



Privacy policy

This Privacy Policy (hereinafter later referred to only as the “**Policy**”) defines the privacy practices employed by **Fintokey**, a platform operated by **Fintokey a.s.**, incorporated in Masarykova 409/26, Brno-mesto, 602 00 Brno, Czech Republic, reg.no.: 09110127 (hereinafter later referred to only as the “**Company**”) in providing and/or receiving the **Service** (as defined in the Terms and conditions) to its customers and/or from providers such as vendors, affiliates, marketing services providers etc. if provided by natural persons and/or companies structure, in which case Company processes personal data of its directors, shareholders and/or employees if necessary (hereinafter referred collectively only as the “**Subjects**” or specifically as “**Client**” / “**Provider**”) and shall be read in the light of the legal agreements and policies provided by Company.

I. Purpose of this privacy policy

This Policy aims to define the process how the Company collects and processes personal data of the Clients through the use of Fintokey.com and its services or within the scope of Company and Provider contractual relationship (hereinafter later referred to only as the “**Website**” or “**Service**”), including any data the Client/Provider may provide through the Website when signing up thereto.

The Services are not intended for minors (persons below 18 years of age) and no data related to minors may be collected.

II. Data controller

The Company is the controller and person/entity responsible for Subject’s personal data. **It is important that the personal data the Company holds about the Subject is accurate and up to date. The Subject is obliged to inform the Company of any changes in his/her personal data.**

Contact details:

Business name:	Fintokey a.s.
reg.no.:	09110127
reg. office:	Masarykova 409/26, Brno-mesto, 602 00 Brno, Czech Republic
e-mail address:	support@fintokey.com

We have appointed a data protection officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the DPO using the details set out below. **It is important that the personal data we hold about you is accurate and current. Please keep us**



informed if your personal data changes during your relationship with us.

DPO: Advokátní kancelář Mgr. Jiří Mikuláščík

Email address: dpo@fintokei.com

Postal address: Masarykova 409/26, Brno-mesto, 602 00 Brno, Czech Republic

Telephone number: +420 608912313

You have the right to make a complaint at any time to Czech Data Protection Commissioner. We would, however, appreciate the chance to deal with your concerns before you approach the Commissioner so please contact us in the first instance.

III. Data collected

Personal data, or personal information, means any information about an individual which may be used to identify that person. It does not include data where the identity has been removed (anonymous data).

As per the conditions defined herein the Company may collect, use, store and transfer different kinds of personal data about the Subject. For the purpose of this policy, the data is divided into the following groups:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier.
- **Contact Data** includes resident address, e-mail address and telephone numbers.
- **Financial Data** includes bank account and payment card details.
- **Transaction Data** includes details about payments to and from you.
- **Technical Data** includes internet protocol (IP) address, Subject's login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices the Subject uses to access Services.
- **Profile Data** includes the username and password of the Subject, his interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how Subject uses the Services.
- **Marketing and Communications Data** includes preferences of the Subject in relation to receiving marketing from the Company and/or third parties and respective communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this

privacy notice.

We do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

IV. If the subject does not provide personal data

Where the Company is required to collect personal data by law, or under the terms of respective agreement with such Subject, but the Subject does not provide such data after being requested so, the Company may not be able to perform the agreement with the Subject (concluded or in the process of conclusion). In such case, the Company may have to cancel the agreement with the Subject with the obligation to notify the Subject thereabout.

V. Fintokey academy

In addition to the data described above, where the Subject accesses or uses the Fintokey Academy mobile application (the “Academy”), the Company processes the following further categories of personal data:

- Authentication data – e-mail address and authentication identifiers used to sign in to the Academy through the Company’s authentication provider (currently Clerk Inc., clerk.com; the production custom authentication domain being academy.fintokey.com). Where the Subject signs in via a single sign-on provider (e.g. Google), the Company receives the e-mail address and the relevant unique identifier from that provider.
- Educational and engagement data – completed lessons, completed quizzes, drills attempted, success rates, experience points (XP), level, daily streaks and other gamified progress data.
- Demo trading data – activity on the in-app demo trading environment (orders, positions, balance, instrument preferences) carried out in a simulated environment with virtual funds.
- Reward and redemption data – unlocked and redeemed Discount Codes for Fintokey evaluation programs, eligibility status and conditions met.
- Device and technical data – device identifier, operating system, application version, language, time zone, IP address and similar technical information necessary to deliver the Academy.

