Unilink

UNILINK WEBSITE PRIVACY POLICY

Last updated: 24.10.2018

Unilink takes ***Personal Data*** protection seriously, therefore ***We*** comply with the law when ***We*** are processing ***Personal Data***. ***We*** want ***You*** to feel safe when ***You*** visit ***Our Site*** and use ***Our Services*** – and that is why ***We*** are providing ***You*** with this ***Privacy Policy. You*** can find herein information out about ***Our Data*** collection and use of **Your *Personal Data***.

This Policy sets forth current privacy practices with respect of the ***Data We*** collect when ***You*** interacts with ***Our Site*** or by using ***Our Services***.

The integral part of this Privacy Policy is ***Our Cookies Policy***, where ***You*** can learn more about ***Our*** use of ***Cookies*** technology.

I. Glossary

1. "***Applicable Laws***" shall mean all the laws and regulations relevant to the collection, processing and storage of ***Personal Data***, especially all the data protection laws and the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as: "***the GDPR***").
2. "***the Company***" or "***We***" or "***Us***" or ***„Our***" shall mean FinoTech Limited with a registered office at 5 The Mall Street, London W5 2PJ, incorporated under the Companies Act 2006 as a private company, registered in the Registrar of Companies for England and Wales, under the Company number: 10761117, TIN: 7311025296.
3. "***Cookies***" shall mean small text files stored in a web browser by a website (here specifically: Site) or by an ad server. By storing certain information in a ***Cookie***, those web browsers, ad servers, and explicitly ***the Site*** are able to remember ***Your*** preferences and recognize websites visited and/or web browsers used from one visit to another.
4. "***Legal Basis***" shall mean the legal basis for the collection, processing and storage of ***Your Personal Data***.

5. "***Log Data***" shall mean the information that is automatically reported by ***Your*** browser each time ***You*** access ***the Site*** or use ***Our Services*** and which is sent by ***Your*** web browser that ***Our*** servers automatically record. Log Data may include information such as ***Your*** IP address, browser type, web requests, domain names or pages viewed.
6. "***Personal Data***" or "***Information***" or "***Data***" shall mean any Information as defined in Article 4.1 of ***the GDPR*** i.e any information relating to an identified or identifiable natural person ('***data subject***'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
7. "***Profiling***" shall mean any form of automated processing of ***Personal Data*** consisting of the use of ***Personal Data*** to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
8. "***the Site***" shall mean the Unilink website: https://unilink.io/
9. "***Services***" shall mean services provided by ***the Company*** via ***the Site*** in accordance with the Terms and Conditions.
10. "***You***" "***Your***" "***Yours***" shall mean an individual that uses ***the Services*** via ***the Site*** or/and an individual who uses ***the Site*** but has no access to the areas of ***the Site*** and ***Services***.

II. Personal Information We collect about You

We collect Information about ***You*** when:

- ***You*** use of ***Our*** contact and registration forms
- ***You*** use of ***Our*** newsletter form
- ***You*** use of ***Our Services***
- ***You*** use of ***the Site***

The categories of your Data that we collect may include:

1. Name and surname
2. Company name
3. Company address
4. Company phone number

5. Mobile telephone number
6. Skype number/ Telegram ID
7. Tax identification number
8. E-mail address
9. Payment and invoice details
10. other ***Personal Data*** provided voluntarily by ***You***

III. Log Data, Cookies and similar technologies

When ***You*** interact with ***the Site***, ***We*** may also automatically collect information from ***Your*** site activities through the usage of ***Cookies***, ***Log Data*** and similar technologies on ***the Site***.

Using those technologies aims at personalizing ***the Site*** to better meet ***Your*** needs, as well as to provide ***You*** with customized ***the Site*** content and to act within our advertising purposes. ***We*** may also use this information for the purposes of analytics and monitoring of the effectiveness of our performance, including the collection of the aggregate ***the Site*** usage ***Data*** (e.g. the overall number of ***the Site*** visitors or pages viewed).

The above-mentioned information may include:

- ❏ information about ***Your*** interactions with ***the Site***;
- ❏ technical information about ***Your*** computer hardware and software that may include URL information, cookie data, ***Your*** IP address, the types of devices ***You*** are using to access ***the Site*** and/or use ***the Services***, device ID, device attributes, network connection type, browser type, language, internet service provider, clickstream data, access times, the files viewed on ***the Site***;
- ❏ demographic information such as ***Your*** ZIP code, age, gender and preferences by using Log Files; such information is not associated with ***Your*** name or other ***Personal Data***.

