we may receive personal information from other banks and financial institutions. For example, when you ask us to, we may collect information about bank accounts that you choose to connect to your Wise account (for example through Open Banking in the UK or EEA, or when you're setting a direct debit method such as ACH in the US, or EFT in Canada);
- Information from connected persons: if you are a "connected person" for a Wise customer, then that Wise customer may provide your personal data to us. For instance, if you're a payment beneficiary, data could include name, account details, email, and additional verification information if necessary for fulfilling our legal obligations or requested by the recipient bank;
- Advertising networks, analytics providers, and search information providers: may provide us with information about you, including confirmation of how you found our website;
- Information from fraud prevention agencies and government or private databases: In some jurisdictions, we may check the information you have provided to us with government or private identity record databases, fraud prevention agencies, other private entities, or with credit reference agencies to confirm your identity and to combat fraud.
- Information from publicly available sources: We may collect information from publicly available sources, such as media stories, online registers or

directories, and websites for enhanced due diligence checks, and KYC purposes.

2.4 Information from social networks

- If you log into our services using your social network account (including Apple ID, Facebook, or Google) we will receive the information that is necessary for us to authenticate your access, such as your profile and email address, in accordance with the social network's privacy policy.
- When visiting our social network pages, the social media networks (such as Facebook or Instagram) collect personal data about you that they compile into statistics. While we can view these aggregated statistics, we cannot access the underlying personal data or link it to specific individuals or followers.
- We also collect information about you when you use our social network pages (such as Instagram, or LinkedIn) to contact us by creating your own post, tagging us, commenting on our posts, or sending us private messages.
- Occasionally, we'll use publicly available information about you from selected social media networks or media to carry out enhanced due diligence checks.

2.5 Children's data

Our services are designed for adults and are not directed toward children. If we discover we have inadvertently collected data from a child we will take immediate steps to delete that information.

3. Ways we use your information

3.1 Legal basis: We will only use your personal data when the law allows us to. In most cases, our legal basis will be one of the following:

- Contract necessity: where processing personal data is necessary to carry out or enter into our agreement with you (for example, if the processing is needed to make and receive payments);
- Legal obligation: where we have a legal obligation to process your personal data to comply with laws and regulations (such as collecting identification documents to comply with anti-money laundering laws);
- Legitimate interests: where we have a legitimate reason to process your personal data that is reasonable when balanced against your rights and interests (for example, to understand how our services are used and to improve them);
- Consent: where you have given us your consent to process your data;

- Substantial public interest: where we process sensitive or special category data (revealing or relating to someone's health, ethnicity, political views, religious beliefs, sexual orientation, or other protected characteristics) and that processing is in the substantial public interest (for example, to support vulnerable customers).

3.2 Purposes for which we will use your personal data: the ways we plan to use your personal data, along with the corresponding legal bases, are described below. While this table may not list consent as a legal basis for every processing activity, in some countries, such as those where consent is the most appropriate or only lawful basis, we rely on it. For additional details, refer to the country specific appendices [here](#) .

What we use your data for	The legal basis for doing so
<p>To determine if you are eligible to use our services</p> <p>We carry out checks to verify your identity during onboarding in order to comply with Know Your Customer "KYC" obligations under anti-money laundering laws. In some countries , as part of our KYC processes we extract face scan information (known as "biometric data") from a selfie or video that you provide to compare with the picture of you on identity documents (see our Facial Scan Privacy Notice).</p>	<p>Legal obligations</p> <p>Consent (for biometric data collection)</p>

To provide our products and services to you We will process personal data as necessary to:	Contract necessity Legal obligation
<ul style="list-style-type: none"> Provide you with the money transfer and Wise account services you've requested; Where available, to provide you with our Assets product if you chose to use it. Please refer to relevant Asset Customer Agreement, and to the Data Controller Appendix for the entity responsible; Provide Group Spending customers the ability to invite other customers to Group spending; 	
<ul style="list-style-type: none"> Provide you with customer support services, and to monitor or record any communications between you and us, including phone calls, for training and quality purposes; 	Legitimate interests. It is in our legitimate interests to monitor service quality
<ul style="list-style-type: none"> Provide features which make it easier for you to find, be found, and connect with other Wise customers. See section 4 for more details. 	<p>Legitimate interests for certain discoverability features. It is in our legitimate interests to help Wise customers find each other and transfer money easily.</p> <p>Consent (to access your mobile phone contact list and for certain discoverability features). See section 4 for more details.</p>

To ensure account safety, including protecting you from fraud

We process personal data:

- To prevent, detect, or protect against actual or suspected fraud, unauthorised transactions, claims, liability, and financial or other crimes. In some cases this may include collecting biometric data. For example, if you change the phone number linked to your account or to recover access to your account (see our [Facial Scan Privacy Notice](#)). To keep our anti-fraud measures effective, we can't always share all the details about how we prevent fraud;
- As part of our efforts to keep our services safe and secure.