Where the Subject uses the Academy via Guest access, the Company does not associate Academy activity with a registered account, does not store XP, levels, streaks or Discount Codes, and the Subject cannot be identified for marketing or for the issuance of Discount Codes.

Academy event data and selected user properties are transmitted from the Academy to the Company’s Fintokey Admin API, which then forwards relevant data to the Company’s analytics and CRM provider (Bloomreach), in order to identify registered users by e-mail, segment users, automate communications and operate the discount-code mechanics. The legal bases of processing are performance of the



contract with the Subject and the Company's legitimate interests in operating, securing and improving the Academy and converting Academy users into clients of the Company's evaluation programs.

Fintokei academy account deletion

You may request deletion of your account and the related personal data via: (a) the "Delete account" function in the Client zone or the Fintokei Academy app (if available), or (b) e-mail to academy@fintokei.com. We verify identity (typically by a confirmation link to the registered e-mail) and complete the deletion within fourteen (14) days of verification.

Deletion covers the account, profile data (including username, e-mail, password, preferences, XP, level, streaks and redeemed Discount Codes), behavioral events linked to the account, and the authentication record at our authentication provider (Clerk).

VI. How is the subject's personal data collected

The Company uses different methods to collect data from and about the Subject, including the following:

- **Direct interactions.** The Subject may provide his personal data to the Company by filling in forms or by distant communication with the Company via post, phone, email or otherwise. This includes personal data the Subject provides, if he:
 - applies for the Fintokei services by filling the registration form;
 - applies for the Fintokei services by contacting Company's representatives, assigned for the communication with subjects;
 - applies for the Fintokei services through any form of marketing tool (newsletter, landing page, etc.);
 - applies for the Fintokei mobile app.
- **Introducing Brokers and other affiliates:** Company may be provided with Subject's personal data through Company's Introducing Brokers and/or other affiliates. In this case Subject acknowledges that the introducing party may disclose or make available to the Company personal data for the purposes of the services provided by the Company. Both the Company and the Introducing Broker are Controllers of such data for the purpose of providing their services. The Company and the Introducing Broker are acting in common and not jointly in respect of any personal data.
- **Automated technologies or interactions.** As the Subject interacts with the Website and also in accordance with the Cookies policy, technical data about his equipment, browsing actions and patterns may be collected automatically. The Company collects such personal data by using cookies, server logs and other similar technologies. Technical Data about the Subject may also be requested if such Subject visits other websites by employing cookies of the Company.
- **Third parties or publicly available sources.** Company may receive personal data about the

Subject from various third parties and public sources such as:

- analytics providers such as Google based outside the EU;
- advertising networks based outside and within the EU.

VII. How the company uses personal data of the subjects

Subject's personal data will be used only in case where the law allows the Company to do so. Most commonly, Company will use Subject's personal data in the following circumstances:

- where there is a need to perform the agreement (concluded or in a process of conclusion with the Subject),
- where it is necessary for Company's legitimate interests (or those of a third party) unless such interests are overridden by the interests or fundamental rights and freedoms of the Subject,
- where the Company shall comply with a legal or regulatory obligation,
- where freely given, specific, informed and unambiguous consent has been granted by the Subject (if applicable).

In cases not covered by the abovementioned legal grounds for data processing, a consent of the data subject (Subject) is required. This applies particularly to situations when personal data is used for the purposes of third parties direct marketing communications to the Subject via e-mail or text messages. The Subject has the right to withdraw his consent to processing of personal data for marketing purposes at any time by contacting the Company at the following email support@fintokey.com

VIII. Purposes for which the company uses personal data of the subjects

In a table format below, there is a description of all the ways the Company plans to use the personal data of its subjects and the legal bases the Company relies on in such case. The Company has also identified what its legitimate interests are, where appropriate.

