The Privacy Policy

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions.

The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

- **You** means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.
  Under GDPR (General Data Protection Regulation), You can be referred to as the Data Subject or as the User as you are the individual using the Service.
- **Company** (referred to Fincake Ltd. located at British Virgin Islands, Road Town, Tortola, Quijano Chambers, P.O. Box 3159. as either “Fincake”, "the Company", "We", "Us" or "Our" in this Agreement) refers to
  For the purpose of the GDPR, the Company is the Data Controller.
- **Affiliate** means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.
- **Account** means a unique account created for You to access our Service or parts of our Service.
- **Website** refers to the Fincake website, accessible from https://fincake.io/

- **Service** refers to the Fincake application.
- **Service Provider** means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service, to assist the Company in analyzing how the Service is used or to assist the Company in promoting the Service.
  For the purpose of the GDPR, Service Providers are considered Data Processors.
- **Third-party Social Media Service** refers to any website or any social network website through which a User can log in or create an account to use the Service.
- **Personal Data** is any information that relates to an identified or identifiable individual.
  For the purposes for GDPR, Personal Data means any information relating to You such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.
  For the purposes of the CCPA, Personal Data means any information that identifies, relates to, describes or is capable of being associated with, or could reasonably be linked, directly or indirectly, with You.
- **Cookies** are small files that are placed on Your computer, mobile device or any other device by a website, containing the details of Your browsing history on that website among its many uses.
- **Usage Data** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
- **Data Controller**, for the purposes of the GDPR (General Data Protection Regulation), refers to the Company as the legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data.
- **Do Not Track (DNT)** is a concept that has been promoted by US regulatory authorities, in particular the U.S. Federal Trade Commission (FTC), for the Internet industry to develop and implement a mechanism for allowing internet users to control the tracking of their online activities across websites.
- **Business,** for the purpose of the CCPA (California Consumer Privacy Act), refers to the Company as the legal entity that collects Consumers' personal information and determines the purposes and means of the processing of Consumers' personal information, or on behalf of which such information is

collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California.

- **Consumer,** for the purpose of the CCPA (California Consumer Privacy Act), means a natural person who is a California resident. A resident, as defined in the law, includes (1) every individual who is in the USA for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the USA who is outside the USA for a temporary or transitory purpose.
- **Sale,** for the purpose of the CCPA (California Consumer Privacy Act), means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Consumer's Personal information to another business or a third party for monetary or other valuable consideration.

Collection of Information

Information You Provide to Us

We collect information you provide directly to us. For example, we collect information when you create an Fincake Account, participate in any interactive features of the Services, fill out a form, participate in a contest or promotion, make a purchase, communicate with us via third party social media sites, request customer support, or otherwise communicate with us.

When You Sign Up or Register for an Fincake Account or Services

If you sign up for an Fincake Account or other Services, we will collect basic information about you including your name, email address, Telegram handle or blockchain wallet. You may provide this information to us directly, or by signing in to your account/service with a third party, including without limitation, Google (see "Information We Collect from Other Sources" below). We will use the information that we collect about you to:

- Create and maintain your Fincake Account;
- Allow you to log in to Fincake;
- Contact you about your Fincake Account and/or our Services (this may include marketing emails).

Information You Give Us. Information we collect from you may include:

- Identity information, such as your first name, last name, username or similar identifier, title, date of birth and gender;
- Contact information, such as your postal address, email address and telephone number;
- Profile information, such as your username and password, interests, preferences, feedback and survey responses;
- Feedback and correspondence, such as information you provide in your responses to surveys, when you participate in market research activities, report a problem with Service, receive customer support or otherwise correspond with us;
- Financial information, such as your credit card or other payment card details;
- Transaction information, such details about purchases you make through the Service and billing details;
- Usage information, such as information about how you use the Service and interact with us;
- Marketing information, such as your preferences for receiving marketing communications and details about how you engage with them;
- Financial information, such as bank account number and bank routing number; financial assets holdings; and
- Technical information, such as your Ethereum wallet address, application programming interface (API)-key and network information regarding transactions.

Information We Get From Others. We may get information about you from other third party sources and we may add this to information we get from your use of the Services. Such information may include:

- Metamask or Phantom wallet address;
- telegram id and telegram name.