Learn more about our collecting and processing of this ***Data***, by see ***Our Cookies Policy***.

IV. Purposes and Legal Basis for Data processing

Your local law may require to set out ***the Legal Basis*** on which ***We*** rely in order to process ***Your Data***. Below ***You*** will find an outline of the purposes for which ***We*** may process ***Your Data*** accompanied by an indication of a relevant ***Legal Basis*** for such processing pursuant to the ***GDPR***:

1. Entering into a contract with ***You*** (in particular registering your account and verifying ***Your*** identity) - ***the Legal Basis***, based on which ***We*** process ***Your Data*** in these circumstances is entering into a contract with ***You*** [**Article 6(1b) of *the GDPR***].
2. Performing the contract, in particular performing ***the Services***, ensuring ad security and ad fraud functionality, managing ***Your*** account, providing ***You*** with customer support, processing transactions / issuing invoices, handling ***Your*** requests, complaints and chargebacks, ***automated individual decision-making*** with respect to calculation of remuneration, ***Profiling*** aiming at evaluation of certain personal aspects relating to a natural person for ensuring ad security and ad fraud functionality, in particular to analyse or predict aspects concerning that natural person's personal preferences, interests, behaviour, location and usage of ***Cookies*** technology in connection with an ***End User's*** device - ***the Legal Basis***, based on which ***We*** process ***Your Data*** for that purpose is performance of a contract concluded with ***You*** [**Article 6(1b) of *the GDPR***].
3. Subscription of the newsletter from **Our** blog, being run by Unilink's copywriter. After subscribing the newsletter **You** will receive the spam concerning summary of most interesting articles; promotions of products or services rolled out by the **Our** authorised counterparties, as well trading promotions announced by **Us**. To this end, **We** process **Your** localisation; **Your** IP; **Your** email - if it contains **Your** name and surname. ***We*** process ***Your Data*** based on the **Yours** (subscriber's) consent to the processing of **Your** personal data for the purpose of subscribing newsletter [**Article 6 (1a) GDPR**].
4. Pursuing claims or defending against claims, responding to ***Your*** inquiries, improving ***Services***, detecting, preventing, and responding to actual or potential fraud, illegal activities, or intellectual property infringement by the means of automated individual decision-making with respect to calculation of remuneration, ***Profiling*** aiming at evaluation of certain personal aspects relating to a natural person for ensuring ad security and ad fraud functionality and monitoring compliance with the Terms and Conditions, ensuring accountability (demonstration of compliance with ***Our*** obligations under the law), storing ***Data*** for archiving or statistical purposes - ***The Legal Basis***, based on which ***We*** process ***Your Data*** in these circumstances is ***Our*** legitimate interest [**Article 6(1f) of *the GDPR]*** to: pursue claims or defend against claims, responding your inquiries, improve ***the Services***, detect, prevent, and respond to actual or potential fraud, illegal activities, or intellectual property infringement, monitor compliance with the Terms and Conditions. ***Our*** legitimate

interest is also ensuring accountability (i.e. demonstration of compliance with ***Our*** legal obligations under the law, in particular under ***the GDPR***), as well as storing ***Data*** for archiving and statistical purposes. **Balance of interests:** After assessment ***Our*** interests and ***Your*** interests, rights and freedoms, ***We*** believe that the collection the ***Data***, specified above will not interfere excessively with ***Your*** privacy or will not constitute an excessive burdensomeness for ***You***. In the course of evaluating ***Your*** interests, rights and freedoms, ***We*** have taken into account the following circumstances: upgrading the standards of ***the Site***, resulting in the better quality of ***the Services***; avoiding the risk of suspension of ***the Services*** due to the illegal, activities of dishonest users; preventing ***the Company*** from negative legal consequences, influencing on ability of upgrading the standards of using ***the Site***.

