

Global Privacy Policy | Fintopio

Latest version as of Apr 12, 2024

Introduction:

Fintopio FZ LLC (hereinafter referred to as the “**company**”, “**Fintopio**”, “**we**”, “**us**” or “**our**”), is a global entity on a mission to create a financial ecosystem that connects communities globally through innovative solutions, fostering financial inclusion while adhering to regulatory requirements.

At Fintopio, we value the privacy of our users (“**you**”, or “**your**”) and are dedicated to protecting personal data with the utmost care and security. This Global Privacy Policy (this “**Policy**”) outlines our practices regarding the collection, use, and protection of your personal data across our website (<https://fintopio.com/>), Telegram Bot, Web application or mini app, and/or wallet, (collectively; “**Fintopio’s Platform**” or simply, the “**Platform**”), our services, and interactions with users worldwide. We are committed to ensuring compliance with the European Union (EU) General Data Protection Regulation (GDPR), the United Arab Emirates’ (UAE) Federal Decree Law No. 45 of 2021 (applicable to UAE residents), and other relevant data protection laws globally.

Please note that your use of the Platform and/or services is subject to your acceptance of this Policy. If you do not agree with our practices regarding the collection, use, and protection of your personal data as detailed in this Policy, you should not access or use our Platform, and/or any of our services. It is important to review this Policy carefully before deciding to use our Platform and services. Your continued use of our Platform and services following any changes to this Policy will be considered as your acceptance of those changes. This Policy includes the following sections:

1. The Scope and applicability of this Policy,
2. Amendments to this Policy,
3. Who we are,
4. The data we collect about you and how we collect it,
5. How and why, we share your data,
6. How we use/process your data and the legal bases for doing so,
7. The controls, choices, and rights that you have,
8. Cookies and how we use them,
9. Marketing and advertising,
10. The privacy policies of other websites/applications/platforms,
11. Our practices on children’s privacy,
12. Our data security and integrity policies and practices,
13. Our global data transfer, and storage/retention practices,
14. How you can contact us with complaints and questions,
15. How to contact the relevant regulatory authorities,
16. Privacy Notice for UK and EU residents,
17. Privacy Notice for EMEA residents.
18. The Definitions of “Terms” used in this Policy.

1. The Scope and applicability of this Policy

This Policy outlines how we handle the information provided or gathered on our website and applications, including those made available on external sites or platforms. Our practices adhere to the privacy laws relevant to the regions where we operate. Occasionally, we might issue specific privacy notices related to our services, procedures, or regions, which should be considered in conjunction with this policy. To be precise, this Policy extensively details our practices for handling Personal Data across various touchpoints, including but not limited to, (i) interactions on our website at <https://fintopio.com/>, (ii) use of our services, (iii) use of our web and/or mobile applications, (iv) engagement in our marketing initiatives, (v) connecting with us at industry events, (vi) job applications, (vii) legal and compliance communications, and (viii) business-related interactions such as partnerships and other business opportunities.

This Policy provides an overview of user rights related to their Personal Data and furnishes information on how to reach out to us for further clarification on our privacy practices. Additionally, for residents of the European Economic Area (EEA) or the United Kingdom (UK), this Policy outlines additional rights pertaining to Personal Data, with an in-depth elaboration available in our dedicated Privacy Notice for "**UK and EU residents**". Regarding the rights of residents of countries in the Middle East, Africa and European countries that are not part of the EU, please consult our dedicated Privacy Notice for "**EMEA residents**".

It's important to note that information shared with us via third-party sites or platforms (for instance, through our apps on these sites) may also be collected by the host site or platform. The data we collect falls under the purview of this Policy, whereas the data collection by the third-party sites or platforms follows their own privacy policies. Therefore, the privacy preferences set on these third-party platforms do not influence how we handle the information obtained directly through our applications. Additionally, be aware that our website and applications might include links to external sites not under our control. We do not oversee the privacy practices of such external sites, and we recommend that you read their privacy policies if you provide personal information to them.