Information Automatically Collected. We may automatically record certain information about how you use our Sites (we refer to this information as “Log Data“). Log Data may include information such as a user’s Internet Protocol (IP) address, device and browser type, operating system, the pages or features of our Sites to which a user browsed and the time spent on those pages or features, the frequency with which the Sites are used by a user, search terms, the links on our Sites that a user clicked on or used, and other statistics. We use this information to administer

the Service and we analyze (and may engage third parties to analyze) this information to improve and enhance the Service by expanding its features and functionality and tailoring it to our users' needs and preferences.

We may use cookies, local storage or similar technologies to analyze trends, administer the Sites, track users' movements around the Sites, and to gather demographic information about our user base as a whole. Users can control the use of cookies and local storage at the individual browser level.

When You Provide Information to Build Your Profile

You can update your Profile at any time by visiting the "Profile" page in the Settings menu when logged into your Fincake Account. We recommend that you update your Profile regularly, to ensure that the Fincake functions offered to you are appropriate for your current circumstances. You further agree to update such information upon Fincake's request, if Fincake considers the information provided as untrue, incorrect, incomplete and/or inconsistent with other information provided by you at any time. You acknowledge that we may rely upon such information and that you are responsible for any damages or losses which may result from any inaccuracies, including without limitation, the inappropriateness of our Services to your Profile. You do not have to complete your Profile and therefore do not have to provide the information; however, if you choose not to, we will be unable to offer Fincake's full functionality to you.

When You Contact Us

If you contact us by telephone, email, post or use another function offered by Fincake, such as the chat feature, we will collect any information about the communication and any additional information that you choose to give us. We will use this information to review, investigate and respond to any comment or question that you may raise. Please note that we record and retain all telephone calls and other communication with us and may use it in our dealings with you, including any dispute resolution or legal proceedings.

When an Fincake User Invites You to Use Fincake

Users of Fincake can invite their contacts to sign up for an account with us. We only collect the email addresses of individuals that users choose to invite to join Fincake and Fincake only uses the email addresses for sending an invitation to the individual at the request of the existing Fincake user.

Retention of Your Personal Data

We retain information we collect as long as it is necessary and relevant to fulfill the purposes outlined in this privacy policy. In addition, we retain personal information to comply with applicable law where required, prevent fraud, resolve disputes, troubleshoot problems, assist with any investigation, enforce our Terms of Use, and other actions permitted by law. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymize your personal information (so that it can no longer be associated with you) in which case we may use this information indefinitely without further notice to you.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

Disclosure of Your Personal Data

Affiliates

We may disclose your personal information to our subsidiaries and corporate affiliates (i.e. our family of companies that are related by common ownership or control) for purposes consistent with this Privacy Policy.

Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

We may share personal information when we do a business deal, or negotiate a business deal, involving the sale or transfer of all or a part of our business or assets. These deals can include any merger, financing, acquisition, or bankruptcy transaction or proceeding.

Compliance with Laws and Law Enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency). We may share personal information for legal, protection, and safety purposes

Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation, including KYC and AML requirements.
- Protect and defend the rights or property of the Company, our agents, customers, and others. This includes enforcing our agreements, policies, and terms of use.
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

Professional Advisors and Service Providers

We may share information with those who need it to do work for us. These recipients may include third party companies and individuals to administer and provide the Service

on our behalf (such as bill and credit card payment processing, customer support, hosting, email delivery and database management services), as well as lawyers, bankers, auditors, and insurers.

We may share your information with third-party companies and individuals who help us administer and provide the Service. These may include providers of bill and credit card payment processing, customer support, hosting, email delivery, and database management services, as well as lawyers, bankers, auditors, and insurers. These recipients will only have access to the information necessary to perform their specific tasks on our behalf and are obligated to protect your information and use it only for the purpose for which it was disclosed. We require that they adhere to the same level of confidentiality and security that we maintain for your information.

Other

You may permit us to share your personal information with other companies or entities of your choosing. Those uses will be subject to the privacy policies of the recipient entity or entities.

We may also share aggregated and/or anonymized data with others for their own uses.