5. Conducting necessary tax and accounting operations - ***the Legal Basis***, based on which ***We*** process ***Your Data*** for this purpose is being compliance with legal obligations ***We*** are subject [**Article 6(1c) of *the GDPR***] i.e. to conduct relevant tax and accounting operations in the ordinary course of ***Our*** commercial activity.
6. Performing marketing of ***Our*** products and ***Services*** (***Our*** direct marketing, customer satisfaction survey, analysis), including ***Profiling*** aiming at evaluation of certain personal aspects relating to a natural person for ensuring ad security and ad fraud functionality, in particular to analyse or predict aspects concerning that natural person's personal preferences, interests, behaviour, location and usage of ***Cookies*** technology in connection with an ***End User's*** device - ***the Legal Basis***, based on which ***We*** process ***Your Data*** in these circumstances is ***Our*** legitimate interest [**Article 6(1f) of *the GDPR***] to promote ***Our*** products and services. **Balance of interests:** After assessment ***Our*** interest and ***Your*** interests, rights and freedoms, ***We*** believe that marketing will not interfere excessively with ***Your*** privacy and will not be an excessive burdensomeness for ***You***. In the course of assessment interests, rights and freedoms, ***We*** have taken into account the following circumstances:

   a) as part of the marketing of our clients' products and services, ***We*** do not provide ***Your Personal Data***, in this way ***We*** limit the circle of people having access to ***Your Personal Data***;

   b) ***We*** ensure that ***We*** have implemented appropriate guarantees to protect ***Your*** privacy, namely:

      i. ***We*** only use ***Data*** about the professional sphere of ***Your*** life. ***We*** are only interested in what pertains to using ***the Site***, not ***Your*** private life;

ii. ***We*** only use ***Data*** about ***Your*** activity on ***the Site***, not what ***You*** do on other websites.

Depending on ***Your*** location, there may be solutions to help ***You*** control ***Your*** online behavioural advertising preferences (such as whether certain third parties may collect and use your Site Usage Information for targeted advertising purposes). For example, in Europe the website www.youronlinechoices.com allows ***You*** to choose which companies can deliver customized ads while in the US ***You*** may use the Network Advertising Initiative's Opt-Out Tool and the Digital Advertising Alliance's Opt-Out Tool.

From time to time ***We*** also may ask ***You*** for ***Your*** voluntary consent to the specific form of marketing, i.e. sending commercial information via e-mail (newsletter) or contacting with ***You*** by phone or skype for ***Our*** business purposes in accordance with applicable law (telecommunication law, act on providing services by electronic means).

Additionally, when ***You*** give us ***Your*** voluntary consent, ***We*** process ***Your Personal Data*** by using ***Cookie*** technology in scope and for the purposes described in ***the Site's Cookies*** notification and ***Cookies Policy***.

VI. Your rights

If ***You*** are based in European Union or ***the GDPR*** applies to ***You*** under ***the Applicable Law***, ***You*** have certain rights and protections under the law regarding the collection, processing, and use of information about ***You***.

The Company ensures the implementation of ***Your*** rights listed below. ***You*** can exercise ***Your*** rights by submitting a request via email to dataprotection@finotech.com

The right to withdraw consent.

You have the right to withdraw any consent, if the processing of ***Your Personal Data*** on Unilink is based on ***Your*** consent and ***You*** provided it at the time of registration to Unilink, as well during using individual functionalities offered on Unilink - only in event of Unilink as well individual services and functionalities offered on Unilink provide data processing solely based on ***Your*** consent (e.g. subscription of the newsletter from the blog). Withdrawal of

consent has effect since the moment of its withdrawal. The withdrawal of consent shall not affect the lawfulness of processing, performed by ***the Company*** based on ***Your*** consent before its withdrawal.

Withdrawal of consent does not entail any negative consequences for ***You***. However, it may prevent ***You*** from continuing to use the Unilink or functionality that the Company can lawfully provide only based on ***Your*** consent.

Legal basis: Article 7(3) of the GDPR.

The right to object to the Data being used

You have the right to object at any time to the use of ***Your*** personal data, if ***the Company*** processes ***Your*** data based on its legitimate interest, e.g. in relation to the improving of Unilink services.

If ***Your*** objection turns out to be legitimate and ***the Company*** has no other legal basis to process ***Your Personal Data***, ***the Company*** will delete ***Your*** data which is subject of the objection raised by ***You***.

Legal basis: Article 21 of the GDPR.

