



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.

Fintokey 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 Fintokey Academy app (if available), or (b) e-mail to academy@fintokey.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 Fintokey services by filling the registration form;
 - applies for the Fintokey services by contacting Company's representatives, assigned for the communication with subjects;
 - applies for the Fintokey services through any form of marketing tool (newsletter, landing page, etc.);
 - applies for the Fintokey 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 Fintokei 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 Fintokei 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@fintokei.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 Fintokey 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@fintokey.com or dpo@fintokey.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 Fintokei 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 Fintokei 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 Fintokei simulated accounts, the Fintokei Academy mobile application, the Fintokei 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, Fintokei simulated accounts, Fintokei Academy and Fintokei 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 Fintokei 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.

プライバシーポリシー

本プライバシーポリシー（以下「**本ポリシー**」といいます。）は、**Fintokey**（チェコ共和国 Masarykova 409/26, Brno-město, 602 00 Brno に所在し、登録番号09110127を有する **Fintokey a.s.**（以下「**当社**」といいます。）が運営するプラットフォームです。）が、自然人又は法人組織により提供される場合において、その顧客に対して、又はベンダー、アフィリエイト、マーケティングサービス提供者等のプロバイダーから、一般取引条件で定義される**本サービス**を提供し、若しくは受領するに当たって採用するプライバシー上の取扱いを定めるものです。当該の場合、当社は必要に応じてその取締役、株主及び/又は従業員の個人データを処理します（以下、これらを総称して「**データ主体**」といい、個別に「**顧客**」又は「**プロバイダー**」といいます。）。本ポリシーは、当社が提供する法的合意及び方針に照らして解釈されるものとします。

I. 本プライバシーポリシーの目的

本ポリシーは、Fintokey.com 及びその各サービスの利用を通じて、又は当社とプロバイダーとの契約関係の範囲内において（以下「**本ウェブサイト**」又は「**本サービス**」といいます。）、当社が顧客の個人データをどのように収集し処理するかという過程を定めることを目的とします。これには、顧客／プロバイダーが本ウェブサイトへの登録時に提供する一切のデータを含みます。

本サービスは未成年者（18歳未満の者）を対象としておらず、未成年者に関するデータを収集することはありません。

II. データ管理者

当社は、データ主体の個人データについて責任を負う管理者です。当社がデータ主体について保有する個人データが正確かつ最新であることは重要です。データ主体は、自己の個人データに変更が生じた場合、当社に通知する義務を負います。

連絡先：

商号： **Fintokey a.s.**

登録番号： 09110127

登記上の所在地： Masarykova 409/26, Brno-město, 602 00 Brno, チェコ共和国

電子メールアドレス： support@fintokey.com

当社は、本プライバシー通知に関する事項を統括する責任者として、データ保護責任者（DPO）を選任しています。本プライバシー通知に関するご質問（法的権利の行使に関するご請求を含みます。）がある場合には、以下の連絡先によりDPOまでご連絡ください。当社が保有する貴方の個人データが正確かつ最新であることは重要です。当社との関係が継続する間に個人データに変更が生じた場合には、当社にお知らせください。

DPO：

電子メールアドレス： dpo@fintokey.com

郵送先住所： Masarykova 409/26, Brno-město, 602 00 Brno, チェコ共和国

電話番号： +420 608912313

貴方は、いつでもチェコ・データ保護監督機関に対して異議を申し立てる権利を有します。もっとも、当社としては、監督機関に申し立てる前にまず当社にご連絡いただき、貴方の懸念に対応する機会を頂ければ幸いです。

III. 収集する個人データ

個人データ又は個人情報とは、個人を識別するために用いることができる、当該個人に関する一切の情報をいいます。これには、識別性が除去されたデータ（匿名データ）は含まれません。

本ポリシーに定める条件に従い、当社はデータ主体に関する様々な種類の個人データを収集し、利用し、保管し、移転することがあります。本ポリシーの目的上、データは次の各区分に分類されます。

- **識別データ**には、名、旧姓、姓、ユーザー名又はこれに類する識別子が含まれます。
- **連絡先データ**には、居住地住所、電子メールアドレス及び電話番号が含まれます。
- **金融データ**には、銀行口座及び決済カードの情報が含まれます。
- **取引データ**には、貴方への支払い及び貴方からの支払いに関する詳細が含まれます。
- **技術データ**には、インターネットプロトコル（IP）アドレス、データ主体のログイ

ンデータ、ブラウザの種類及びバージョン、タイムゾーン設定及び所在地、ブラウザのプラグインの種類及びバージョン、オペレーティングシステム及びプラットフォーム、並びにデータ主体が本サービスへのアクセスに用いる機器上のその他の技術が含まれます。

- **プロフィールデータ**には、データ主体のユーザー名及びパスワード、関心事項、嗜好、フィードバック並びにアンケートへの回答が含まれます。
- **利用データ**には、データ主体による本サービスの利用方法に関する情報が含まれます。
- **マーケティング・コミュニケーションデータ**には、当社及び/又は第三者からのマーケティングの受領に関するデータ主体の嗜好、並びに関連するコミュニケーション上の嗜好が含まれます。

当社はまた、統計的又は人口統計的データ等の**集約データ**を、あらゆる目的のために収集、利用及び共有します。集約データは貴方の個人データから導出されることがありますが、当該データは貴方の身元を直接又は間接に明らかにするものではないため、法律上は個人データとはみなされません。例えば、当社は特定のウェブサイト機能にアクセスする利用者の割合を算出するために貴方の利用データを集約することがあります。ただし、当社が集約データを貴方の個人データと結合又は関連付け、それにより貴方を直接又は間接に識別し得るようになった場合には、当社は当該結合データを個人データとして取り扱い、本プライバシー通知に従って利用します。