2. Amendments to this Policy.

This Policy shall be maintained in its most current version at all times. We reserve the unilateral right to amend or revise this Policy, including making changes to ensure compliance with the latest legal and jurisprudential developments. Any such amendments shall become effective immediately upon their publication on our website unless an alternative effective date is expressly stated within the text of the amendment itself.

While we shall endeavour to implement supplementary notification methods to inform users of any updates to this Policy, it is incumbent upon users to periodically review our Website to acquaint themselves with the most recent version of our Privacy Policy.

3. Who we are.

We are **Fintopio FZ LLC**, a company duly registered in, and operating under the laws of the Emirate of Dubai, United Arab Emirates (UAE), the processor and controller of your personal information. As the Data Controller, Fintopio FZ-LLC is responsible for securely handling

your data, ensuring its confidentiality, and using it solely for the purposes outlined in this Policy.

Company Name: **Fintopio FZ LLC,**
Address: **5DMC, Dubai Media City, Dubai,**
Country: **United Arab Emirates (UAE).**

Fintopio stands at the forefront of digital financial innovation, offering a seamless cryptocurrency wallet service accessible through our Platform. With a keen eye on universally accessible payment solutions, Fintopio is set to redefine the digital financial landscape, ensuring that secure, simple, and accessible financial transactions are a reality for everyone, across the globe. Through this Policy, we aim to safeguard the information you share with us, ensuring a secure and transparent financial experience.

4. The data we collect about you and how we collect it.

a) Information you provide to us:

To create an account and/or a wallet and gain access to our Platform and services, you will be required to furnish us with certain personal information. This data is pertinent for specific specified purposes, which are further elaborated upon below. The information may be (i) required by law (e.g., to verify your identity and comply with "Know Your Customer (KYC)" obligations), (ii) necessary for us to provide our services to you as requested by you (e.g., your email address is required to open an account). If we decide to incorporate additional features and services, you might be required to furnish us with supplementary details upon our request. Noncompliance with the information requirements will result in the inability to use our Services.

The following categories of information may be gathered from you:

CATEGORY OF PERSONAL DATA	TYPES OF PERSONAL DATA
Contact Information	Email address, country, region.
Personal Identification Data.	Full name, email address, gender, home address, phone number, date of birth, nationality, signature, utility bills, photographs, and a video or voice recording of you.
Employment Information	Job title, salary wage rate, and company.
Transaction Information	Information about the transaction you make on our services, such as the name of the recipient, your name and email.
Government Identifiers	Government issued identity documents such as passport, national identification number, national identity card details, drivers licence numbers.
Sensitive and Biometric Personal Data	We may also collect sensitive personal data when permitted by local law or with your consent, such as biometric information, for example to verify your identity by comparing the facial scan data extracted from your selfie or video with the photo in your government issued

	identity document.
Business information	Proof of legal registration, personal identification data for all ultimate beneficial owners (UBOs), personal data about the board of directors (BOD) senior managers responsible for the operations of the legal entity.
Financial Information	Bank account information, payment card information, transaction data, tax identification, source of funding, source of wealth.
Communications	Surveys, feedback, and quiz responses, information contained in the Survey. Communications with us including call recordings with our customer services team.
Blockchain Data	We may analyze public blockchain data, including wallet addresses, transaction IDs, timestamps of transactions or events, and transaction amounts.

b) Information we collect from our affiliates and third parties.

We may collect information about you from our affiliates or third-party sources as necessary or permitted by applicable law.