We will not share the personal information we hold about you except in the following circumstances:

- between and among the Fincake and our current and future parents, affiliates, subsidiaries, and other companies under common control and ownership; and
- with professional advisors, vendors, consultants, and other service providers, such as payment service providers, IT hosting companies, banks, other financial institutions and credit reporting/reference agencies who need access to such information to carry out work on our behalf;
- in connection with, or during negotiations of, any merger, sale of company assets, financing or acquisition of all or a portion of Fincake by another company;
- disclosure in accordance with, or required by, any applicable law or legal process, including lawful requests by public authorities to meet national security or law enforcement requirements;
- if we believe your actions are inconsistent with our user agreements or policies, or to protect the rights, property, and safety of Fincake or others; or.

- where we have your consent. For example, if you use the “...” feature, we will get your permission before sharing your personal information with a third party.

Sharing of Your Personal Information

We understand that your personal information is sensitive and private. We will only share your personal information with other companies or entities of your choosing with your explicit consent. Please note that any such sharing will be subject to the privacy policies of the recipient entity or entities.

In addition, we may share aggregated and/or anonymized data with third parties for their own uses.

We take the responsibility of safeguarding your personal information seriously, and we will not share the personal information we hold about you except in the following circumstances:

- Between and among Fincake and our current and future parents, affiliates, subsidiaries, and other companies under common control and ownership.
- With professional advisors, vendors, consultants, and other service providers, such as payment service providers, IT hosting companies, banks, other financial institutions, and credit reporting/reference agencies who need access to such information to carry out work on our behalf.
- In connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of Fincake by another company.
- Disclosure in accordance with, or required by, any applicable law or legal process, including lawful requests by public authorities to meet national security or law enforcement requirements.
- If we believe your actions are inconsistent with our user agreements or policies, or to protect the rights, property, and safety of Fincake or others.
- Where we have your consent. For example, if you use a feature that involves sharing your personal information with a third party, we will obtain your explicit consent beforehand.

We value your privacy and will always strive to keep your personal information secure and confidential.

Security of Your Personal Data

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure.We are not responsible for any interception or interruption of any communications through the internet or for changes to or losses of data. Users of the Services are responsible for maintaining the security of any password, biometrics, user ID or other form of authentication involved in obtaining access to password protected or secure areas of any of our digital services. In order to protect you and your data, we may suspend your use of any of the Services, without notice, pending an investigation, if any breach of security is suspected.

Security of Your Personal Data

We take the security of your personal data seriously and implement reasonable measures to protect it from unauthorized access, disclosure, alteration, or destruction. However, please be aware that no method of transmission over the internet or electronic storage is 100% secure, and we cannot guarantee the absolute security of your personal data.

We are not responsible for any interception or interruption of any communications through the internet or for changes to or losses of data. Users of the Services are responsible for maintaining the security of any password, biometrics, user ID, or other form of authentication involved in obtaining access to password-protected or secure areas of any of our digital services.

To protect you and your data, we reserve the right to suspend your use of any of the Services, without notice, pending an investigation if any breach of security is suspected.

In addition to our own security measures, we may use third-party security services and tools to further enhance the protection of your personal data. These may include but are not limited to firewalls, encryption technologies, and secure servers. We regularly review and update our security protocols and policies to ensure the highest level of protection for your personal data.

Advertising and Analytics Services Provided by Others

We may allow others to provide analytics services and serve advertisements about our products and services on our behalf across the web and in mobile applications. This may involve cookies and other technologies to collect information about your use of the Services. This information may be used by Fincake to, among other things, analyze and track data, determine the popularity of certain content, deliver advertising and content targeted to your interests on our Services, and better understand your online activity in connection with the Services.

Detailed Information on the Processing of Your Personal Data

Service Providers have access to Your Personal Data only to perform their tasks on Our behalf and are obligated not to disclose or use it for any other purpose.

Analytics

We may use third-party Service providers to monitor and analyze the use of our Service.

Detailed Information Regarding the Processing of Your Personal Data

We take your privacy seriously and only share your personal data with trusted service providers who assist us in providing our services. These service providers only have access to your personal data in order to perform tasks on our behalf, and they are obligated not to disclose or use it for any other purpose.