当社は、貴方に関する**特別な種類の個人データ**（人種若しくは民族、宗教上若しくは思想上の信条、性生活、性的指向、政治的意見、労働組合への加入、健康に関する情報、遺伝データ及び生体データに関する詳細を含みます。）を収集しません。また、犯罪歴及び犯罪行為に関する情報も収集しません。

IV. データ主体が個人データを提供しない場合

法律により、又は当該データ主体との該当する合意の条件に基づき、当社が個人データを収集することを要求されているにもかかわらず、要請後もデータ主体が当該データを提供しない場合、当社はデータ主体との合意（締結済み又は締結手続中のもの）を履行できないことがあります。この場合、当社はデータ主体との合意を解除せざるを得ないことがあります、その旨をデータ主体に通知する義務を負います。

V. Fintokey Academy

上記のデータに加え、データ主体が Fintokei Academy モバイルアプリケーション（以下「アカデミー」といいます。）にアクセスし又はこれを利用する場合、当社は次の追加区分の個人データを処理します。

- 認証データ – 当社の認証プロバイダー（現在は Clerk Inc.、clerk.com。本番用カスタム認証ドメインは academy.fintokei.com）を通じてアカデミーにサインインするために用いられる電子メールアドレス及び認証識別子。データ主体がシングルサインオンプロバイダー（例：Google）を通じてサインインする場合、当社は当該プロバイダーから電子メールアドレス及び該当する一意の識別子を受領します。
- 教育・エンゲージメントデータ – 修了したレッスン、修了したクイズ、試行したドリル、正答率、経験値（XP）、レベル、デイリーストリーク、その他のゲーミフィケーション化された進捗データ。
- デモ取引データ – 仮想資金を用いたシミュレーション環境において行われる、アプリ内デモ取引環境での活動（注文、ポジション、残高、銘柄の嗜好）。
- 報酬・引換データ – Fintokei の評価プログラムに適用される、解放済み及び使用済みの割引コード、適格性のステータス並びに充足された条件。
- デバイス・技術データ – デバイス識別子、オペレーティングシステム、アプリケーションのバージョン、言語、タイムゾーン、IPアドレス、その他アカデミーの提供に必要なこれに類する技術情報。

データ主体がゲストアクセスによりアカデミーを利用する場合、当社はアカデミー上の活動を登録アカウントに紐付けず、XP、レベル、ストリーク又は割引コードを保存せず、また、マーケティング又は割引コードの発行のためにデータ主体を識別することはできません。

アカデミーのイベントデータ及び選択された利用者属性は、アカデミーから当社の Fintokei Admin API へ送信され、同 API は、登録利用者を電子メールにより識別し、利用者をセグメント化し、コミュニケーションを自動化し、割引コードの仕組みを運用するために、関連データを当社の分析・CRMプロバイダー（Bloomreach）へ転送します。処理の法的根拠は、データ主体との契約の履行、並びにアカデミーの運用・保護・改善及びアカデミー利用者を当社評価プログラムの顧客へ転換することに係る当社の正当な利益です。

Fintokei Academy アカウントの削除

貴方は、(a) クライアントゾーン又は Fintokei Academy アプリ内の「アカウント削除」機能、又は (c) academy@fintokei.com 宛ての電子メールにより、貴方のアカウント及び関連する個人データの削除を請求することができます。当社は本人確認（通常は登録済み電

子メールへの確認リンクによります。)を行い、確認から30日以内に削除を完了します。

削除の対象は、アカウント、プロフィールデータ（ユーザー名、電子メール、パスワード、嗜好、XP、レベル、ストリーク及び使用済み割引コードを含みます。）、アカウントに紐付く行動イベント、並びに当社の認証プロバイダー（Clerk）における認証記録です

VI. データ主体の個人データの収集方法

当社は、データ主体から及びデータ主体に関するデータを収集するため、次の方法を含む様々な方法を用います。

- **直接的なやり取り。**データ主体は、フォームへの記入により、又は郵便、電話、電子メールその他の手段による当社との遠隔のやり取りにより、当社に個人データを提供することがあります。これには、データ主体が次の場合に提供する個人データが含まれます。
 - 登録フォームに記入して Fintokey の各サービスに申し込む場合
 - データ主体とのコミュニケーションを担当する当社の担当者に連絡して Fintokey の各サービスに申し込む場合
 - 何らかの形態のマーケティングツール（ニュースレター、ランディングページ等）を通じて Fintokey の各サービスに申し込む場合
 - Fintokey モバイルアプリに申し込む場合
- **紹介ブローカー（IB）その他のアフィリエイト：**当社は、当社の紹介ブローカー及び/又はその他のアフィリエイトを通じてデータ主体の個人データの提供を受けることがあります。この場合、データ主体は、紹介を行った当事者が当社の提供するサービスの目的のために当社に対し個人データを開示し又は利用可能にすることがあることを了承します。当社及び紹介ブローカーはいずれも、それぞれのサービスを提供する目的において当該データの管理者です。当社及び紹介ブローカーは、個人データに関して、共同（jointly）ではなく各別共通（in common）に行動します。
- **自動化された技術又はやり取り。**データ主体が本ウェブサイトとやり取りする際、また、クッキーポリシーに従い、その機器、閲覧行動及びパターンに関する技術データが自動的に収集されることがあります。当社は、クッキー、サーバーログその他これに類する技術を用いて当該個人データを収集します。データ主体が当社のクッキーを利用する他のウェブサイトを訪れた場合にも、当該データ主体に関する技術データが要求されることがあります。
- **第三者又は公開された情報源。**当社は、次のような様々な第三者及び公開情報源