Subject's personal data may be processed on more than one lawful ground depending on the specific purpose for which Company uses personal data. If necessary, the Subject may contact the Company at support@fintokey.com for the purpose of obtaining necessary details about the specific legal ground the Company relies on when processing his personal data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To register the Subject as a new Client / Provider	(a) Identity (b) Contact	Performance of agreement with the Subject.

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To manage Company's relationship with the Subject, including: (a) Notification of any changes to the terms or privacy policy (b) Asking the Subject to leave a review or to take a survey	(a) Identity (b) Contact (c) Marketing data	Performance of agreement with the Subject.
To deliver relevant Service content and advertisements to the Subject and to measure or understand the advertising efficiency.	(a) Identity (b) Contact (c) Technical Data (d) Profile Data (e) Usage Data	Performance of a contract with the Subject. Necessary for Company's legitimate interests (study of Subject's behaviour and their use of Fintokei, business growth, marketing strategy information).
For Affiliates – 3 rd parties which introduce Service to Subject, it is necessary to allow access to restricted scope of personal data to allow functionality of specific discounts, cashbacks, promotions, coupons etc.	(a) Identity (b) Contact	Necessary for Company's legitimate interests and generally beneficial to the performance of the agreement, such that it enables the distribution of the Service through intermediaries, including affiliates, thereby facilitating the provision of Services to the Subject on more favorable terms. Subjects who are not linked to any such intermediary are not affected.
To use data analytics to improve the Service, products/services, marketing, customer relationships and experiences.	(a) Identity (b) Contact (c) Technical Data (d) Profile Data (e) Usage Data	Performance of a contract with the Subject. Necessary for Company's legitimate interests (definition of respective Subjects' categories, Service update, business development, marketing strategy development).
To make suggestions and recommendations to the Subject with regard to any product that may be of interest to the Subject.	(a) Identity (b) Contact (c) Technical Data (d) Profile Data (e) Usage Data	Necessary for Company's legitimate interests (business growth and development of portfolio of Subjects with real accounts).
To administer and protect Company's business and the Services (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical Data (d) Profile Data (e) Usage Data	Performance of a contract with the Subject. Necessary for Company's legitimate interests (provision of administration and IT services, network security, fraud prevention, business reorganisation).

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use hashed, first-party user-provided data from our website lead forms for offline lead measurement and server-side event tracking (Conversations API). This allows to track offline conversions and to improve the accuracy of our conversion measurement on platforms like Google and Meta.	(a) Identity (b) Contact (c) Technical	Necessary for our legitimate interests (to help us measure the effectiveness of our ad campaigns)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Identity (b) Contact (c) Technical	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
Asserting legal claims and defence in legal disputes, prevention and investigation of criminal offenses creditors or insolvency administrators requesting foreclosures	(a) Identity (b) Contact (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to able to defend the company status, its interests if necessary or convenient obliged to provide such data to public authorities)
KYC/AML/CFT	(a) Identity (b) Contact	Necessary for Company's legitimate interests Necessary to comply with a legal obligation
To operate, train, evaluate and improve the Fintokey Intelligence analytical / informational tool, including risk modelling, anti-fraud scoring, behavioural pattern analysis and product development.	(a) Technical Data (b) Profile Data (c) Usage Data (d) Transaction Data (where relevant)	Necessary for Company's legitimate interests (operation and improvement of the Fintokey Intelligence tool, risk management, anti-fraud, product development); performance of a contract with the Subject; compliance with a legal obligation (where applicable, e.g. AML/CFT).

IX. Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. If you do not grant us your consent but you are our Client, we are entitled to send you a commercial newsletter (or give you telemarketing calls) under the conditions of directive 2002/58/EC of the European Parliament and of the Council. In any case, you are entitled to reject such marketing communication simply by (a) opting-out button in the newsletter body, (b) using our contact form, or (c) contacting us at the following email dpo@fintokey.com.

X. Promotional offers

Company may use Subject's identity, contact, technical, usage and profile data to form a view with regard to potential needs or possible interests of the Subject. Thus, the Company may provide products, services and offers relevant for the Subject (marketing purposes form a legitimate interest of the Company in relation to its products or services).