Analytics

In order to monitor and analyze the use of our service, we may use third-party service providers. These providers may collect and analyze certain information about your device and how you use our service, such as your IP address, browser type, referring/exit pages, and other similar information. This information is used to help us better understand how our service is being used and to make improvements. Our service providers are contractually obligated to use this information solely for the purpose of providing us with analytical insights and are not permitted to disclose or use it for any other purpose.

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualise and personalise the ads of its own advertising network.

You can opt-out of having made your activity on the Service available to Google Analytics by installing the Google Analytics opt-out browser add-on. The add-on prevents the Google Analytics JavaScript (ga.js, analytics.js and dc.js) from sharing information with Google Analytics about visits activity.

For more information on the privacy practices of Google, please visit the Google Privacy Terms web page: https://policies.google.com/privacy?hl=en

Advertisements

Some Personal Data may be shared with advertising services in order to promote the Company's brand and Services to Our target audience.

Email Marketing

We may use your personal data to contact you with newsletters, marketing or promotional materials, and other information that may be of interest to you. You have the option to unsubscribe from receiving any or all of these communications from us by following the unsubscribe link or instructions provided in any email we send, or by contacting us directly.

We may use email marketing service providers to manage and send emails to you. These providers have access to your personal data only to the extent necessary to provide their services and are contractually obligated to use it solely for that purpose.

Advertisements

In order to promote our brand and services to our target audience, some personal data may be shared with advertising services. This data may include information such as your device type, IP address, and browsing behavior. However, we do not share any personally identifiable information with these services without your explicit consent. If

you would like to opt-out of targeted advertising, you can do so by adjusting your device settings or contacting us directly.

Payments

We may provide paid products and/or services within the Service. In that case, we may use third-party services for payment processing (e.g. payment processors).

We will not store or collect Your payment card details. That information is provided directly to Our third-party payment processors whose use of Your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of the Sites may become inaccessible or not function properly. For more information about the cookies we use, please see our Cookies Policy.

Information we will never collect. We will never ask you to share your private keys or wallet seed. Never trust anyone or any site that asks you to enter your private keys or wallet seed.

Children's Privacy

Our Service does not address anyone under the age of 18. We do not knowingly collect personally identifiable information from anyone under the age of 18. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 18 without verification of parental consent, We take steps to remove that information from Our servers.

Privacy of Minors

Fincake's services are not intended for use by individuals under the age of 18. We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or legal guardian and you become aware that your child has provided personal information to us, please contact us immediately. If we

become aware that we have collected personal information from anyone under the age of 18 without obtaining verified parental consent, we will take prompt steps to remove that information from our servers. We are committed to protecting the privacy of minors and complying with all applicable laws and regulations regarding the collection and use of personal information from children.

Links to Other Websites

Our Service may contain links to other websites that are not operated by Us. If You click on a third party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page.

We will let You know via email and/or a prominent notice on Our Service, prior to the change becoming effective and update the "Last updated" date at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Information choices and changes: accessing, updating, correcting, and deleting your information

You may access information that you have voluntarily provided through your account on the services, and to review, correct, or delete it by sending a request to privacy@fincake.io you can request to change contact choices, opt-out of our sharing with others, and update your personal information and preferences.

Contact Us

If you have any questions about this Privacy Policy, You can contact us by email info@fincake.io

GDPR

For our European users we can confirm that we comply with the European General Data Protection Regulation (“GDPR”). Please see our Data Protection Impact Assessment (“DPIA”) which demonstrates the measures we have taken to comply with our Data Protection obligations.

Data Protection Impact Assessment – Report.

Step 1 – Identify the need for a DPIA.

Fincake as a data controller for a web page (and potentially a mobile app in the future) that processes data directly from user accounts and also from the synchronisation of other platforms, such as banks and other financial institutions, is undertaking a DPIA in order to identify any areas of risk in the collection and processing of its user data.

Fincake will be collecting personal data of data subjects who are citizens of the European Union (“EU”) and are based in the European Economic Area (“EEA”) in order to provide them with services through the Fincake web and mobile app. It is therefore appropriate to use a DPIA to identify any risks associated with the collection, processing, transmission, retention, review and deletion of all personal data being collected for the purposes of providing a service to its users.