からデータ主体に関する個人データを受領することがあります。

- EU域外に拠点を置く Google 等の分析プロバイダー
- EU域内外に拠点を置く広告ネットワーク

VII. 当社によるデータ主体の個人データの利用方法

データ主体の個人データは、法律が当社にこれを認める場合に限り利用されます。当社は、最も一般的には、次の場合にデータ主体の個人データを利用します。

- ・ 契約（データ主体との締結済み又は締結手続中のもの）を履行する必要がある場合
- ・ データ主体の利益又は基本的権利及び自由がこれに優越する場合を除き、当社（又は第三者）の正当な利益のために必要な場合
- ・ 当社が法令上又は規制上の義務を遵守する場合
- ・ データ主体により、自由に与えられ、特定され、説明を受けた上での明確な同意が付与された場合（該当する場合）

上記の処理の法的根拠に該当しない場合には、データ主体（本人）の同意が必要となります。これは特に、電子メール又はテキストメッセージにより第三者のダイレクトマーケティングのためにデータ主体へ個人データを利用する場合に当てはまります。データ主体は、マーケティング目的での個人データの処理に対する同意を、いつでも次の電子メール support@fintokey.com に連絡することにより撤回する権利を有します。

VIII. 当社によるデータ主体の個人データの利用目的

以下の表には、当社がそのデータ主体の個人データを利用しようとするすべての方法、及びその場合に当社が依拠する法的根拠を記載しています。当社は、該当する場合には、その正当な利益が何であるかも特定しています。

データ主体の個人データは、当社が個人データを利用する特定の目的に応じて、複数の適法な根拠に基づいて処理されることがあります。下表に複数の根拠が記載されている場合において、当社が個人データの処理に当たり依拠する特定の法的根拠に関する詳細を得る必要があるときは、データ主体は support@fintokey.com まで当社にご連絡いただけます。

目的／活動	データの種類	正当な利益の根拠を含む、処理の適法な根拠
データ主体を新規の顧客／プロバイダーとして登録するため	(a) 識別 (b) 連絡先	データ主体との合意の履行。
次の事項を含む、当社とデータ主体との関係を管理するため： (c) 取引条件又はプライバシーポリシーの変更の通知 (d) データ主体へのレビュー投稿又はアンケート回答の依頼	(a) 識別 (b) 連絡先 (c) マーケティングデータ	データ主体との合意の履行。
データ主体に関連する本サービスのコンテンツ及び広告を配信し、広告効果を測定し又は把握するため。	(a) 識別 (b) 連絡先 (c) 技術データ (d) プロファイルデータ (e) 利用データ	データ主体との契約の履行。 当社の正当な利益（データ主体の行動及び Fintokey の利用状況の調査、事業の成長、マーケティング戦略情報）のために必要。
アフィリエイト（本サービスをデータ主体に紹介する第三者）について、特定の割引、キャッシュバック、プロモーション、クーポン等の機能を可能とするために、限定された範囲の個人データへのアクセスを認める必要があるため。	(a) 識別 (b) 連絡先	当社の正当な利益のために必要であり、かつ、アフィリエイトを含む仲介者を通じた本サービスの提供を可能にし、それによりデータ主体により有利な条件で本サービスを提供することを促進する点で、合意の履行に一般的に資する。かかる仲介者と関連しないデータ主体は影響を受けない。
本サービス、製品／サービス、マーケティング、顧客関係及び顧客体験を改善するためにデータ分析を用いるため。	(a) 識別 (b) 連絡先 (c) 技術データ (d) プロファイルデータ (e) 利用データ	データ主体との契約の履行。 当社の正当な利益（各データ主体の区分の定義、本サービスの更新、事業の発展、マーケティング戦略の策定）のために必要。

目的／活動	データの種類	正当な利益の根拠を含む、処理の適法な根拠
データ主体が関心を持ち得る製品に関して、データ主体に提案及び推奨を行うため。	(a) 識別 (b) 連絡先 (c) 技術データ (d) プロファイルデータ (e) 利用データ	当社の正当な利益（事業の成長、及び実口座を有するデータ主体のポートフォリオの拡充）のために必要。
当社の事業及び本サービスを管理し保護するため（トラブルシューティング、データ分析、テスト、システム保守、サポート、報告及びデータのホスティングを含みます。）	(a) 識別 (b) 連絡先 (c) 技術データ (d) プロファイルデータ (e) 利用データ	データ主体との契約の履行。 当社の正当な利益（管理及びITサービスの提供、ネットワークセキュリティ、不正防止、事業再編）のために必要。
当社の事業及び本ウェブサイトを管理し保護するため（トラブルシューティング、データ分析、テスト、システム保守、サポート、報告及びデータのホスティングを含みます。）	(a) 識別 (b) 連絡先 (c) 技術	(a) 当社の正当な利益（事業運営、管理及びITサービスの提供、ネットワークセキュリティ、不正防止、並びに事業再編又はグループ再構築の文脈におけるもの）のために必要 (b) 法的義務を遵守するために必要
貴方に関連するウェブサイトのコンテンツ及び広告を配信し、当社が貴方に表示する広告の効果を測定し又は把握するため	(a) 識別 (b) 連絡先 (c) プロファイル (d) 利用 (e) マーケティング・コミュニケーション (f) 技術	当社の正当な利益（顧客による当社の製品／サービスの利用方法の調査、その開発、事業の成長及びマーケティング戦略への反映）のために必要