1. **Affiliates:** As a standard aspect of doing business, we may, in compliance with relevant laws, collect information about you from a group of companies associated with us by common control or ownership ("**Affiliates**"). This allows us to provide you with the Services offered by our Affiliates. We may obtain information about you such as Personal Identification Data, Transactional Information, Business Information, Usage Information.
2. **Blockchain Data:** We might engage in the examination of publicly accessible blockchain information, which could include a variety of data points such as transaction identifiers, the quantities involved in transactions, the specific wallet addresses used, as well as the timestamps associated with each transaction or event.
3. **Business Clients:** When our Payments and Remittances Services are utilised to facilitate a transaction involving virtual assets (VAs), it is possible that the third-party merchant involved in the transaction may provide us with a variety of your personal information. The information in question has the potential to comprise an extensive range of particulars, such as your complete name, various contact details (so that we may reach you), and intricate details pertaining to the nature and particulars of the transaction in question.

c) Information we collect from you automatically.

We reserve the right to automatically collect specific categories of information, such as when you utilise our services or engage in interactions with us, to the extent permitted by law. This data aids in the resolution of customer support concerns, the improvement of our platform and service performance, maintenance or enhancement of the user experience, and fraud prevention by detecting unauthorised access to your account.

Data that is automatically gathered comprises:

CATEGORY OF PERSONAL DATA	TYPES OF PERSONAL DATA
Browsing Information	Internet Protocol ("IP") address, device identification number, browsing information including name and version, data on internet connectivity, information from the operator and carrier, login credentials, browser category and model, time zone settings and location data, language data, and application version. browser plug-in versions and varieties, operating system and platform, as well as any other data that may be stored or accessible on the devices to which you grant access while using our Platform.
Usage Data	<p>Authentication data, security questions, click-stream data, public social networking posts, and other data acquired by cookies or similar technologies.</p> <p>Details on the operation of our Services as you utilise them, including but not limited to, any errors you may have encountered, information regarding the site's performance, and other diagnostic data.</p>
Marketing and Research Information	<p>Identifiers encompass personal information such as name and address, email address (if employed for direct marketing), and IP address or other online identifiers.</p> <p>Demographic information (such as gender, income, family status, age, and interests)</p> <p>Browser and web history data, preferences indicated by the selection, viewing, and purchase of products, services, and content, as well as mobile device information including device identification number, type of device, and mobile operating system (where applicable).</p> <p>Individual profiles and analytics derived from the data that is gathered about them. Regarding further details, kindly refer to our Cookie Policy (cookie policy link).</p> <p>Preferences in marketing and interests, whether explicit or implicit.</p>

5. How and why we share your data.

We may disclose your Personal Information to third parties, including our affiliate entities, when we deem it necessary and in alignment with our contractual obligations to you

(such as those outlined in our Terms & Conditions) or as required by applicable laws, regulations, or legal proceedings. In instances where your Personal Information is shared with our affiliates, we commit to ensuring that these entities either abide by this Privacy Policy or adhere to practices that offer equivalent or greater protection.

1. **Disclosure to Legal and Regulatory Bodies:** We may disclose your personal data to judicial bodies, law enforcement agencies, regulatory authorities, legal counsels, and other relevant parties in the following circumstances:
 - a) to adhere to legal requirements and obligations;
 - b) to support the initiation, exercise, or defense of legal claims or rights;
 - c) to fulfill requests from law enforcement and regulatory bodies, which includes (1) complying with legal demands such as subpoenas, judicial orders, search or seizure warrants, or equivalent legal processes, and (2) responding to international law enforcement requests under mutual legal assistance treaties (MLATs) or formal letters of request;
 - d) to observe "**travel rules**" or similar regulations that necessitate sharing your information with other financial institutions, regulatory bodies, or industry partners;
 - e) when we firmly believe that disclosing personal information is crucial for safeguarding the rights, property, or safety of our clients/users, us, or the public, and to prevent imminent physical harm or significant financial loss;
 - f) to examine breaches of our Terms of Service or other relevant policies; or
 - g) to identify, investigate, prevent, or take action regarding fraudulent activities, illegal actions, or security and technical concerns, including reporting suspected unlawful activities or aiding law enforcement in such investigations.
2. **Business/Corporate Transactions:** Should Fintopio undergo significant business changes such as restructuring, being acquired, merging with another entity, divesting certain assets, or engaging in other substantial corporate transactions, such events might necessitate and potentially lead to the disclosure of your personal information as a component of these business activities. This sharing of information is often a critical element in facilitating and finalizing such transactions, ensuring a smooth transition and continuity of services.
3. **With Our affiliated entities:** We may exchange and/or your personal information among its affiliated companies for several purposes, including but not limited to delivering our services to you, preventing fraudulent activities, carrying out identity checks, adhering to legal requirements, and during events such as sales, mergers, acquisitions, or other significant business transactions.
4. **Collaboration with Service Providers and External Entities:** We partner with external companies and professionals to facilitate certain tasks on our behalf. This includes tasks such as data analysis and storage, marketing support, payment processing, content delivery, IT support, identity verification, and credit risk assessment and management. These third-party service providers are granted access only to the personal information necessary for executing their specific duties and are prohibited from using it for any unrelated purposes. Additionally, they are obligated to handle the personal information in line with our contractual agreements and in compliance with relevant data protection legislation. In cases permitted by applicable laws, your personal data might also be shared with another data controller when you exercise your right to data portability.