Contract necessity

Legal obligation

Legitimate interests. It is in our legitimate interests to detect, prevent, and investigate fraud, money laundering and other crimes to protect our business and our customers.

Consent for biometric data collection.

Compliance with legal and regulatory obligations protecting our business and enforcing our rights
We may process your personal data:

- To comply with legal and/or regulatory requirements, including to respond to requests from public and government authorities, possibly outside your country of residence, upon demonstration of lawful authority;
- If you use our Assets product, to comply with our obligations to determine your tax status and compliance with associated tax regulations;
- To prevent, detect, or protect against actual or suspected fraud, unauthorised transactions, claims, liability, and financial or other crimes, including conducting or co-operating with investigations of fraud or other illegal activity where we believe it is reasonable and appropriate to do so;
- To take steps to recover amounts owed to us, including via insurance claims, and to allow us to recover or limit damages that we may sustain;
- To allow a third party or a financial institution that incorrectly sent money to recover money received by you in error or due to fraud;
- To verify information you provide to us, and to enforce our Customer Agreement with you;
- To investigate, manage, and resolve complaints;
- To prevent and manage incidents of abusive or aggressive behaviour towards our employees.

Legal obligations
Legitimate Interests (it is in our legitimate interests to protect our business, customers and employees from harm)

Marketing and analytics

- To personalise the marketing messages you receive about products and services we offer so they are more relevant and interesting;
- To measure or understand the effectiveness of our advertising and to deliver relevant advertising to you;
- To provide you with information about other similar products and services we offer which we feel may interest you.

Legitimate interests. It is in our legitimate interests to let our customers know about our products and services which may interest them, to personalise marketing communications and to understand the effectiveness of our advertising. Consent where we are required to collect your consent by law.

Maintaining and improving our services

We may process your personal data:

- To administer our services and for internal operational, planning, audit, troubleshooting, data analysis, testing, research, statistical, and survey purposes;
- To undertake system or product development, including helping third party suppliers improve the services they provide to us;
- To improve our services and to ensure that they are presented in the most effective manner;
- We may use Artificial Intelligence ("AI"), including machine learning models and generative AI large language models (LLMs) to improve the efficiency and effectiveness of our services and our financial crime and fraud prevention processes. We will always let our customers know if they are interacting with an AI system.

Legitimate interests. It is in our legitimate interests to maintain, develop and improve our services.

Understanding if you need extra support We process your personal data to help you if your personal circumstances indicate that you may need extra assistance (for example if you have suffered a bereavement or are experiencing financial difficulties);	Substantial public interest (if we process your sensitive personal data to adhere to legal requirements that apply to us). Consent where we are required to collect your consent by law.
In some countries, it's a legal requirement for us to proactively identify and assist vulnerable customers.	

4. How we share your personal data

We may share your personal data with the following third parties:

4.1 Other [Wise companies](#) may assist in providing our services to you, improving our operations, and supporting business functions such as customer support, technology, marketing, fraud prevention and compliance.

4.2 Service providers acting on our behalf and other partners. We may share your data with trusted third-party service providers and partners, such as:

- Banks and other financial institutions we work with to provide you our services (such as supporting the execution of payments, or provision of the Wise account). These third parties act as independent, separate data controllers who determine why and how they will process your data;
- Advertisers and advertising networks to select and serve relevant advertisements to you and others. This includes social media networks (with whom we share data like your mobile number and email address in a secure format) so they can match this to personal data they already hold about you. They can then display messages to you and others about our products and services, or make sure you do not get irrelevant ads (for example, if you're already using the Wise product that we want to advertise);
- Analytics and search engine providers that assist us in the improvement and optimisation of our site;
- Cloud storage providers and other technology service providers, that provide hosting, IT services, maintenance, and technical support to ensure our platforms and services function smoothly.

These service providers and partners are required to process your data securely and only for the purposes specified in our agreement with them.