目的／活動	データの種類	正当な利益の根拠を含む、処理の適法な根拠
当社ウェブサイトのリードフォームから取得した、ハッシュ化された自社のユーザー提供データを、オフラインのリード測定及びサーバーサイドのイベントトラッキング（Conversions API）に用いるため。これにより、オフラインのコンバージョンを追跡し、Google や Meta 等のプラットフォーム上でのコンバージョン測定の精度を向上させることができます。	(a) 識別 (b) 連絡先 (c) 技術	当社の正当な利益（広告キャンペーンの効果測定に資するため）のために必要
当社のウェブサイト、製品／サービス、マーケティング、顧客関係及び顧客体験を改善するためにデータ分析を用いるため	(a) 識別 (b) 連絡先 (c) 技術	当社の正当な利益（当社の製品及びサービスの顧客類型の定義、ウェブサイトの最新性及び関連性の維持、事業の発展、並びにマーケティング戦略への反映）のために必要
法的請求の主張及び法的紛争における防御、犯罪の予防及び捜査、債権者又は破産管財人による差押えの請求への対応	(a) 識別 (b) 連絡先 (d) 利用 (e) マーケティング・コミュニケーション (f) 技術	当社の正当な利益（必要又は適切な場合に当社の地位及び利益を防御できるようにするため、又は公的機関への当該データの提供義務を負う場合のため）のために必要
KYC／AML／CFT	(a) 識別 (b) 連絡先	当社の正当な利益のために必要 法的義務を遵守するために必要
リスクモデリング、不正対策スコアリング、行動パターン分析及び製品開発を含め、Fintokey Intelligence 分析／情報	(a) 技術データ (b) プロファイルデータ (c) 利用データ	当社の正当な利益（Fintokey Intelligence ツールの運用及び改善、リスク管理、不正対策、製品開発）のために必要。データ主体との契約

目的／活動	データの種類	正当な利益の根拠を含む、処理の適法な根拠
ツールを運用、訓練、評価及び改善するため。	(d) 取引データ（関連する場合）	の履行。法的義務（該当する場合、例：AML／CFT）の遵守。

IX. マーケティング

当社は、特にマーケティング及び広告に関して、特定の個人データの利用について貴方に選択肢を提供するよう努めています。貴方が同意を付与しない場合であっても、貴方が当社の顧客であるときは、当社は、欧州議会及び理事会指令2002/58/ECの条件の下で、貴方に商業ニュースレターを送付し（又はテレマーケティングの電話をかけ）る権利を有します。いずれの場合も、貴方は、(a) ニュースレター本文中のオプトアウトボタン、(b) 当社のお問い合わせフォーム、又は (c) 次の電子メール dpo@fintokey.com への連絡により、当該マーケティング・コミュニケーションを拒否することができます。

X. プロモーション・オファー

当社は、データ主体の識別、連絡先、技術、利用及びプロファイルの各データを用いて、データ主体の潜在的なニーズ又は関心について見解を形成することがあります。これにより、当社はデータ主体に関連する製品、サービス及びオファーを提供することがあります（マーケティング目的は、その製品又はサービスに関する当社の正当な利益を構成します。）。

データ主体は、当社に情報を求めた場合、又は情報を受領する目的で本サービスへのアクセス時に自己の詳細情報を提供した場合に限り、かつ、いずれの場合もマーケティング通知の受領をオプトアウトしていない限りにおいて、当社からマーケティング・コミュニケーションを受領することがあります。

当社は、コンバージョンのオフライン追跡を可能にする機能である Google 拡張コンバージョンツールを利用することがあります。当社は、これを、安全かつプライバシーに配慮した方法で当社の Google 広告キャンペーンへの効果を追跡するために利用します。これにより、コンバージョン測定を高め、広告キャンペーンをより適切に最適化し、サービス改善のためにその効果を測定することができます。当社は、Google 拡

張コンバージョンの利用に当たり、第三者と一切の個人情報を共有しません。

同様に、当社は Meta コンバージョンAPI (CAPI) を利用します。このサーバーサイドのトラッキング技術により、当社は特定のウェブイベント（フォーム送信やアカウント登録等）を当社サーバーから直接 Meta (Facebook/Instagram) へ送信することができます。貴方のプライバシーを保護するため、当社は、貴方の電子メールアドレスや電話番号等のハッシュ化（仮名化）された個人データのみを送信し、Meta はこれを既存の利用者データベースと照合します。この処理により、当社は、ブラウザベースのクッキーに依存せずに広告キャンペーンの効果を測定し、広告配信を正確に最適化することができます。データは送信前にハッシュ化され、Meta のデータ処理条件に従い、専らアトリビューション及び最適化の目的で処理されます。

XI. 第三者によるマーケティング

Fintokey グループ各社以外の会社とマーケティング目的でデータ主体の個人データを共有するに先立ち、当社はデータ主体の明示的なオプトイン同意を必要とします。

XII. オプトアウト

データ主体は、自己に送付された各マーケティングメッセージ中のオプトアウトリンクをたどることにより、又はいつでも次の電子メールアドレス support@fintokey.com 若しくは dpo@fintokey.com に連絡することにより、いつでも当社又は第三者に対しマーケティングメッセージの送信を停止するよう求める権利を有します。

XIII. クッキー

データ主体は、本ウェブサイト上のすべて又は一部のクッキーを拒否し、又はクッキーの設定若しくはアクセスを変更するよう、自己のブラウザを設定する権利を有します。クッキーを無効化又は拒否した場合、本ウェブサイトの一部にアクセスできなくなり、又は正常に機能しなくなることがある旨ご留意ください。当社が使用するクッキーに関する詳細は、クッキーポリシーをご参照ください。

XIV. 目的の変更

データ主体の個人データは、それが収集された目的のために利用されます。ただし、データの処理の法的根拠が当社にその他の目的での利用を認め、かつ当該目的が当初の目的と適合する場合は、この限りではありません。

無関係な目的でデータを利用する場合、当社はデータ主体に通知し、その法的根拠を説明します。データ主体の個人データは、上記の規定に従い、かつ当該利用が法律により要求され又は許容される場合に限り、データ主体の認識又は同意なく処理されることがあります。

XV. データ主体の個人データの第三者への開示

当社は、Fintokey に関連するサービスを適切に遂行する目的で、データ主体の個人データを第三者と共有することがあります。データ主体の個人データのセキュリティは、当該第三者により十分に尊重され、法律に従って取り扱われます。当該データ主体の個人データは、第三者が自己の目的のために利用することはできず、当社によって特定された目的のためにのみ、かつ当社の指示に従って処理されます。