The Subject may receive marketing communications from the Company only if he has requested information from the Company or provided his details when accessing the Service for the purpose of



receiving information and, in each case, not opting out the receipt of marketing notifications.

We may use the Google Enhanced Conversions tool, which is a feature that allows the offline tracking of conversions. We use it to track performance back to our Google ad campaigns in a secure and privacy compliant way. This helps us improve the accuracy of our conversion measurement, optimize our ad campaigns better and it allows us to measure their effectiveness in order to improve our services. We do not share any personal information with third-parties while using Google Enhanced Conversions.

Similarly, we utilize the Meta Conversions API (CAPI). This server-side tracking technology allows us to send specific web events (such as form submissions or account registrations) directly from our server to Meta (Facebook/Instagram). To protect your privacy, we transmit only hashed (pseudonymized) personal data—such as your email address or phone number—which Meta matches against its existing user database. This process enables us to measure the effectiveness of our advertising campaigns and optimize ad delivery accurately, independent of browser-based cookies. The data is hashed before transmission and is processed strictly for attribution and optimization purposes in accordance with Meta’s data processing terms.

XI. Third-party marketing

Before sharing Subject’s personal data for marketing purposes with any company outside Fintokei group of companies, the Company needs an express opt-in consent of the Subject.

XII. Opting out

The Subject shall have the right to ask the Company or third parties to stop sending any marketing messages at any time by following the opt-out links in any marketing message sent to him or by contacting the Company at any time at the following e-mail address: support@fintokei.com or dpo@fintokei.com.

XIII. Cookies

The Subject shall have the right to set his browser to refuse all or some cookies, or to alter the settings or access of cookies on the Website. If you disable or refuse cookies, please note that some parts of this Website may become inaccessible or not function properly. For more information about the cookies Company uses, please see the Cookies Policy.

XIV. Change of purpose

Personal data of the Subject may be used for the purposes for which they have been collected, unless the legal basis of processing the data enables the Company to use it for other purpose and such purpose is compatible with the original one.

In case of data use for an unrelated purpose, the Company shall notify the Subject and explain the legal basis therefor. Subject's personal data may be processed without his knowledge or consent only in compliance with the rules specified above, where such use is required or permitted by the law.

XV. Disclosure of subject's personal data to third parties

The Company may share Subject's personal data with third parties for the purpose of carrying out its services related to Fintokey properly. Security of Subject's personal data shall be fully respected by such third parties and treated in accordance with the law. Such Subject's personal data may not be used by third parties for their own purposes while they may be processed only for specified purposes by the Company and in accordance with Company's instructions.

Company's service providers and vicarious agents may also receive data for these purposes if they maintain business confidentiality. These companies deliver IT services, logistics, printing services, legal, accounting, telecommunications and consulting as well as sales and marketing.

With regard to the transfer of data to recipients outside of the Company, it should first be noted that Company commits itself to secrecy about all customer-related facts and valuations from which it become aware. In principle, Company may only disclose information about the Subject if required by statutory provisions, if Subject has given the consent, or if the Company is otherwise authorized to provide information. Under these conditions, in the case of a legal or regulatory obligation, recipients of personal data may be public bodies and institutions (e.g. regulatory authorities, tax authorities, law enforcement authorities).

Other data recipients may be those for whom the Subject have given the consent to submit the data or to whom Company may delegate personal information due to legitimate interests.

XVI. Data security

The Company is obliged to put appropriate security measures in place to prevent Subject's personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, the Company shall limit access to Subject's personal data to only such employees or third parties that are actively participating on the performance of subject of the Agreement. Such employees or third parties will only process Subject's personal data on the basis of Company's instructions while respecting the duty of confidentiality.

The Company shall implement procedures to deal with any suspected personal data breach and notify

the Subject and any applicable regulator thereabout, where legally required so.

XVII. GOOGLE recaptcha

The Website and certain Company applications use Google reCAPTCHA (including reCAPTCHA Enterprise) provided by Google LLC and/or Google Ireland Limited (“Google”) to protect against fraudulent activity, bot traffic, account takeover, abuse and spam. For these purposes, reCAPTCHA collects technical information such as IP address, device and browser characteristics, mouse and touch interactions, and other behavioural and environmental signals, and transmits them to Google for analysis.