4.3 Beneficiaries: that receive limited information when you initiate a payment transaction;

4.4 Regulators, law enforcement agencies, and public authorities, including judicial and administrative courts, if we are under a duty to disclose or share your personal data in response to a subpoena, warrant, court order, properly constituted police request or as otherwise required by law, or in order to enforce or apply our Customer Agreement and other applicable agreements, or to protect the rights, property, or safety of Wise, our customers, our employees, or others;

4.5 Fraud prevention agencies and providers of fraud prevention services to prevent, detect, or protect against actual or suspected fraud, unauthorised transactions, claims, liability, and financial or other crimes, including conducting or co-operating with investigations of fraud or other illegal activity where we believe it is reasonable and appropriate to do so, or where required by law;

4.6 Third parties or a financial institution: to recover debt or in relation to your insolvency or to allow them to recover money received by you in error or due to fraud;

4.7 Business Transfers: In the event of a merger, acquisition, or sale of assets, your data may be transferred to the relevant parties involved in the transaction, subject to confidentiality agreements and applicable data protection law;

4.8 Amazon, as part of the [Amazon Payment Service Provider Programme](#). If your Wise account details are or have been entered into Amazon Seller Central, Amazon may ask us to send them details about you, your accounts, payments from those accounts since 1st January 2015, and external accounts linked to your Wise account. If you do not wish for Wise to provide the above information to Amazon, you should not provide your Wise account details to Amazon and you will not be able to use your Wise account to receive money from your Amazon storefront.

4.9 Other Wise Customers:

As a Wise customer, you will be provided with a unique WiseTag. Other Wise users can search for you in the app using your WiseTag to send or request money.

Our discoverability features also allow other Wise customers to find you using the email or phone number linked to your Wise account without the need for bank details. Default settings might vary depending on the country where you live. You can change them anytime in the app. [Learn more](#)

If you sync your phone's contact list, we will add any of your contacts who are also Wise customers and have discoverability enabled to your recipient list, making it easy to send them money. When other Wise customers who have you as a contact sync their contacts, you will be added to their recipient list if you have discoverability enabled.

For customers who use Group spending, shared balance transaction data is shared with and visible to other members of the Group spending account.

4.10 With Your Consent: In some cases, we may share your information with other third parties when you provide explicit consent to do so.

If you would like further information about who we have shared your data with, or to be provided with a list specific to you, you can request this by writing to privacy@wise.com.

5. International Data Transfers

5.1 As a global provider of money transfer services and multi-currency accounts it is sometimes necessary to transfer your personal data to countries other than your country of residence or to use services supported by our staff (including those of outsourced partners) in other jurisdictions.

5.2 When transferring personal data to other countries we take measures to comply with data protection laws applicable to those transfers. In particular where a transfer is to a country with data protection regulations that do not offer an equivalent level of data protection to your country, we will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this notice.

5.3 When a data transfer mechanism is mandated by applicable law we:

- (i) Transfer to countries or recipients that are recognised as having an adequate level of protection for Personal Data under applicable law;
- (ii) Enter into EU Standard Contractual Clauses approved by the European Commission and the UK International Data Transfer Addendum issued by the Information Commissioner's Office with the data importer.
- (iii) Employ other lawful methods available to us under applicable law.

More information about the third parties to whom we may transfer personal data, their locations, and the contractual arrangements in place to comply with applicable data protection laws can be provided to you if you send a request to privacy@wise.com.

6. Profiling and automated decision making

6.1 We may use some elements of your data, such as your country of residence and transaction history, to customise our services and the information we provide to you, and to address your needs. For example, if you frequently send funds from

one particular currency to another, we may use this data to inform you of new product updates or features that may be useful for you. If you do not want us to process your personal data to personalise electronic marketing communications, you can opt out of receiving electronic marketing communications at any time (see section 10 below).

6.2 We use automated processes to check that your application to access Wise services and your use of Wise services meet our required standard, including verifying your identity, and to help prevent fraud or other illegal activities. These processes may make an automated decision to reject your application or a proposed transaction, to block a suspicious attempt to log into your Wise account, or to close your account. If this happens, you will be notified and offered the opportunity to request further information about how the decision was reached and request a manual review. In any case, if you feel that an automated process may have impacted you, please contact [Wise Customer Support](#).

6.3 If we, a fraud prevention agency, or other third parties providing fraud prevention services determine that a fraud or money laundering risk is posed, we may refuse to provide the services requested or we may stop providing existing products and services to you. A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, or these other third parties, and may result in others refusing to provide services, financing or employment to you.