When engaging with third-party services or websites linked through our services (such as linking your Fintopio or wallet account with your banking services), those third-party providers may receive information about you that is shared by us, yourself, or others. It's important to be aware that the use of third-party services or products not covered by this Privacy Policy will be governed by their own terms and privacy policies.

5. **With Your Approval:** Additionally, we might share your Personal Data in scenarios explicitly outlined to you when the data is initially gathered, or in any specific context that you have agreed to. If you opt-in to receive regular email updates from us, including updates about our company, details on products and services, and other information, you have the freedom to withdraw from these communications at any time by utilizing the 'Unsubscribe' option included in each email.

6. How we use/process your data and the legal bases for doing so.

At Fintopio, we leverage the personal information in our possession for various purposes. Below is a detailed overview of the types of data we gather and the legal justifications for their collection.

How we process your data	Legal bases for processing your data
<p>- To provide our Services to you:</p> <p>1. We use your personal data to deliver our services to you, process your orders, enable transactions, and ensure the completion of the transactions you initiate. For instance, when you use the trading services (offered by third parties) on our platform, we may require specific details like your identification, contact details, and payment information.</p> <p>Personal Identifiers, Business Details, Transaction Records, Communication Details, Financial Data, Web Navigation Insights, and User Interaction Metrics are among the various categories of Personal Data processed by us.</p> <p>Note that We cannot provide our Services to you without this information.</p>	<ul style="list-style-type: none"> • Processing is necessary for the provision of our services and/ or the performance of a contract that you are a party to. • Processing is essential to serve both our legitimate interests and yours, particularly in enhancing the documentation associated with your transactions.
<p>- To enhance the integrity, safety, and security of our Platform.</p> <p>We process your personal data to:</p> <p>1. comply with applicable security laws and regulations, to monitor and verify identity or service access, to combat malware or security risks, and to enhance security.</p> <p>2. maintain the integrity of our services, identify and resolve violations of our Terms and Conditions, investigate suspicious activity, detect, prevent, and combat unlawful behaviour, identify fraud, and verify accounts</p>	<p>For the performance of a contract to which</p>