With effect from 2 April 2026, Google operates reCAPTCHA as a data processor on behalf of its customers. Accordingly, the Company acts as the data controller in respect of personal data collected through reCAPTCHA on the Company’s digital surfaces, and Google processes such data on the Company’s behalf under the Google Cloud Platform Service Specific Terms and the Google Cloud Data Processing Addendum. For information about how Google processes reCAPTCHA data and Google’s applicable security and sub-processor commitments, please refer to those documents available at cloud.google.com/terms.

The legal basis for the Company’s use of reCAPTCHA is the Company’s legitimate interest in preventing fraud, abuse and unauthorised access to the Service, in protecting the Subject’s account and in maintaining the security and integrity of the Company’s systems. Where consent is required for the placement of reCAPTCHA cookies or similar technologies on the Subject’s device, such consent is collected through the Company’s cookie banner; for further information, please see the Cookies Policy.

XVIII. International transfers

The Company might need on certain occasions for the purposes of carrying out the services to transfer personal data outside the European Economic Area (EEA).

Whenever the Company transfers Subject’s personal data out of the EEA, Company ensures a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Company will only transfer personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- Where Company uses certain service providers, Company may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.

XIX. Automated decision-making and profiling

The Company may carry out limited profiling activities for fraud prevention, anti-money-laundering, risk-management and security purposes (including bot/fraud scoring through reCAPTCHA and similar tools), as well as for the operation of the Fintokey Intelligence analytical tool and for marketing segmentation. The Company does not subject the Subject to decisions producing legal effects concerning him/her or similarly significantly affecting him/her based solely on automated processing within the meaning of Article 22 GDPR, unless such decision is necessary for the performance of a contract, authorised by Union or Member State law, or based on the Subject's explicit consent, in each case with appropriate safeguards including the right to obtain human intervention, to express the Subject's point of view and to contest the decision.

XX. Personal data breaches

The Company maintains procedures to detect, contain and remediate personal data breaches. Where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Company will notify the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, in accordance with Article 33 GDPR. Where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company will also communicate the breach to the affected Subjects without undue delay, in accordance with Article 34 GDPR.

XXI. Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every Subject in the European Economic Area has the right to lodge a complaint with a supervisory authority, in particular in the EEA Member State of his/her habitual residence, place of work or place of the alleged infringement, in accordance with Article 77 GDPR. For Czech residents this is the Czech Data Protection Authority (Úřad pro ochranu osobních údajů, www.uoou.cz). A list of EEA supervisory authorities is published by the European Data Protection Board (edpb.europa.eu).

XXII. Jurisdiction-specific provisions

This section sets out provisions that apply, in addition to and as a supplement to the remainder of this Policy, to natural persons depending on their place of residence or other connection to a specific jurisdiction. In the event of any conflict between this section and the remainder of this Policy in respect of a person to whom a sub-section below applies, the applicable sub-section shall prevail to the extent of the conflict. Capitalised terms not defined here have the meaning given elsewhere in this Policy.

A. Residents of the Republic of Korea (PIPA)

This sub-section applies to natural persons who are information subjects under the Personal Information Protection Act of the Republic of Korea (Act No. 10465, as amended; "PIPA").

i. Status of the Company and basis of processing

The Company is the “personal information controller” (개인정보처리자) in respect of the personal information of Korean information subjects collected through the Website, the Client zone, the Trading Platform, the Fintokey simulated accounts, the Fintokey Academy mobile application, the Fintokey Intelligence tool and any other Ancillary Service. Pursuant to Articles 15, 17, 22-2, 23 and 28-8 of PIPA, the Company processes personal information of Korean information subjects on the basis of the prior, freely-given, specific and informed consent set out below, supplemented by other lawful bases recognised by PIPA where applicable (in particular performance of a contract with the information subject and compliance with statutory obligations).

ii. Consent grants by the Korean information subject

By ticking the relevant consent box(es) at the point of registration and/or by continuing to use the Service after being presented with this Policy in the Republic of Korea, the Korean information subject expressly grants the following consents. Each consent below is independent and may be granted or refused separately; refusal of consents marked as “required” may make the relevant part of the Service unavailable.