7. Cookies

7.1 Our website and app use small files known as cookies, along with similar technologies like pixel tags and web beacons. These help us distinguish you from other users, see how you use our site and products while providing you with the best experience. They also enable us to improve our services and make sure that the ads you see online are more relevant to you and your interests. For more information about the cookies and technologies we use, as well as their purposes, see our [Cookie Policy](#).

7.2 We also use pixels or web beacons in some of our emails to help us understand whether our email was delivered and opened, and whether links within the email were clicked. We use this information to measure the performance of our email campaigns, and to help us improve our future email communications.

8. Data Retention

8.1 We will retain your personal data only for as long as is necessary to fulfil the purposes for which we collected it. As a regulated financial institution, Wise is required by law to store some of your personal and transactional data beyond the closure of your account with us. Typically we are required to retain that personal

data for between five and ten years following account closure, depending on applicable laws.

8.2 We will always delete data that is no longer required by a relevant law or jurisdiction in which we operate. We do this automatically, so you don't need to contact us to ask us to delete your data. Deletion methods include shredding, destruction and secure disposal of hardware and hard-copy records, and deletion or over-writing of digital data.

9. How we protect your personal information

9.1 We take the safeguarding of your information very seriously. The transmission of information via the internet is not completely secure. Although we do our best to protect your personal data, we cannot guarantee the security of your data during transmission. Any transmission is at your own risk. Once we have received your information, we use strict procedures and security features to ensure it stays secure, including:

- Communications over the internet between you and Wise systems are encrypted using strong asymmetric encryption. This makes it unreadable to anyone who might be listening in;
- We update and patch our servers in a timely manner;
- We run a [Responsible Disclosure](#) and bug bounty program to identify any security issues in Wise services;
- Our technical security team proactively monitors for abnormal and malicious activity in our servers and services;
- When information you've given us is not in active use, it is encrypted at rest.

You can find out more from our [Security page](#).

9.2 We are regularly audited to confirm we remain compliant with our security certifications, including SOC 2 and PCI-DSS. As part of these audits, our security is validated by external auditors.

9.3 We restrict access to your personal information to those employees of Wise who have a business reason for knowing such information and third party service providers' processing data on our behalf. All Wise employees who have access to your personal data are required to adhere to this notice and all third-party service providers are requested by Wise to ensure appropriate safeguards are in place. In addition, contracts are in place with third-party service providers that have access to your personal data, to ensure that the level of security and protective measures required in your jurisdiction is in place, and that your personal data is processed only as instructed by Wise.

9.4 We continuously educate and train our employees about the importance of confidentiality and privacy of customers' personal information. We maintain physical, technical and organisational safeguards that comply with applicable laws and regulations to protect your personal information from unauthorised access.

10. Your rights

You may have certain rights in relation to the processing of your personal data. Whether or not your local law requires it, Wise will always respond to requests for information about personal data processing, requests for a copy of the personal data we hold about a customer, requests to delete personal data and requests to opt out from receiving direct marketing communications. Other rights may be available depending on your country.

If you have any questions about our use of your personal data, contact us at privacy@wise.com.

Your right	How to exercise your right
------------	----------------------------

Request a copy of your personal data	If you ask us, we will provide you with a copy of the personal data we hold about you. To comply with laws globally and within your region, we will need to exclude certain data such as personal data of third parties and information relating to prevention or detection of crime.
--------------------------------------	---

Request correction of your personal data	We will correct inaccurate or out of date information about you where you ask us to. We may need to verify the accuracy of the new data you provide to us. Certain details can be updated under your settings on the app or website, but we are always happy to assist you via Customer Support channels as well.
--	--

Request deletion of your personal data	<p>You can ask us to delete personal data when:</p> <ul style="list-style-type: none"> (i) there is no good reason for us to continue to process it; (ii) you have successfully exercised your right to object to processing (see below); (iii) we may have processed your personal data unlawfully; (iv) we are required to delete your personal data to comply with laws, or (v) we have been processing with your consent and you withdraw your consent.
	<p>We may not always be able to comply with your deletion request. As a regulated financial institution we are required to hold customers' personal data for a period after the account closure. If we cannot delete your personal data we will always explain why.</p>
Withdraw your consent	<p>Where our lawful basis for processing is based on your consent, you can withdraw your consent at any time. This will not affect the lawfulness of processing which may have taken place before consent was withdrawn. If you withdraw your consent, we may not be able to provide certain products or services to you.</p>
Request to stop direct marketing to you	<p>If you ask us to, we will stop sending direct marketing to you. Our marketing activities may involve profiling you for the purpose of direct marketing. If you object, you can opt out of direct marketing, by contacting us or adjusting your notification preferences in the settings section of your account.</p>
Request human review of an automated decision	<p>Where we use wholly automated decision making-processes, you may request that we provide information about the decision-making methodology and ask us to verify that an automated decision that results in a significant impact on you has been made correctly.</p> <p>We will inform you where we make solely automated decisions that may significantly impact you. You can request human review of automated decisions by contacting Customer Support.</p>