Right to erasure ('right to be forgotten')

You have the right to request the erasure of all or some of ***Your Personal Data***.

You have the right to request erasure of ***Personal Data*** if:

a) ***You*** withdrew ***Your*** specific consent to the extent to which ***Your Personal Data*** was processed based solely on ***Your*** consent;

b) ***Your Personal Data*** has ceased to be necessary for the purposes for which it was collected or processed;

c) ***You*** raised an objection to the use of ***Your*** data for marketing purposes;

d) ***You*** raised an objection to the use of ***Your*** data in order to conduct statistics on the use of Unilink, and the opposition was considered justified;

e) ***Your Personal Data*** is processed unlawfully.

Despite the request to erase ***Personal Data***, in connection with opposition or withdrawal of consent, ***the Company*** may retain certain ***Personal Data*** provided by ***You*** in the field of asserting or defending claims. This applies in particular to ***Personal Data***, received solely from ***You***, regardless of means of communication, without limitation: name, surname, email address, documents provided by ***You*** during e.g. the email communication with ***the Company***, which ***the Company*** retains for purposes of handling complaints and claims related to the use of Unilink.

Legal basis: Article 17 of the GDPR.

Right to restriction of Processing

You have the right to request a restriction on the processing of ***Your Personal Data***. If ***You*** submit such a request, it will prevent ***You*** from using certain functionalities or services, involving the ***Personal Data*** processing covered by the request. ***You*** will also not receive any messages, including marketing messages.

You have the right to request restrictions on the use of ***Your Personal Data*** in the following cases:

a) when ***You*** contest the accuracy of ***Your Personal Data*** - then ***the Company*** will restrict their use for the time needed to verify the accuracy of ***Your Data***, but no longer than for 7 days since the receipt of ***Your*** request;

b) if the processing of ***Your*** data is unlawfully, and instead of erasure ***Your Personal Data***, ***You*** will demand restriction of their use;

c) where ***Your Personal Data*** has ceased to be necessary for the purposes for which ***the Company*** has collected or used it, but it is necessary for ***You*** to determine, assert or defend claims;

d) if ***You*** object to the use of ***Your Data*** - then the restriction occurs for the time needed to consider whether, due to ***Your*** special situation, protection of ***Your*** interests, rights and freedoms override the interests based on which ***the Company*** processes ***Your Personal Data***.

Legal basis: Article 18 of the GDPR.

Right of access to the Data.

You have the right to obtain confirmation from ***the Company***, whether ***the Company*** process ***Your Personal Data***, and if this is the case, ***You*** have the right to:

a) get access to ***Your Personal Data***;

b) obtain information about the purposes of processing, categories of ***Personal Data*** being processed, the recipients or categories of recipients of this ***Data***, the planned period of storage of ***Your*** data or criteria for determining this period, information concerning ***Your*** rights under the ***GDPR*** and the right to file a complaint to the supervisory authority, the source of these ***Data***, on automated decision-making, including ***Profiling*** and safeguards applied in connection with the transfer of these data outside the European Union;

c) obtain a copy of ***Your Personal Data***.

Legal basis: Article 15 of the GDPR.

The right to rectify Your Personal Data

You have the right to rectify and supplement ***Your Personal Data***. ***You*** have the right to request us to correct this ***Data*** (if it is incorrect) and to supplement it (if it is incomplete).

Legal basis: Article 16 of the GDPR.

The right to Data portability.

You have the right to receive ***Your Personal Data*** that ***You*** provided to ***the Company*** and then send it to another ***Personal Data*** controller chosen by ***You***, e.g. to another ***Controller*** of similar services. ***You*** also have the right to request that ***Personal Data*** be sent by ***the Company*** directly to such other ***Controller***, if it is technically possible.

The Company will send ***Your Personal Data*** in the form of a csv file. The csv format is a commonly used, machine-readable format that allows you to send the received data to another ***Controller*** of ***Personal Data***.

Legal basis: Article 20 of the GDPR.

When does the Company meet Your request?

While - by exercising the aforementioned rights - ***You*** request, that ***the Company*** comply with this request or refuse to comply with it without delay, but no later than one month after receipt. However, if - due to the complexity of the request or the number of requests - ***the Company*** will not be able to meet ***Your*** request within a month, ***the Company*** will meet them within the next two months, informing ***You*** in advance about the intended extension.