- (Required — Article 15 PIPA) I consent to the collection and use by the Company of my Identity Data, Contact Data, Financial Data, Transaction Data, Technical Data, Profile Data, Usage Data and Marketing and Communications Data, as described in this Policy, for the purposes of (i) registering and managing my account, (ii) providing and maintaining the Service (including the Client zone, Trading Platform, Fintokey simulated accounts, Fintokey Academy and Fintokey Intelligence), (iii) processing payments, (iv) customer support, (v) fraud and abuse prevention, KYC/AML/CFT, and (vi) compliance with applicable law. The retention period is as set out in the “DATA RETENTION” section of this Policy.
- (Required — Article 17 PIPA) I consent to the provision by the Company of my personal information to third-party processors and recipients as described in the “DISCLOSURE OF SUBJECT’S PERSONAL DATA TO THIRD PARTIES” section of this Policy, including IT, hosting, analytics, payment, authentication, anti-fraud, communications and legal service providers, solely for the purposes set out in that section.
- (Required — Article 28-8 PIPA) I consent to the cross-border transfer of my personal information to recipients located outside the Republic of Korea (including the European Economic Area, the United Kingdom, and other jurisdictions where the Company and its processors operate). The categories of personal information transferred, the recipients, the countries of destination, the purposes of transfer, the retention periods and the contact point for inquiries are as described in this Policy. The transfer is carried out through electronic means via the Company’s information and communications network.
- (Optional — Article 22-2 PIPA) I consent to the use of my Contact Data and Marketing and Communications Data by the Company for direct marketing communications, including by e-mail and any other electronic means, regarding the Service, related products, promotions and

offers. I may withdraw this consent at any time as described below without affecting access to the Service.

- (Optional — Article 23 PIPA — sensitive information) The Company does not, in principle, collect sensitive information (민감정보) about Korean information subjects. Should the Company be required to collect any sensitive information for legal or contractual reasons (e.g. limited categories required for KYC/AML purposes), the Company will obtain a separate, specific consent in advance.

iii. Withdrawal of consent

The Korean information subject may withdraw any consent given under this sub-section at any time by contacting the Company at support@fintokey.com or the DPO at dpo@fintokey.com. Withdrawal does not affect the lawfulness of processing carried out before withdrawal. Withdrawal of a required consent may result in the Company being unable to continue providing the relevant part of the Service.

iv. Rights of the Korean information subject

In addition to the rights described in the “LEGAL RIGHTS OF THE SUBJECTS” section of this Policy, the Korean information subject has, under PIPA, the right to: (i) request access to and a copy of personal information held about him/her (Article 35); (ii) request correction or deletion (Article 36); (iii) request suspension of processing (Article 37); (iv) be notified of personal-information breaches (Article 34); and (v) file a complaint with the Personal Information Protection Commission (개인정보보호위원회) or with the Korea Internet & Security Agency Personal Information Infringement Report Center (privacy.go.kr).

v. Domestic representative (Article 31-2 PIPA)

Where the Company meets the statutory thresholds in Article 31-2 PIPA and the related Enforcement Decree (broadly, foreign information and communications services providers without an address or place of business in Korea whose previous-year annual total turnover reaches KRW 1 trillion or which store/manage on average 1 million or more Korean information subjects’ personal information per day during the relevant three-month period), the Company will appoint and disclose a domestic representative in Korea and update the contact details accordingly. Until such appointment, the contact details for the DPO set out in this Policy apply.

vi. Children under 14

The Service is not intended for and is not directed at children under 14 years of age. The Company does not knowingly collect personal information from a Korean child under 14 without the prior consent of his/her legal representative.

vii. Contact and complaints

Questions, requests and complaints relating to the processing of personal information of Korean information subjects may be sent to support@fintokey.com or to the DPO at dpo@fintokey.com. The

Korean information subject may also file a complaint with the Personal Information Protection Commission (www.pipc.go.kr).