Object to processing based on legitimate interests	If our legal basis for any processing is based on legitimate interests and you disagree with it, you can request an assessment. If there is an overriding reason why we need to process the data (other than in the case of direct marking) we may not accept your request but we will always explain why we need to process your data.
Ask us to suspend processing	<p>You can ask us to suspend the processing of your personal data in the following situations:</p> <ul style="list-style-type: none">(i) if you want us to determine the data's accuracy;(ii) where our processing of the data is unlawful but you do not want us to delete it at this time;(iii) where you want us to retain the data even if we no longer need it because you need it to establish, exercise or defend legal claims; or(iv) you have objected to us using your data but we need to confirm whether or not we have overriding legitimate grounds to continue using it.
Request transfer of your data to another company	If you ask us to, we will provide your chosen third party with the personal data you provided to us in a structured, commonly used, machine-readable format.

11. Changes to our Privacy Policy

To keep up with changing legislation, best practice, and changes in how we process personal information, we may revise this notice at any time. In the case of significant or material changes to this notice, we will let you know.

12. Contact

12.1 Please send any questions, comments or requests about this notice to our privacy team at privacy@wise.com, where you can also contact our Data Protection Officer. You can also write to us or our Data Protection Officer at our registered office that applies to you, as listed [here](#).

12.2 If you feel that we have not addressed your questions or concerns adequately, or you believe that your data protection or privacy rights have been infringed, you

can complain to any supervisory authority or other public body with responsibility for enforcing privacy laws, as listed in the [Data Controller Appendix](#).

In the event of an inconsistency between this privacy notice and the English version, the English version will prevail.

Country specific provisions

If there is a conflict or inconsistency between the privacy notice, [U.S. Consumer Privacy Notice](#) or the appendices below the US Consumer Privacy Notice or the relevant appendix prevails.

Appendix 1 EEA (European Economic Area) - disclosure of your personal data

If you are an EEA resident holding a balance with us (Multi-Currency Account), we are legally obliged to disclose the following personal data to the Central Point of Contact of the National Bank of Belgium ("CPC").

On a continuous basis:

- Belgian bank and payment accounts and powers of attorney on these accounts. For each account, the account number, the capacity of the customer (account holder or proxy holder) and the start or end date of the account must be reported;
- the existence of certain financial contracts concluded in Belgium: start or end date of the contractual relationship with the customer and type of contract;
- the existence of certain financial transactions involving cash: the type of transaction, the capacity of the customer (the customer themselves or their authorised representative) and the date of the transaction.

Periodically:

- the amount standing to the credit of the relevant cash accounts on June 30, and December 31, of each calendar year;
- the "aggregate amount" of such investment services contracts, i.e., the value of the assets under our custody and our liabilities to clients under those contracts on June 30, and December 31, of each calendar year.

To enable identification of the persons behind these accounts, financial contracts and transactions involving cash, we must also report the following information:

- for natural persons: National Register number (or BIS number) or, failing that, last name and first name, date of birth, place of birth (optional) and country of birth;
- for legal persons: number under which they are registered at the Crossroads Bank for Enterprises or, failing that, full name, legal form, if any, and country of establishment.

This data is recorded by the CPC and kept for a period of 10 years. The CPC keeps a list of the information requests it receives for five years.

Under strict conditions, the CPC may disclose this data to the Belgian tax authorities and other authorities and persons that are legally entitled to request information from the CPC. The data may be used in the context of (i) tax-related inquiries, (ii) the investigation of criminal offences, (iii) the combatting of money laundering, terrorist financing and serious criminal offences, and (iv) for any other purpose authorised under Belgian law.

You have the right to consult the data linked to your name by the CPC at the National Bank of Belgium (Boulevard de Berlaimont 14, 1000 Brussels). You may do so by visiting the [NBB's website](#) and following the stipulated process. You also have the right to ask, preferably via us, for any inaccurate data recorded by the CPC and linked to your name to be corrected or deleted.