当社のサービスプロバイダー及び履行補助者も、業務上の秘密を保持することを条件に、これらの目的のためにデータを受領することがあります。これらの会社は、ITサービス、物流、印刷サービス、法務、会計、電気通信及びコンサルティング、並びに営業及びマーケティングを提供します。

当社外の受領者へのデータの移転に関しては、まず、当社が知り得た顧客に関するすべての事実及び評価について秘密を保持することを誓約していることに留意すべきです。原則として、当社は、法令上の規定により要求される場合、データ主体が同意した場合、又はその他情報提供が認められる場合に限り、データ主体に関する情報を開示することができます。これらの条件の下で、法令上又は規制上の義務がある場合には、個人データの受領者は公的機関及び団体（例：規制当局、税務当局、法執行当局）となる場合があります。

その他のデータ受領者としては、データ主体がデータの提供に同意した者、又は当社が正当な利益に基づき個人情報を委ねる者が考えられます。

XVI. データセキュリティ

当社は、データ主体の個人データが偶発的に滅失し、無断で利用若しくはアクセスされ、改変され、又は開示されることを防止するため、適切なセキュリティ対策を講じる義務を負います。さらに、当社は、データ主体の個人データへのアクセスを、合意の目的

の履行に実際に関与している従業員又は第三者に限定します。当該従業員又は第三者は、守秘義務を尊重しつつ、当社の指示に基づいてのみデータ主体の個人データを処理します。

当社は、個人データ侵害の疑いに対処し、法的に要求される場合には、その旨をデータ主体及び該当する規制当局に通知するための手続を実施します。

XVII. GOOGLE reCAPTCHA

本ウェブサイト及び一部の当社アプリケーションは、不正行為、ボットトラフィック、アカウント乗っ取り、不正利用及びスパムから保護するため、Google LLC 及び/又は Google Ireland Limited（以下「Google」といいます。）が提供する Google reCAPTCHA（reCAPTCHA Enterprise を含みます。）を使用します。これらの目的のため、reCAPTCHA は、IPアドレス、デバイス及びブラウザの特性、マウス及びタッチ操作、その他の行動的及び環境的シグナル等の技術情報を収集し、分析のために Google に送信します。

2026年4月2日より、Google はその顧客に代わってデータ処理者として reCAPTCHA を運用します。これに伴い、当社は、当社のデジタル環境上で reCAPTCHA を通じて収集される個人データについてデータ管理者として行動し、Google は、Google Cloud Platform Service Specific Terms 及び Google Cloud Data Processing Addendum に基づき、当社に代わって当該データを処理します。Google が reCAPTCHA データをどのように処理するか、及び Google の適用あるセキュリティ並びに副処理者に関する確約については、cloud.google.com/terms において入手可能なこれらの文書をご参照ください。

当社による reCAPTCHA の使用の法的根拠は、不正、不正利用及び本サービスへの無断アクセスを防止し、データ主体のアカウントを保護し、並びに当社システムのセキュリティ及び完全性を維持することに係る当社の正当な利益です。reCAPTCHA のクッキー又はこれに類する技術をデータ主体の機器に設置するために同意が必要な場合、当該同意は当社のクッキーバナーを通じて取得されます。詳細はクッキーポリシーをご参照ください。

XVIII. 国際移転

当社は、サービスを遂行する目的のため、一定の場合に、欧州経済領域（EEA）外へ個人データを移転する必要があることがあります。

当社がデータ主体の個人データを EEA 外へ移転する場合には常に、当社は、次の保護措置のうち少なくとも一つを実施することにより、同等の保護水準が確保されるように

します。

- 当社は、欧州委員会により個人データについて十分な保護水準を提供すると認められた国に限り、個人データを移転します。
- 当社が特定のサービスプロバイダーを利用する場合、当社は、欧州における保護と同等の保護を個人データに与える、欧州委員会承認の特定の契約を用いることがあります。

XIX. 自動化された意思決定及びプロファイリング

当社は、不正防止、マネー・ローンダリング対策、リスク管理及びセキュリティの目的（reCAPTCHA 等のツールによるボット／不正スコアリングを含みます。）のため、並びに Fintokei Intelligence 分析ツールの運用及びマーケティングのセグメント化のため、限定的なプロファイリング活動を行うことがあります。当社は、GDPR第22条にいう自動化された処理のみに基づき、データ主体に法的効果を生じさせ又は同様に重大な影響を及ぼす決定にデータ主体を服させることはありません。ただし、当該決定が契約の履行のために必要な場合、EU法若しくは加盟国法により認められる場合、又はデータ主体の明示的な同意に基づく場合は、この限りではなく、いずれの場合も、人による介入を得る権利、データ主体の見解を表明する権利及び当該決定に異議を述べる権利を含む適切な保護措置を伴います。

XX. 個人データ侵害

当社は、個人データ侵害を検知し、封じ込め、是正するための手続を維持します。個人データ侵害が自然人の権利及び自由に対するリスクを生じさせるおそれがある場合、当社は、GDPR第33条に従い、不当に遅滞することなく、可能な場合にはこれを認識した時から72時間以内に、管轄の監督機関に通知します。当該侵害が自然人の権利及び自由に対する高いリスクを生じさせるおそれがある場合、当社は、GDPR第34条に従い、影響を受けるデータ主体に対しても不当に遅滞することなく当該侵害を伝達します。

XXI. 監督機関に異議を申し立てる権利

その他の行政上又は司法上の救済を妨げることなく、欧州経済領域内のすべてのデータ主体は、GDPR第77条に従い、特に常居所地、就業地又は侵害が主張される地のEEA加盟国において、監督機関に異議を申し立てる権利を有します。チェコ居住者の場合、これはチェコ・データ保護機関（Úřad pro ochranu osobních údajů、www.uoou.cz）です。EEA各監督機関の一覧は、欧州データ保護会議（edpb.europa.eu）により公表されています。