<p>and related activity.</p> <p>3. enhance the functionality, performance analysis, error resolution, and overall usability and efficacy of our services.</p> <p>Personal Identification Data, Business Information, Transactional Information, Contact Information, Financial Information, Browsing Information, and Usage Data comprise the categories of personal data that are processed by us.</p> <p>We may be unable to guarantee the security of our services if we do not process your personal data.</p>	<p>you are a party.</p>
<p>- To enhance the integrity, safety, and security of our services.</p> <p>For credit risks and the prevention and detection of fraud.</p> <p>Personal Identification Data, Business Information, Transactional Information, Contact Information, Financial Information, Browsing Information, and Usage Data comprise the categories of personal data that are processed by us.</p> <p>We process Personal Identification Data to safeguard against and counteract fraud and misuse of our services, aiming to protect you from account breaches and financial losses, while also ensuring the security of our users, and our services. Additionally, we may employ scoring techniques for evaluating and handling credit risks. It's important to note that for risk and fraud detection purposes, we might resort to automated decision-making processes. In such instances, we ensure the implementation of appropriate measures to protect your rights, freedoms, and legitimate interests, which includes the provision for human intervention, allowing you to present your perspective, and the opportunity to challenge the decision.</p>	<p>Processing is required to further our legitimate interests and those of our users. For instance, it is necessary to prevent and detect fraud and abuse to safeguard the security of our users, ourselves, and others.</p>
<p>- Communicate with you regarding matters pertaining to services and transactions.</p> <p>To correspond with you regarding our Services, specifically concerning account-related or administrative matters. We will maintain contact with you in order to provide you with information pertaining to our services. For instance, we may notify you of significant security concerns, updates, or other details concerning your transactions. In the absence of such communications, crucial account-related developments that could impact your ability to use our services might escape your notice. For legal or security purposes, you cannot opt out of receiving critical service</p>	<p>For the performance of a contract to which you are a party.</p>

<p>communications, such as emails or mobile notifications.</p>	
<p>- Managing our relationship with you under contract. In order to establish and uphold your wallet and/or account.</p> <p>To process payments and accept and manage orders using your personal data.</p> <p>Personal Identification Data, Business Information, Contact Information, and Financial Information comprise the category of personal data that is processed.</p> <p>Failing to process your personal data for these intentions may result in the denial of account creation or, if an account is already established, its closure.</p>	<p>For the performance of a contract to which you are a party.</p>
<p>- To improve our services;</p> <p>To enhance our services and provide you with a better user experience.</p> <p>Personal Identification Data, Business Information, Transactional Information, Browsing Information, and Usage Data comprise the categories of personal data processed by us.</p>	<p>The processing is required in furtherance of our legitimate interest to enhance the quality of our services and the satisfaction of our users.</p>
<p>- To Uphold Legal and Regulatory Compliance.</p> <p>Key aspects of our primary services, including our trading platforms, and payments and remittances services, are governed by stringent and precise legal and regulatory frameworks. These mandates necessitate the collection, utilization, and preservation of specific personal data, including Personal Identification details and, in certain instances, Sensitive Personal Information (such as biometric data). For instance, adherence to our "Know Your Customer" (KYC) responsibilities, as dictated by relevant laws and regulations, is crucial, especially in relation to Anti-Money Laundering regulations.</p> <p>Personal Identification Data, Business Information, Sensitive and Biometric Information, Government Identifiers, Contact Information, and Financial Information comprise the Personal Data category.</p> <p>Failure to furnish legally mandated personal data may result in the inability to establish an account or the closure of an existing wallet and/or account.</p>	<ul style="list-style-type: none"> • To fulfil our legal responsibilities under relevant legislation and regulations, including anti-money laundering laws and regulations. • For grounds of substantial public interest as determined by EU or EU Member State law, processing is required. We comply with the anti-money laundering directives of the European Union (EU) and the legislation of the relevant EU Member States that implements these directives. As such, we may be obligated to process data from your identification documents, including a photograph and a visual representation of your face (referred to as the "liveness check").
<p>- To adhere to other legal and regulatory obligations.</p> <p>Information may be accessed, read, preserved, and disclosed in accordance with the specific</p>	