B. Residents of Japan (APPI)

This sub-section applies to natural persons whose personal information is processed in the context of their connection to Japan and which therefore falls within the scope of the Act on the Protection of Personal Information of Japan (Act No. 57 of 2003, as amended; “APPI”). It applies in particular by virtue of the extraterritorial provisions of Article 171 APPI.

i. Status of the Company and purposes of use

The Company is a “personal information handling business operator” (個人情報取扱事業者) under APPI in respect of the personal information of Japanese information subjects. In accordance with Articles 17 and 21 APPI, the Company specifies the purposes of use of personal information as set out in the “PURPOSES FOR WHICH THE COMPANY USES PERSONAL DATA OF THE SUBJECTS” section of this Policy (including, where applicable, the purposes related to Fintokey Academy and Fintokey Intelligence) and uses personal information only within the scope necessary to achieve those purposes.

ii. Consent grants by the Japanese information subject

By ticking the relevant consent box(es) at the point of registration and/or by continuing to use the Service after being presented with this Policy in Japan, the Japanese information subject expressly grants the following consents. Each consent below is independent and may be granted or refused separately; refusal of consents marked as “required” may make the relevant part of the Service unavailable.

- (Required — Articles 17 and 21 APPI) I consent to the use by the Company of my personal information for the purposes of use specified in this Policy, including the operation of the Service, the Fintokey Academy and the Fintokey Intelligence tool, customer support, fraud and abuse prevention, KYC/AML/CFT, and compliance with applicable law.
- (Required — Article 27 APPI) I consent to the provision by the Company of my personal information to third parties as described in the “DISCLOSURE OF SUBJECT’S PERSONAL DATA TO THIRD PARTIES” section of this Policy, for the purposes set out in that section. Where the recipient acts as a contractor (委託先) under Article 25 APPI, the Company supervises such contractor and no separate consent is required.
- (Required — Article 28 APPI) I consent to the provision by the Company of my personal information to third parties located in a foreign country outside Japan (including the European Economic Area, the United Kingdom and other jurisdictions where the Company and its processors operate). I acknowledge that I have been provided with the information required under Article 28 APPI, including the name of the relevant foreign country, information on the relevant data-protection system of that country (where reasonably available), and information

on the measures taken by the recipient for the protection of personal information, in each case as further described in this Policy and on request from the DPO.

- (Optional — Article 27 APPI) I consent to the use of my Contact Data and Marketing and Communications Data by the Company for direct marketing communications, including by e-mail and any other electronic means, regarding the Service, related products, promotions and offers. I may withdraw this consent at any time without affecting access to the Service.
- (Required where applicable — Article 20(2) APPI) The Company does not, in principle, collect special care-required personal information (要配慮個人情報) about Japanese information subjects. Should the Company be required to collect any such information for legal or contractual reasons (e.g. KYC/AML), the Company will obtain a separate, specific consent in advance.

iii. Withdrawal of consent

The Japanese information subject may withdraw any consent given under this sub-section at any time by contacting the Company at support@fintokey.com or the DPO at dpo@fintokey.com. Withdrawal does not affect the lawfulness of processing carried out before withdrawal. Withdrawal of a required consent may result in the Company being unable to continue providing the relevant part of the Service.

iv. Rights of the Japanese information subject

In addition to the rights described in the “LEGAL RIGHTS OF THE SUBJECTS” section of this Policy, the Japanese information subject has, under APPI, the right to: (i) request disclosure of retained personal information and of third-party-provision records (Articles 33 and 33-2); (ii) request correction, addition or deletion (Article 34); (iii) request suspension of use, deletion or suspension of third-party provision (Articles 35 and 35(3)); and (iv) lodge a complaint with the Company directly. Requests may be sent to support@fintokey.com or to the DPO at dpo@fintokey.com.

v. Complaints and supervisory authority

The Japanese information subject may file a complaint with the Personal Information Protection Commission of Japan (個人情報保護委員会, www.ppc.go.jp).

vi. Children

The Service is not intended for and is not directed at children. The Company does not knowingly collect personal information from a Japanese child under 16 years of age without the prior consent of his/her legal representative.