XXII. 法域別の規定

本セクションは、本ポリシーのその他の部分に追加して、かつこれを補完するものとして、居住地その他の特定の法域との関連に応じて自然人に適用される規定を定めます。以下のいずれかのサブセクションが適用される者に関し、本セクションと本ポリシーのその他の部分との間に矛盾がある場合には、矛盾の限度において当該サブセクションが優先します。本セクションで定義されない大文字表記の用語は、本ポリシーの他の箇所与えられた意味を有します。

C. 大韓民国の居住者 (PIPA)

本サブセクションは、大韓民国個人情報保護法（法律第10465号、改正を含む。以下「PIPA」といいます。）上の情報主体である自然人に適用されます。

viii. 当社の地位及び処理の根拠

当社は、本ウェブサイト、クライアントゾーン、取引プラットフォーム、Fintokey シミュレーション口座、Fintokey Academy モバイルアプリケーション、Fintokey Intelligence ツールその他の付随サービスを通じて収集される韓国の情報主体の個人情報に関し、「個人情報処理者」（개인정보처리자）です。PIPA第15条、第17条、第22条の2、第23条及び第28条の8に従い、当社は、以下に定める事前の、自由に与えられ、特定され、説明を受けた上での同意に基づき、該当する場合にはPIPAが認めるその他の適法な根拠（特に情報主体との契約の履行及び法令上の義務の遵守）により補完して、韓国の情報主体の個人情報を処理します。

ix. 韓国の情報主体による同意の付与

登録時に該当する同意ボックスにチェックを入れること、及び/又は大韓民国において本ポリシーの提示を受けた後に本サービスの利用を継続することにより、韓国の情報主体は次の各同意を明示的に付与します。以下の各同意は独立しており、個別に付与し又は拒否することができます。「必須」と表示された同意の拒否は、本サービスの該当部分を利用できなくすることがあります。

- （必須 — PIPA第15条）私は、本ポリシーに記載のとおり、(i) アカountの登録及び管理、(ii) 本サービス（クライアントゾーン、取引プラットフォーム、Fintokey シミュレーション口座、Fintokey Academy 及び Fintokey Intelligence を含みます。）の提供及び維持、(iii) 決済処理、(iv) カスタマーサポート、(v) 不正及び不正利用の防止、KYC/AML/CFT、並びに (vi) 適用法令の遵守の目的のために、当社が私の識別データ、連絡先データ、金融データ、取引データ、技術データ、

プロフィールデータ、利用データ並びにマーケティング・コミュニケーションデータを収集し利用することに同意します。保存期間は本ポリシーの「データの保存」のセクションに定めるとおりです。

- (必須 — PIPA第17条) 私は、本ポリシーの「データ主体の個人データの第三者への開示」のセクションに記載のとおり、当該セクションに定める目的に限り、当社が私の個人情報を第三者の処理者及び受領者 (IT、ホスティング、分析、決済、認証、不正対策、コミュニケーション及び法務の各サービスプロバイダーを含みます。) に提供することに同意します。
- (必須 — PIPA第28条の8) 私は、当社が私の個人情報を大韓民国外に所在する受領者 (欧州経済領域、英国、その他当社及びその処理者が事業を行う法域を含みます。) へ越境移転することに同意します。移転される個人情報の区分、受領者、移転先の国、移転の目的、保存期間及び照会のための連絡先は、本ポリシーに記載のとおりです。移転は、当社の情報通信ネットワークを介した電子的手段により行われます。
- (任意 — PIPA第22条の2) 私は、本サービス、関連製品、プロモーション及びオファーに関し、電子メールその他の電子的手段を含むダイレクトマーケティング・コミュニケーションのために、当社が私の連絡先データ及びマーケティング・コミュニケーションデータを利用することに同意します。私は、本サービスへのアクセスに影響を及ぼすことなく、以下に記載のとおりいつでもこの同意を撤回することができます。
- (任意 — PIPA第23条 — センシティブ情報) 当社は、原則として、韓国の情報主体に関するセンシティブ情報 (민감정보) を収集しません。法令上又は契約上の理由 (例: KYC/AMLのために必要な限定的な区分) により当社がセンシティブ情報を収集する必要がある場合、当社は事前に別途の特定の同意を取得します。

x. 同意の撤回

韓国の情報主体は、support@fintokey.com 又は DPO (dpo@fintokey.com) に連絡することにより、本サブセクションに基づき付与した同意を、いつでも撤回することができます。撤回は、撤回前に行われた処理の適法性に影響を及ぼしません。必須同意の撤回は、当社が本サービスの該当部分の提供を継続できなくなる結果を生じさせることがあります。

xi. 韓国の情報主体の権利

本ポリシーの「データ主体の法的権利」のセクションに記載の権利に加え、韓国の情報主体は、PIPAに基づき、(i) 自己について保有される個人情報へのアクセス及びその写

しを請求する権利（第35条）、(ii) 訂正又は削除を請求する権利（第36条）、(iii) 処理の停止を請求する権利（第37条）、(iv) 個人情報侵害の通知を受ける権利（第34条）、並びに (v) 個人情報保護委員会（개인정보보호위원회）又は韓国インターネット振興院の個人情報侵害申告センター（privacy.go.kr）に異議を申し立てる権利を有します。

xii. 国内代理人（PIPA第31条の2）

当社がPIPA第31条の2及び関連する施行令に定める法定基準（概して、韓国に住所又は事業所を有しない外国の情報通信サービス提供者であって、前年度の年間総売上高が1兆ウォンに達し、又は該当する3か月間において1日平均100万人以上の韓国の情報主体の個人情報を保管・管理するもの）を満たす場合、当社は韓国における国内代理人を選任及び公表し、連絡先を適宜更新します。当該選任までは、本ポリシーに定めるDPOの連絡先が適用されます。

xiii. 14歳未満の児童

本サービスは14歳未満の児童を対象とせず、また同児童に向けられたものでもありません。当社は、その法定代理人の事前の同意なく、14歳未満の韓国の児童から故意に個人情報を収集することはありません。

xiv. お問い合わせ及び苦情

韓国の情報主体の個人情報の処理に関するご質問、ご請求及び苦情は、support@fintokey.com 又は DPO（dpo@fintokey.com）までお送りいただけます。韓国の情報主体は、個人情報保護委員会（www.pipc.go.kr）に対して苦情を申し立てることもできます。