<p>information specified under “How & Why we Share Your Information”, or when we reasonably believe it is necessary to do so in order to comply with the law, legal obligations, regulations, law enforcement, government, or other legal requests, court orders, or disclosure to tax authorities.</p> <p>Personal Identification Information, Business Information, Financial Information, Transactional Information, Browsing Information, Usage Data, and Blockchain Data are the categories of personal data processed by us.</p>	<ul style="list-style-type: none"> • To comply with our legal obligations under applicable laws and regulations. • To respond to legal inquiries even if compliance is not strictly required by law, if we sincerely believe that it is necessary within the relevant jurisdiction.
<p>- To conduct research and foster innovation.</p> <ol style="list-style-type: none"> 1. To gain further insights into your experience with our services, we conduct surveys. 2. To facilitate research and development (R&D) and drive product and service innovations. This data is also used for marketing objectives. 	<p>Processing is required in furtherance of our legitimate interest to enhance and operate our services using the data collected from these surveys.</p>
<p>- For records and internal business purposes.</p> <p>Personal Identification Data, Financial Information, Transaction Information, and Browsing Information comprise the category of personal data processed by us.</p>	<p>Processing is required in furtherance of our legitimate interest to:</p> <ul style="list-style-type: none"> • Maintain records to ensure that you comply with your contractual obligations under the agreement ("Terms and Conditions") regulating our relationship with you. • Fulfil our legal responsibilities to maintain specific records for internal business and research objectives.
<p>- To provide you with marketing communications.</p> <ol style="list-style-type: none"> 1. With your consent, we use your data to deliver tailored marketing communications via push notifications, mobile applications, email, and in-app platforms. 2. Additionally, we use your data to conduct marketing-related profiling. <p>Personal Identification Information, Business Information, Transactional Information, Browsing Information, Usage Data, Marketing and Research Information, and Communications are the categories of personal data processed by us.</p>	<ul style="list-style-type: none"> • We obtain your consent to process your personal data for marketing purposes, except as mandated by applicable law. You may revoke your consent at any time to the processing of your personal data for a specific purpose, at which point we will cease processing your data for that purpose. Preceding the withdrawal of consent, the lawfulness of processing is not impacted by the withdrawal of consent. • Messages pertaining to transactional accounts and correspondence concerning our business relationship will remain unaffected by your decision to opt out of marketing communications.
<p>- To provide you with promotional materials.</p>	<p>Processing pertaining to non-users is</p>

<p>To provide you with promotions, including offers, rewards, and other incentives for using our services, we utilise your information. This would also encompass providing you with the opportunity to participate in a survey, prize draw, or competition.</p> <p>Online Identifiers, Personal Identification Data, Business Data, Transactional Information, Browsing Information, and Usage Data are the categories of personal data that are processed by us.</p>	<p>essential to fulfil our legitimate interests as well as yours, which is to reward your customer loyalty.</p> <p>We obtain users' consent before processing their personal data in order to deliver promotional content. You may revoke your consent at any time to the processing of your personal information for a specific purpose, at which point we will cease processing your information for that purpose. Preceding the withdrawal of consent, the lawfulness of processing is not impacted by the withdrawal of consent.</p>
<p>- Personalisation and recommendations.</p> <p>To identify your preferences and tailor your experience with our services, to recommend features and services that may be of interest to you, and to do so, we use your personal information.</p>	<ul style="list-style-type: none"> • To fulfil our legitimate interest, which is to provide our consumers with a personalised service. • For the performance of a contract to which you are a party.
<p>- To deliver customer services:</p> <p>When you initiate communication with us, we will process your personal data in order to assist you with inquiries, disputes, complaints, problem resolution, and other related matters.</p> <p>Personal Identification Data, Business Information, Transactional Information, Communications, Contact Information, Financial Information, Browsing Information, and Usage Data are the categories of personal data that are processed by us.</p> <p>We may not be able to fulfil your requests unless we process your personal information for this purpose.</p>	<ul style="list-style-type: none"> • For the performance of a contract to which you are a party. • The processing is required in furtherance of our legitimate interest to enhance the quality of our services and the satisfaction of our users.

Anonymized or Aggregated Data: We transform your information into anonymized or aggregated data for various uses, such as generating anonymized demographic or location data, analyzing device usage for our services, or other pertinent analytics.