XXIII. Data retention

Personal data of the Subject shall be retained for as long as necessary to meet the purposes for which they were collected, including the purposes of satisfying any legal, accounting, or reporting requirements.

For the purpose of determination of appropriate retention period for personal data, the Company shall consider the number, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of such personal data, the purposes for which such personal data is processed and if these purposes may be achieved through other means, and the applicable legal requirements.

Personal data processed based on the legitimate interests of the Company for the duration of five years following the termination of the last Contracts. This period concludes upon the commencement of another Contract, at which point a new period begins, and the processing of personal data resumes accordingly.

In some circumstances you can ask us to delete your data: see Request erasure below for further information. In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

If the processing of the personal data requires consent (such as marketing or other purposes stated herein), the data retention period may differ according its very purpose. If not stated otherwise, personal data are processed for the period of 5 years or until Subject withdraws his/her consent.

Processing of personal data of service providers defined above takes five years after they cease being service providers.

Preservation of evidence for other purposes within the statutory limitation period.

Personal data contained in e-mail, chats, phone calls and other means of distant communication might be processed according to the related and relevant purpose specified herein. Processing period might be up to 5 years.

Retained beyond deletion of Fintokey Academy account, in the minimum scope: accounting and tax records — 10 years; KYC/AML records — 10 years from end of the business relationship; data needed to assert or defend legal claims — 4 years; any data whose retention is required by other applicable law. Retained data is access-restricted and used only for that legal purpose.

XXIV. Legal rights of the subjects

Any Subject shall have following rights under data protection laws in relation to his personal data:

- **Request access** to his personal data (commonly known as a “data subject access request”). The Subject is allowed to receive a copy of personal data the Company keeps about him and to check that such data is lawfully processed.
- **Request correction** of his personal data. The Subject may request correction of any incomplete or inaccurate data the Company keeps about him, though the Company may need to verify the accuracy of the new data the Subject provides.
- **Request erasure** of his personal data. The Subject has the right to request the Company to delete or remove personal data where there is no appropriate reason for the Company to process it. The Subject may also request the Company to delete or remove his personal data where he has successfully exercised his right to object to processing (see below), where his information

may have been processed unlawfully or where the Company is required to erase his personal data to comply with local law. The Company may, however, refuse to comply with Subject's request, if the applicable law allows it for specific reasons, which the Subject shall be notified of.

- **Object to processing** of his personal data if the Company relies on a legitimate interest (or those of a third party) but the Subject believes such processing affects his fundamental rights and freedoms. The Subject may also object to processing of his personal data for direct marketing purposes. In justified cases, the Company may prove that it has compelling legitimate grounds to process Subject's information, overriding his rights and freedoms.
- **Request restriction of processing** of his personal data. This allows the Subject to ask the Company to suspend the processing of his personal data in the following scenarios: (a) if the Subject wants the Company to establish the data's accuracy; (b) where Company's use of the data is unlawful but the Subject does not want the Company to erase it; (c) where the Subject needs the Company to keep the data, even if no longer required by the Company, as he may need it to establish, exercise or defend legal claims; or (d) the Subject has objected to Company's use of his data but the Company needs to verify whether it has overriding legitimate grounds to use it.
- **Request the transfer** of his personal data to him or to any third party. The Company will provide such personal data to the Subject or respective third party of his choice in a structured, commonly used, machine-readable format. This right only applies to automated information which the Subject initially provided consent for to the Company to use or where the Company used the information to perform a contract with the Subject.
- **Withdraw consent at any time** where the Company relies on consent to process Subject's personal data. However, this will not affect the lawfulness of any processing carried out before the Subject withdraws his consent.

XXV. No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

XXVI. Children's privacy

We do not knowingly collect any information from anyone under 15 years of age. Our websites, products and services are all directed to people who are at least 15 years old or older. If you are under 15, do not use or provide any information on these websites or on or through any of its features / register on the websites, make any purchases through the websites or provide any information about yourself to us, including your name, address, telephone number or email address. If we learn that we have collected or received personal data from a child under 15, we will delete that information.

XXVII. What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

XXVIII. Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.