For technical reasons, ***the Company*** always needs 72 hours to update the settings ***You*** have selected in ***the Company's*** systems. Therefore, it may happen that ***You*** will receive an email from ***the Company*** during the system update, from which ***You*** have given up.

If ***You*** would like to exercise any of these rights, please contact ***Us***: dataprotection@finotech.com. Please include information that will enable ***Us*** to verify ***Your*** identity within ***Your*** request.

Filing complaints, inquiries and applications

You can make complaints, requests and applications to ***the Company*** regarding the processing of ***Your Personal Data*** and the exercise of ***Your*** rights.

If ***You*** believe that ***Your*** right to the protection of ***Personal Data*** or other rights granted to ***You*** by virtue of the ***GDPR*** have been violated, ***You*** have the right to fill a complaint against ***the Company*** to the Information Commissioner's Office .

VII. How Data is protected

The Company uses various security technologies and procedures that help protect ***Your Personal Data*** from unauthorized access, use, disclosure, alteration or destruction.

Personnel:
Only qualified and authorized employees are permitted to access ***Personal Data***, and they may do so only for permitted business functions.

Security Measures:
We use encryption in the transmission of ***Your Personal Data*** between ***Your*** system and ***Ours***, and ***We*** use firewalls to help prevent unauthorized persons from gaining access to ***Your Personal Data***.

Payments:
All supplied sensitive Information is transmitted via Secure Socket Layer (SSL) technology and then encrypted into our payment gateway providers database only to be accessible by those authorized with special access rights to such systems, and are required to keep the Information confidential. After a transaction, Your private Information will not be stored on our servers.

Additional Safeguards.
We maintain physical, electronic and procedural safeguards in connection with the collection, storage and disclosure of ***Your Data***. ***Our*** security procedures mean that we may request proof of your identity before we disclose ***Personal Data*** to ***You***;

Trusted vendors.
We rely only on vendors who ensure an appropriate level of security of ***Your Data***. In this context, ***We*** use only secure cloud servers, including AWS cloud – a secure, private cloud platform. AWS participates in the EU-US Privacy Shield framework. Amazon Web Services

is our processor. AWS Amazon cloud platform uses various security technologies and procedures to protect ***Personal Data*** and is compliant with third-party assurance frameworks such as without limitation: ISO 27017 for cloud security, ISO 27018 for cloud privacy, PCI DSS Level 1, and SOC 1, SOC 2, and SOC 3. For more details please see AWS Amazon security and privacy policy at www.aws.amazon.com.

We would like you to feel confident using ***the Site*** to conduct business. However, ***You*** should also take care of how ***You*** handle and disclose ***Your Data*** and avoid sending ***Personal Data*** through insecure channels or networks. It is important for you to protect yourself against unauthorized access to ***Your*** password and to ***Your*** computer. Be sure to sign off when ***You*** finish using a shared computer and under no circumstances do not share ***Your*** password with anyone, even with ***Us*** – ***We*** NEVER ask for it.

VIII. International transfer of Data

The Company may transfer ***Data*** to a country outside of the European Economic Area (EEA), i.e. to the territory of United States of America for which the European Commission has adopted an adequacy decision (Privacy Shield), in order to protect storage and processing of data using IT services, as well as operating ***the Site*** and providing ***the Services***.

The EU-U.S. Privacy Shield framework is a “partial” adequacy decision, as, in the absence of a general data protection law in the U.S., only the companies committing to abiding by the binding Privacy Shield principles benefit from easier ***Data*** transfers.

For the above-mentioned reasons, in such cases ***Your Personal Data*** will be transferred to the territory of USA in accordance with applicable laws, with appropriate safeguards in place, only to Privacy Shield certified vendors (according to the EU Commission Decision 2016/1250) or by using standard contractual clauses adopted by the European Commission (EU Commission Decision on standard contractual clauses for the transfer of ***Personal Data*** to processors established in third countries under Directive 95/46/EC (hereinafter referred to as: “***the Model Contract Clauses***”), or based on other applicable transborder ***Data*** transfer mechanisms.

If ***You*** are located in the EEA, ***You*** may contact us if ***You*** require a copy of the safeguards which ***We*** have put in place to protect ***Your Data*** transferred outside of the EEA and ***Your*** privacy rights in these circumstances.