7. The controls, choices, and rights that you have.

Controls and Choices:

The relevant laws that govern your rights regarding your personal data are outlined in the following section for your convenience:

- a) **Email Correspondence:** Should you wish to no longer receive marketing emails from us, you have the option to unsubscribe via the link provided at the bottom of every marketing email. It's important to note, however, that you will still receive essential transactional emails related to your requested products or services. Mandatory communications from us regarding the Platform, updates to our Terms of Service, or this Policy are not subject to opt-out.

- b) **Do Not Track Settings:** Some web browsers offer a **Do Not Track ("DNT")** setting; however, Fintopio does not acknowledge or act on DNT browser signals or similar mechanisms.
- c) **Cookies and Targeted Advertising:** You have the capability to halt or limit the use of cookies and related technologies on your device by adjusting your browser or device settings. Be aware that changing these settings might affect the functionality of the Platform. On mobile devices, cookie-based preferences may not be fully operational. Nevertheless, you can opt out of targeted ads on several mobile apps by following platform-specific guidelines for Android, iOS, and other systems.

To further manage targeted advertising, you can visit and engage with self-regulatory platforms such as the Network Advertising Initiative (<https://thenai.org/opt-out/>), the Digital Advertising Alliance (<https://optout.aboutads.info/>), the European Digital Advertising Alliance (<https://youronlinechoices.eu/>), and the Digital Advertising Alliance of Canada (<https://youradchoices.ca/en/tools>). These platforms offer tools to opt out of targeted advertising from participating companies.

Kindly note, opting out needs to be done individually on each browser and device to ensure your choices are applied across all your access points.

Your rights:

As a valued user of Fintopio's Platform, you are entitled to specific rights concerning your personal data, as outlined below:

1. **Access your personal data:** You are entitled to confirm whether your personal data is being processed by us, obtain disclosure regarding certain aspects of the processing (the purposes of the processing, the categories of personal data concerned, the recipients of your personal data, the retention period of your personal data, etc.) and obtain a copy of the data along with detailed information on how it's being processed.
2. **Right to Restrict Processing:** In certain situations, you may ask us to halt the processing of your personal data temporarily, especially if there's a dispute regarding the data's accuracy or the processing's legality. We may continue processing your data if it's essential for legal claims or under other lawful exemptions.
3. **Right to Withdraw Consent:** For any data processing activities based on your consent, you retain the right to withdraw this consent at any moment. Withdrawing consent does not compromise the legality of processing performed prior to the withdrawal.
4. **Right to Data Portability:** Where applicable, you may request your personal data in a structured, commonly used, and machine-readable format. In some cases, we may also be able to transfer your data directly to another controller on your behalf.
5. **Right to Object:** If you have specific reasons related to your personal circumstances, you may object to the processing of your personal data. This right is particularly relevant when the processing is based on legitimate interests or for direct marketing purposes.
6. **Right to Erasure (to be forgotten):** Under certain conditions, you may request the deletion of your personal data. It's important to note that even after account deletion, we may retain specific personal data to fulfill legal obligations.

7. **Right to Rectification:** Should you find any personal data we hold about you to be inaccurate, you have the right to request corrections or additions to this data. You also have the ability to update your personal data directly within your account settings.
8. **Right to Contest Automated Decisions:** You have the right to challenge and request a review of decisions made solely through automated processes if these decisions impact your eligibility as our customer and/or user, considering our legal duties and interests.
9. **Right to Lodge a Complaint:** Should you have any concerns about our data processing practices, we are here to address them. If issues persist, you have the right to file a complaint with the data protection authority in your region or where you believe a breach may have occurred.

If you have any questions or objections as to how we collect and process your personal data, or want to your rights as stated above, please contact us using help@fintopio.com via our Telegram bot [@fintopiohelp](https://t.me/fintopiohelp).

Please note that to prevent errors and abuse, we may need to verify the requestor's identity and may request additional information from you. Furthermore, please be aware that if you request the deletion of your personal data, we will fulfill this request within 30 days.