Appendix 2 California residents - your rights

If you are a California resident:

- You may have certain rights under the California Consumer Privacy Act ("CCPA") regarding your personal data, including:
 - The right to be informed of the personal data we collect, use, and process. Further detail on:
 - the categories of personal data collected,
 - the sources from which we collect it,
 - the business or commercial purposes of collection,
 - as well as the categories of third parties to whom we disclose personal data, are described within the main Privacy Notice , as supplemented by [Wise U.S. Consumer Privacy Notice](#).
 - The right to request the specific pieces of personal data that we have collected about you in the twelve (12) months preceding your request;
 - The right to request deletion of your personal data that we collected;

- The right to correct any inaccurate information that we hold about you;
 - The right to limit the use of your sensitive personal information to only that which is necessary for providing products or services;
 - The right to opt-out of the sale or sharing of personal information, however please note that Wise does not engage in the sale of personal information as described by the CCPA. As detailed in the main Privacy Notice, we share personal information with other businesses for a variety of reasons. While we often benefit from such exchanges, we do not share personal information for the sole purpose of receiving compensation for that information; and
 - The right not to be discriminated against for exercising any of these rights.
- You should be aware that this section does not apply to:
 - Personal information covered by certain sector-specific privacy laws, including the Gramm-Leach-Bliley Act and its implementing regulations, the California Financial Information Privacy Act, and the Driver's Privacy Protection Act of 1994; or
 - Other information subject to a CCPA exception.
- "Shine the Light" and "Eraser" Laws: you may request a list of all third parties to whom we have disclosed certain information during the preceding year for those third parties' direct marketing purposes. Wise does not engage in such practices.
- If you would like to make a request, please submit it in writing to privacy@wise.com, or by contacting us at +1-888-908-3833. We are obliged to verify your identity and that you are authorised to receive this information before fulfilling your request.

Appendix 3 - India - Data we collect about you and ways we use your information

In addition to Section 3 of this Notice, we may also rely on "legitimate use" as a legal basis to process your personal data. For example, we may do so when you voluntarily provide your personal data to us when using our services.

We may collect your Aadhaar-related data, including your demographic details for the purposes of verifying your identity to use our services. We collect your Aadhaar data based on your voluntary and informed consent. Please note that the provision of your Aadhaar-related data is voluntary, and you may choose to provide us with other officially valid documents notified by financial regulators such as passport, voter identification document and driving licence for such purposes. You will not be denied our services in the event you choose not to provide us with your Aadhaar-related data.

If you have questions or concerns relating to this notice or our processing of your personal data, you may contact our grievance officer at privacy@wise.com.

Appendix 4 - Japan - To whom we disclose your personal data

In this Japan specific appendix, 'we' refers to Wise Payments Japan K.K.

We do not disclose your personal data to any third parties unless consented to by you or otherwise permitted by applicable law.

- We may entrust your personal data to third-party service providers, in which case we will execute a service contract with such third parties and supervise them to secure your personal data.
- We jointly use your personal data described in Section 2 of this Privacy notice with Wise Payments Limited (registered in England and Wales (company number 07209813) with its registered office at Worship Square 65 Clifton Street, London EC2A 4JE, a payment services provider registered as a money services business by Her Majesty's Revenue and Customs (HMRC) and under the supervision of the United Kingdom Financial Conduct Authority (FCA), for the purposes described in Section 3 of this notice.
- The responsible party for this joint use is Wise Payments Japan K.K., with headquarters at 2-13-12, Nihonbashi, Chuo-ku, Tokyo, 103-0027. Please contact us at privacy@wise.com for details of the representative director.

Appendix 5 - UK anti-fraud agency specific provisions

1. Before we provide services, goods or financing to you, we undertake checks for the purposes of preventing fraud and money laundering, and to verify your identity. These checks require us to process personal data about you.
2. The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and money laundering, and to verify your identity.
3. Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information, employment details, device identifiers including IP address, and vehicle details.
4. We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.
5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such

processing is also a contractual requirement of the services or financing you have requested.

6. Fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.
7. As part of the processing of your personal data, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk if our processing reveals your behaviour to be consistent with money laundering or known fraudulent conduct, or is inconsistent with your previous submissions, or you appear to have deliberately hidden your true identity. You have rights in relation to automated decision making. If you want to know more please contact us at privacy@wise.com.
8. If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services or financing you have requested, or to employ you, or we may stop providing existing services to you.
9. A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us at privacy@wise.com.
10. Fraud prevention agencies may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place.
11. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data be erased or corrected, and request access to your personal data.
12. For more information or to exercise your data protection rights, please contact us on privacy@wise.com.
13. You also have a right to complain to the Information Commissioner's Office, which regulates the processing of personal data.