You may also learn more about:

Privacy Shield Program here https://www.privacyshield.gov/Program-Overview and here https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en.

EU Commission Decision on standard contractual clauses for the transfer of ***Personal Data*** to processors established in third countries here:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087
and here:
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

IX. Retention of Your Data

The Company stores ***Your*** Information for a period of time required for the purposes for which it was collected using generally accepted security standards and in compliance with applicable laws. ***The Company*** will not retain ***Your Personal Data*** for longer than 2 years since the date of its collection.

In particular, ***We*** store ***Data*** about ***You*** when ***You*** have an account on ***the Site*** and when ***You*** use ***the Services***. Please note that even if ***You*** delete ***Your*** account, ***the Company*** may have the right to process ***Your Data*** for the purpose of creating statistics, pursuing claims or defending against claims, handling ***Your*** complaints and chargebacks as well as in order to meet the tax and accounting law requirements, where such processing will last only for the period of time necessary to achieve the intended purposes (e.g. for pursuing claims or defending against claims, the period of retention of ***Your Data*** is no longer than limitation period for claims as defined in statutory law).

Please note, that for marketing purposes ***Your Data*** will be processed until such time ***You*** object to it. Where ***You*** have consented to marketing communications via e-mail or other telecommunication means for ***Our*** marketing purposes (e.g. ***You*** agree to receive our newsletter or contacting ***You*** by phone), ***You*** may withdraw ***Your*** consent at any time by contacting as well as ***You*** may unsubscribe from newsletter at any time by clicking the unsubscribe link in an email from ***Us***. In these circumstances, ***Your Personal Data*** will be processed until ***Your*** withdrawn of the consent.

X. Disclosures

We may disclose ***Your Personal Data*** only to the following trusted third parties:

I. ***Authorized Third Parties - We*** may share ***the Data*** with parties directly authorized by ***You*** to receive that ***Data***, such as when ***You*** authorize a third party (e.g. payment service providers) to access to ***Your Data***. The use of ***the Data*** by an authorized third party is subject to the third party's privacy policy;

II. ***Safety, Legal Purposes and Law Enforcement*** - ***We*** may use and disclose the ***Data*** when we believe it is necessary: (i) under applicable law, and (ii) to respond to requests from courts, law enforcement agencies, regulatory agencies, and other public and government authorities.

III. ***Service providers - We*** may also engage third parties that support the operation of ***the Services*** (acting on ***Our*** behalf), such as analytics providers, IT services providers (e.g. cloud or host services providers) or advertising agencies.

XI. Payment Service Providers Notice

In case ***You*** buy ***the Company's Services*** using third-party payment services (such as payment gateways and other payment transaction processors), please note that such payment service provider ***You*** use may collect from ***You*** and process ***Your Data*** on their own in order to perform such payment services. Such third-party service providers have their own privacy policies in respect to ***the Data We*** are required to provide them with for ***Your*** purchase-related transactions. Once ***You*** leave ***the Site*** or are redirected to a third-party website or application, ***You*** are no longer governed by this Privacy Policy or ***Our*** Terms and Conditions.

For these providers, ***We*** strongly recommend to read their privacy policies, so that ***You*** can understand the manner in which ***Your Personal Information*** will be handled by these providers.

XII. Children's privacy

Protecting children's privacy is very important for Unilink. ***The Site*** is not intended for, designed to be used by, or targeted at children. ***We*** do not knowingly collect ***Data*** from any person who is an individual under the age of 18.

XIII. Notice to parents

If ***You*** are a parent or a guardian who knows or has otherwise discovered that ***Your*** child under the age of 18 has submitted his or her ***Personal Data***, or other information, to ***Us***, do not hesitate to contact us using the following email address: dataprotection@finotech.com.

We will promptly remove ***Your*** child's Personal Data or other information from ***Our*** system, cease the use of such ***Data*** and direct any third party with access to it to do the same.

XIV. Online Privacy Policy Only

This online Privacy Policy applies only to Information collected through ***the Site*** and not to Information collected offline.

XV. Contacting Us

FinoTech Limited
5 The Mall street, London W5 2PJ

In case of Personal Data issues, please contact US: dataprotection@finotech.com