Step 2 – Data Processing.

Responsibilities and Standards Applicable to the Processing:

Fincake is collecting personal data directly from its users when they create an account, including personal data of “beneficiaries” and “trusted angels”. Some data is collected when users synchronise 3rd party platforms (e.g. bank accounts, brokerages, crypto exchanges, etc) with their Fincake account. This information may contain personal data, e.g. contents of bank statements and transaction histories, however it will not contain information such as bank account login information or sort codes and account numbers.

Some personal data is also collected from Google and Telegram if the user decides to create a Fincake account using an existing Google account. However, the data collected is limited to only that Fincake requests. This includes the users profile picture, name and email address. Given that Google and Telegram routinely collects a large volume personal data from users including date of birth, gender, email address and mobile phone number it is important to identify if all of this information is shared by Google and Telegram with Fincake. This does not appear to be the case at the moment however, Fincake will monitor this.

The applicable standards are the European General Data Protection Regulation ("GDPR") in relation to all personal data collected from EU citizens and associated implementing legislation, including the UK Data Protection Act 2018 ("DPA'18"). As personal data is being stored on infrastructure located in the United States reference may be made to the California Consumer Privacy Act. Furthermore, at the time of writing this assessment, the EU-US privacy shield has been ruled invalid by the Court of Justice of the European Union ("CJEU"). In the absence of the privacy shield, data controllers must rely on the presence of Standard Contractual Clauses ("SSC's") in all of their third party data processing agreements. Responsibility for ensuring compliance with all applicable standards rests with the directors of Fincake.

Describe the Nature and Scope of the Processing:

Fincake is processing the personal data of their users. This includes first name, last name, email address, password, profile picture, Telegram handle or blockchain wallet.

Personal data is processed solely for the purpose of providing the user with a modern-day wealth tracker and consequently it is necessary to ensure that when a user ceases to login to the app and use the services provided or choose to delete their account, that all processing of personal data of such user is ceased and deleted from Fincake's systems in line with their data retention policy.

Describe the Context and Purpose of the Processing:

Personal data of Fincake users is collected and retained for the purposes of providing the user with a modern-day wealth tracker.

Personal data is shared with third parties by Fincake solely for the purpose of facilitating the provision of the service.

Some personal data may be shared with advertising services in order to target and promote Fincake's own services and brand. However, Fincake will not be sharing data of users who are citizens of the European Union (“EU”) and are based in the European Economic Area (“EEA”).

Personal data shared with third parties will not be subject to any onward data transfer either to additional third parties or third countries.

Step 3 – Types of Personal Data Collected.

Types of collected personal data

The types of personal data collected include:

- First name;
- Last name;
- Email address;
- Password;
- Telegram handle;
- Profile image;
- Blockchain wallet.

Step 4 – Life Cycle of the Personal Data Collected.

Acquiring of Personal Data:

Fincake acquire personal data in 4 ways:

- Directly from the user through the Fincake app or web page when the user sets up an account;
- via Google if the user chooses to create a Fincake account using an existing Google account;

- via Telegram if the user chooses to create a Fincake account using an existing Telegram account;
- Via blockchain crypto wallet if the user chooses to create a Fincake account using an existing blockchain wallet

When a user the Fincake website the user is given 4 options on how they can create account – directly through the Fincake app, by entering email address and password, through Google or Telegram, through blockchain crypto wallet.

Data Processing:

In order to provide the service, Fincake use the following third parties who act as data processors: AWS, Yodlee, Plaid, Salt Edge, Akahu, Lean, Log Rocket, Sentry, Help Scout, Google Analytics and Mailerlite.

Plaid provides account aggregation to top financial institutions in USA, Canada, UK, Spain, France, Ireland and Netherlands. Plaid collects and securely stores the credentials you share, such as User name and password. This information is never stored by, or disclosed to, us. Their Privacy Policy can be viewed at https://plaid.com/legal/#end-user-privacy-policy.

Yodlee provides account aggregation to top financial institutions in USA, Canada, UK, South Africa, UAE, India, Malaysia, Hong Kong, Singapore, Australia and New Zealand . Yodlee collects and securely stores the credentials you share, such as user name and password. This information is never stored by, or disclosed to, us. Their Privacy Policy can be viewed at https://www.yodlee.com/legal/privacy-notice.