D. 日本の居住者（APPI）

本サブセクションは、日本との関連において個人情報が処理される自然人であって、それゆえに日本の個人情報の保護に関する法律（平成15年法律第57号、改正を含む。以下「APPI」といいます。）の適用範囲に属する者に適用されます。これは特にAPPI第171条の域外適用規定によります。

vii. 当社の地位及び利用目的

当社は、日本の情報主体の個人情報に関し、APPI上の「個人情報取扱事業者」（個人情報取扱事業者）です。APPI第17条及び第21条に従い、当社は、本ポリシーの「当社によるデータ主体の個人データの利用目的」のセクションに定めるとおり（該当する場

合には、Fintokey Academy 及び Fintokey Intelligence に関連する目的を含みます。) 個人情報の利用目的を特定し、当該目的の達成に必要な範囲内でのみ個人情報を利用します。

viii. 日本の情報主体による同意の付与

登録時に該当する同意ボックスにチェックを入れること、及び/又は日本において本ポリシーの提示を受けた後に本サービスの利用を継続することにより、日本の情報主体は次の各同意を明示的に付与します。以下の各同意は独立しており、個別に付与し又は拒否することができます。「必須」と表示された同意の拒否は、本サービスの該当部分を利用できなくすることがあります。

- (必須 — APPI第17条及び第21条) 私は、本サービス、Fintokey Academy 及び Fintokey Intelligence ツールの運用、カスタマーサポート、不正及び不正利用の防止、KYC/AML/CFT、並びに適用法令の遵守を含め、本ポリシーに特定された利用目的のために当社が私の個人情報を利用することに同意します。
- (必須 — APPI第27条) 私は、本ポリシーの「データ主体の個人データの第三者への開示」のセクションに記載のとおり、当該セクションに定める目的のために、当社が私の個人情報を第三者に提供することに同意します。受領者がAPPI第25条にいう委託先(委託先)として行動する場合、当社は当該委託先を監督し、別途の同意は不要です。
- (必須 — APPI第28条) 私は、当社が私の個人情報を日本国外の外国に所在する第三者(欧州経済領域、英国、その他当社及びその処理者が事業を行う法域を含みます。)に提供することに同意します。私は、APPI第28条に基づき要求される情報(当該外国の名称、当該国の個人情報保護制度に関する情報(合理的に入手可能な場合)、及び受領者が講ずる個人情報の保護のための措置に関する情報を含みます。)を、いずれも本ポリシーに記載のとおり、また DPO への請求により提供されたことを確認します。
- (任意 — APPI第27条) 私は、本サービス、関連製品、プロモーション及びオファーに関し、電子メールその他の電子的手段を含むダイレクトマーケティング・コミュニケーションのために、当社が私の連絡先データ及びマーケティング・コミュニケーションデータを利用することに同意します。私は、本サービスへのアクセスに影響を及ぼすことなく、いつでもこの同意を撤回することができます。
- (該当する場合は必須 — APPI第20条第2項) 当社は、原則として、日本の情報主体に関する要配慮個人情報(要配慮個人情報)を収集しません。法令上又は契約上の理由(例: KYC/AML)により当社が当該情報を収集する必要がある場合、当社は事前に別途の特定の同意を取得します。

ix. 同意の撤回

日本の情報主体は、support@fintokey.com 又は DPO (dpo@fintokey.com) に連絡することにより、本サブセクションに基づき付与した同意を、いつでも撤回することができます。撤回は、撤回前に行われた処理の適法性に影響を及ぼしません。必須同意の撤回は、当社が本サービスの該当部分の提供を継続できなくなる結果を生じさせることがあります。

x. 日本の情報主体の権利

本ポリシーの「データ主体の法的権利」のセクションに記載の権利に加え、日本の情報主体は、APPIに基づき、(i) 保有個人データ及び第三者提供記録の開示を請求する権利（第33条及び第33条の2）、(ii) 訂正、追加又は削除を請求する権利（第34条）、(iii) 利用の停止、消去又は第三者提供の停止を請求する権利（第35条及び第35条第3項）、並びに (iv) 当社に直接苦情を申し出る権利を有します。請求は、support@fintokey.com 又は DPO (dpo@fintokey.com) までお送りいただけます。

xi. 苦情及び監督機関

日本の情報主体は、日本の個人情報保護委員会（個人情報保護委員会、www.ppc.go.jp）に対して苦情を申し立てることができます。

xii. 児童

本サービスは児童を対象とせず、また児童に向けられたものでもありません。当社は、その法定代理人の事前の同意なく、16歳未満の日本の児童から故意に個人情報を収集することはありません。

XXIII. データの保存

データ主体の個人データは、法令上、会計上又は報告上の要件を満たす目的を含め、それが収集された目的を達成するために必要な期間、保存されます。

個人データの適切な保存期間を判断するに当たり、当社は、個人データの量、性質及び機微性、当該個人データの無断利用又は開示による損害の潜在的リスク、当該個人データが処理される目的及びその目的が他の手段により達成し得るか否か、並びに適用法令上の要件を考慮します。

当社の正当な利益に基づき処理される個人データは、最後の各契約の終了後5年間保存されます。この期間は、別の契約の開始により終了し、その時点で新たな期間が開始し、個人データの処理がこれに応じて再開されます。