Salt Edge and **Akahu** are also data processors can be used by Fincake for account aggregation and data processing. They collect and securely store the credentials you share, such as user name and password, and provide the necessary data to Fincake to provide you with its services. Their Privacy Policies can be viewed at https://www.saltedge.com/privacy_policy and https://akahu.nz/privacy-policy, respectively.

In addition to **Plaid** and **Yodlee**, Fincake also can uses **Lean**, a data processor that provides data enrichment services to help improve the accuracy of the financial data obtained through account aggregation. Their Privacy Policy can be viewed at https://getlean.io/privacy.

Log Rocket and **Sentry** can be used by Fincake for error logging and analysis to help improve the service. **Help Scout** can be used for customer support ticketing,

and Google Analytics is used for website analytics. **Mailerlite** can be used for email marketing and communication.

Fincake ensures that all data processors it uses are fully GDPR compliant and adhere to strict data protection standards. If you have any questions or concerns about how your data is being processed, please do not hesitate to contact Fincake's customer support team.

It is Fincake’s responsibility to ensure that any third party data processors are processing the personal data of Fincake’s users safely and securely. For this reason, Fincake must ensure that Standard Contractual Clauses are in all of their third party processing agreements and that personal data is not retained on third party servers for longer than is necessary. Fincake must also ensure that data processors do not share the personal data of Fincake’s users with any other 3rd parties or third countries.

Data Storage:

Fincake’s servers are operated by Amazon Web Services (“AWS”). All data collected and processed by Fincake, including personal data, is stored on AWS facilities in North Virginia, US (US East Region).

By using AWS servers in the US Fincake is processing and transferring the personal data of EU citizens outside of the EEA. Previously, Fincake could have relied on the EU-US privacy shield framework in order to facilitate the processing and transfer of EU personal data outside of the EEA however, due to the recent European court decision this framework is no longer valid. Therefore, Fincake will ensure that Standard Contractual Clauses are in all of their third party processing agreements where the personal data of EU citizens is stored and processed outside of the EEA.

All data that is stored on Fincake’s AWS servers is encrypted using AES encryption at 256 bit. Other security measures such as 2 factor authentication is in place.

Backup servers – Fincake will confirm details of the provision, location and security measures in place on the backup system along with the testing regime operated to validate the integrity of the backups that are taken.

Data Retention:

Personal data is retained on the system on the basis that if a user fails to login to the system for a period of 45 days (or as set by the user) a series of 5 reminder emails/notifications, known as the “Life Beat Check”, will be sent to the user. These emails will contain a link/button that the user can click on and say “I’m okay”. The user is not required to login to their Fincake account. Just clicking on the link and visiting a webpage is enough to reset the “inactive timer”. In the event that all 5 reminders, sent over a period of 10 days, are unanswered, the beneficiaries and/or trusted angels would be contacted via email and supplied with a copy of the users data in a downloadable format. As a final “longstop”, 12 months after the last user activity on the account a further reminder will be sent to the user and/or beneficiaries/trusted angels and in the event of no response after a period of an additional month (30 days) the user account will then be deleted from Fincake’s systems including backups in its entirety.

Deletion of Data:

Deletion of data should take place in line with the data retention policy outlined above. Any specific programs or systems to be used in the deletion of data may be detailed here.

Assess the Necessity and Proportionality:

The personal data collected represented the totality of the personal data required from the user to deliver the service requested by the user. No additional data is acquired apart from the minimum necessary to provide the service. This is subject to the information acquired from a user’s Google/Telegram account being limited solely to information that is necessarily required for the provision of the service. If Google/Telegram were to provide any additional personal data over and above the profile and contact information detailed above, such as details of the users location and travel history based on mobile device GPS data, search history information or purchasing history, such information would constitute far more personal data than is strictly required for the provision of service to the user. Under the terms of GDPR controllers are encouraged to adopt the principles of data minimisation and only to collect the bare minimum of data required for the performance of the service.

Step 5 – Legal Basis for Processing such Personal data.

Under article 6 of GDPR Fincake is acquiring and processing the personal data of users for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Step 6 – Data Subject Rights.

Right of Access (under Article 15 of the GDPR):

All data subjects who are resident in the European Union and whose personal data is processed by Fincake are entitled to make a subject access request regarding how their personal data is processed.

Under this right a data subject is entitled to receive details as to what items of their personal data are being processed and retained, the systems being used for this purpose and the basis upon which such systems are being used by Fincake. A statutory 30 day deadline applies for Fincake to respond to any Data Subject Access Request (“DSAR”) that may be received.

Fincake has an option in the application that ensures that users are able to download a full copy of the personal data that Fincake processes. This option is provided to the user via the webpage. Users can contact Fincake should they have any issues accessing this system by writing to info@fincake.io. Their request will responded to within the 30 day deadline.

Right to Rectification (under Article 16 of the GDPR):

Under GDPR data subjects are able to request that all personal data held by an organisation may be updated and corrected as necessary.

While the personal data collected by Fincake is primarily supplied at the point of registration as a new user, or in the process of using the app, it is important that the user retains the right to be able to change any of this information during their life time as a user of the Fincake app. It currently appears to be the case that a user has the ability to change or update any of their personal information via the settings in the app. It is important that the feature is retained.

Right to Erasure (under Article 17 of the GDPR):

Each data subject has the right under GDPR to request that their personal data can be erased and in effect be “forgotten” by a data controller or processor. In making such a request the data subject will expect that their personal data is deleted from all relevant systems such as user accounts, marketing information, any third party processing and any long term data retention. Under the right to erasure a data subject has the statutory right to expect this to be undertaken within 30 days.

In practice it is common for some personal data of the data subject to be maintained for professional or regulatory purposes, for example in order to guard against a professional conflict of interest or in order to comply with statutory limitation. However, in this instance it is difficult envisage a scenario where any personal data relating to a data subject making a request under the right to erasure should be retained by Fincake.

Consequently it will be necessary to ensure that a suitably robust system is in place to ensure that any such requests made by a data subject may be processed within 30 days and to ensure that their data is securely eradicated from all Fincake systems including marketing email communications, server backups and any third party data processing.

Data subjects resident in the European Union have the right to exercise the erasure of their personal data from Fincake’s systems. Part of this process can be completed by the user themselves via Fincake settings. To make sure there is no more data saved in the backups, they can contact Fincake and facilitate a request under the right to erasure and Fincake has 30 days in which to comply.

Right to Restriction of Processing (under Article 18 of the GDPR):

Each data subject resident in the EU has the right to request that Fincake as data controller shall restrict the processing of personal data in the event that the accuracy of any personal data is contested, where the processing may be unlawful, where Fincake no longer needs the personal data to supply its service or where the data subject has objected to the processing of the personal data. In the event of such as restriction being exercised by a data subject, the processing of personal data would only be able to recommence with the consent of the data subject.

Consequently, it is important that, as with the right to erasure, Fincake has the ability to identify individual personal data records and restrict the processing of such data in the event if such a request by the data subject.

All data subjects resident in the EU has the right under GDPR to request a restriction of processing by writing to info@fincake.io.

Right to Data Portability (under Article 20 of the GDPR):

Data subjects located in the EU are entitled to a right to receive a copy of the personal data that they have provided to Fincake or to request that their data be transmitted to another data controller on the condition that their personal data is being processed on the basis of consent or pursuant to a contract. As identified at step 5 of this assessment, Fincake is processing the personal data of its users for the performance of a contract to which the data subject is party to therefore users of Fincake have the right to data portability.

Consequently, the Fincake privacy policy must identify that all data subjects resident in the EU has the right under GDPR to request a portable copy of their information to and provide a means for data subjects to be able to contact Fincake and facilitate such a request.

Right to Object (under Article 21 of the GDPR):

You have right to object to our reliance on our legitimate interests as the basis of our processing of your personal information that impacts your rights.

Right to be informed.

You have the right to be informed about the collection and use of Your Personal Data. To ensure this right we provide you with this Privacy Policy.

Right to lodge a complaint with a supervisory authority

If you believe that anyone, including the Fincake, breaches your privacy you are entitled among others to file a complaint to your local supervisory authority to ensure protection of your rights.