一定の状況においては、貴方は当社にデータの削除を求めることができます。詳細は以

下の「削除の請求」をご参照ください。一定の状況においては、当社は、調査又は統計の目的のために貴方の個人データを匿名化（貴方と関連付けられなくなるようにすること）することがあり、その場合、当社は、貴方への別途の通知なく、無期限にこの情報を利用することがあります。

個人データの処理に同意が必要な場合（マーケティングその他本ポリシーに記載の目的等）、データの保存期間はその目的に応じて異なることがあります。別段の定めがない限り、個人データは5年間、又はデータ主体がその同意を撤回するまで処理されます。

上記に定めるサービスプロバイダーの個人データの処理は、当該者がサービスプロバイダーでなくなった後5年間行われます。

その他の目的のための証拠の保全は、法令上の時効期間内において行われます。

電子メール、チャット、電話その他の遠隔コミュニケーション手段に含まれる個人データは、本ポリシーに定める関連する目的に従って処理されることがあります。処理期間は最長で5年間となることがあります。

Fintokei Academy アカウントの削除後も、最小限の範囲で保存されるもの：会計及び税務記録 — 10年間。KYC／AML記録 — 取引関係の終了から10年間。法的請求の主張又は防御に必要なデータ — 4年間。その他の適用法令により保存が要求される一切のデータ。保存されるデータはアクセスが制限され、当該法的目的のためにのみ利用されます。

XXIV. データ主体の法的権利

いずれのデータ主体も、その個人データに関し、データ保護法令に基づき次の権利を有します。

- **アクセスの請求**（一般に「データ主体アクセス請求」として知られます。）。データ主体は、当社が自己について保有する個人データの写しを受領し、当該データが適法に処理されていることを確認することができます。
- **訂正の請求**。データ主体は、当社が自己について保有する不完全又は不正確なデータの訂正を請求することができます。ただし、当社は、データ主体が提供する新たなデータの正確性を確認する必要がある場合があります。
- **削除の請求**。データ主体は、当社が個人データを処理する適切な理由がない場合に、当社に対し個人データの削除又は除去を請求する権利を有します。データ主体はまた、処理に対する異議申立ての権利（下記参照）を有効に行使した場合、自己の情報が違法に処理された可能性がある場合、又は当社が現地法を遵守するために個人データを消去することを要求される場合にも、当社に個人データの削除又は除去を請求することができます。ただし、適用法令が特定の理由により認める場合、当社はデータ主体の請求に応じることを拒否することがあり、その旨

はデータ主体に通知されます。

- **処理に対する異議。**当社が正当な利益（又は第三者の正当な利益）に依拠しているが、データ主体が当該処理は自己の基本的権利及び自由に影響を及ぼすと考える場合、データ主体はその個人データの処理に異議を述べるすることができます。データ主体はまた、ダイレクトマーケティング目的での個人データの処理に異議を述べるすることができます。正当な理由がある場合、当社は、データ主体の権利及び自由に優越する、処理のためのやむを得ない正当な根拠を有することを証明することができます。
- **処理の制限の請求。**これにより、データ主体は、次の場合に当社に対し個人データの処理の停止を求めることができます。(a) データ主体が当社にデータの正確性の確認を求める場合、(b) 当社によるデータの利用が違法であるが、データ主体がその消去を望まない場合、(c) 当社がもはやデータを必要としないが、データ主体が法的請求の立証、行使又は防御のためにこれを必要とし得るため、当社にデータの保持を必要とする場合、又は (d) データ主体が当社によるデータの利用に異議を述べたが、当社がこれに優越する正当な根拠を有するか否かを確認する必要がある場合。
- **移転の請求。**データ主体は、その個人データを自己又は任意の第三者に移転するよう請求できます。当社は、当該個人データを、構造化され、一般に用いられ、機械可読の形式で、データ主体又はその選択する第三者に提供します。この権利は、データ主体が当初当社に利用することを同意した自動化された情報、又は当社がデータ主体との契約の履行のために情報を利用した場合にのみ適用されます。
- **同意の撤回。**当社がデータ主体の個人データの処理について同意に依拠している場合、データ主体はいつでも同意を撤回できます。ただし、これは、データ主体が同意を撤回する前に行われた処理の適法性には影響を及ぼしません。

XXV. 通常、手数料は不要です

貴方は、自己の個人データへのアクセス（又はその他の権利の行使）のために手数料を支払う必要はありません。ただし、貴方の請求が明らかに根拠を欠き、反復的又は過剰である場合、当社は合理的な手数料を請求することがあります。あるいは、当社はこれらの状況において貴方の請求に応じることを拒否することがあります。

XXVI. 児童のプライバシー

当社は、15歳未満の者から故意に情報を収集することはありません。当社のウェブサイト

ト、製品及びサービスはすべて、15歳以上の者を対象としています。15歳未満の場合は、これらのウェブサイト上で、又はその機能を通じて、いかなる情報も利用又は提供せず、ウェブサイトに登録せず、ウェブサイトを通じて購入を行わず、また氏名、住所、電話番号又は電子メールアドレスを含む自己に関する情報を当社に提供しないでください。15歳未満の児童から個人データを収集又は受領したことが判明した場合、当社は当該情報を削除します。

XXVII. 当社が貴方に求めることがある事項

当社は、貴方の本人確認を行い、貴方の個人データへのアクセス権（又はその他の権利の行使）を確保するため、貴方に特定の情報を求めることがあります。これは、個人データが受領する権利を有しない者に開示されないようにするためのセキュリティ上の措置です。当社はまた、対応を迅速化するため、貴方の請求に関連して追加情報を求めるためにご連絡することがあります。

XXVIII. 対応期限

当社は、すべての正当な請求に1か月以内に対応するよう努めます。貴方の請求が特に複雑である場合、又は貴方が多数の請求を行った場合には、1か月を超えることがあります。この場合、当社は貴方に通知し、随時状況をお知らせします。