8. Cookies and how we use them.

Cookies are diminutive text files that are downloaded to a user's computer or mobile device upon visiting a website, or are stored on the user's device, enabling the website to identify the device. Cookies retain data pertaining to the user's sessions, encompassing details such as accessed advertisements, language preference, time and duration of each visit, and the content viewed. "First party cookies" refer to those that are exclusively managed by Fintopio; whereas "third party cookies" refers to cookies that originate from, and are managed by third parties.

Cookies are a multifunctional mechanism that performs numerous tasks, including facilitating efficient page navigation, remembering user preferences, and enhancing the overall user experience. They facilitate our ability to determine your preferences and ensure that online advertisements are more pertinent to your interests. A variety of cookie sets exist, which are elaborated in our Cookie Policy at [\(Link\)](#).

We acknowledge that Cookies should be regarded as personal data and their handling should be subject to the relevant legislation. If you do not consent to our use of Cookies, you have the option to modify your Cookie settings within your browser preferences. Below, you will find links providing further information on adjusting settings for various browsers:

Chrome	link to Chrome Cookie Settings
Edge	link to Edge Cookie Settings
Safari	link to Safari Cookie Settings
Firefox	link to Firefox Cookie Settings

If you wish to exercise more control over Cookie settings, you can install specialized browser programs or add-ons commonly referred to as anti-tracking tools. These tools enable you to select which Cookies are permitted to be stored on your device.

Revisiting Your Cookie Preferences: We recognise the significance of retaining the ability to modify your cookie preferences in response to evolving privacy concerns. We have included a Cookie Settings link at the bottom of each page of our website to facilitate this. You can effortlessly reestablish the cookie banner by clicking on this link, providing you with the ability to assess and modify your choices at any given moment. Our inclusion of this function signifies our dedication to granting you complete authority over the data gathered throughout your engagements with our website.

9. Marketing, and advertising.

By using our services, you acknowledge and agree to the display of marketing content and advertisements tailored to enhance your user experience. We may utilize information gathered during your interaction with our site to present you with promotions, offers, and advertising that we believe may be of interest to you. Our aim is to provide you with relevant and valuable marketing communications; however, you will always have the option to opt-out or customize your advertising preferences through your account settings or by following the instructions provided in our communications. Please note that opting out of marketing communications does not exempt you from receiving non-promotional, service-related notices.

10. The privacy policies of other websites/applications/platforms.

Our website and/or platform may contain links to external sites or platforms that are not operated or controlled by us. Kindly be informed that when you click on these links and leave our website and/or platform, you will be subject to the privacy policies and practices of the external sites or platforms, which may differ significantly from our own. We expressly disclaim any liability for the content, operations, privacy policies, or practices of any third-party sites, platforms and/or services that you access through our platform. We strongly encourage you to review the privacy policy of every site or platform you visit to ensure your personal information is treated with the care and respect it deserves.

It is strongly advised that you thoroughly examine the privacy policy of every site or platform you visit or access, in order to ascertain that your personal information is treated properly and in compliance with the relevant data protection regulations, and data privacy practices.

11. Our practices on children's privacy.

We are committed to protecting the privacy of children. Fintopio Services are not designed for, targeted at, or intentionally marketed to children under the age of **eighteen (18)** (or a higher age threshold where applicable by local law). We do not knowingly collect, use, or disclose personal information from children under the specified age without obtaining prior consent from a parent or legal guardian.

Should we become aware that we have inadvertently received personal information from a child under the relevant age threshold without the requisite parental or guardian consent, we will take steps to immediately delete such information from our records. We encourage

parents and guardians to take an active role in their children's online activities and interests and to educate them about safe internet use practices. If you believe we might have any information from or about a child in violation of this Policy, please contact us promptly.

12. Our data security and integrity policies and practices.

Our systems are created with your privacy and security in mind. We have implemented the necessary security measures to safeguard your information from accidental loss, unauthorised use or access, modification, or disclosure. Using encryption software and protocols, we make every effort to safeguard your personal information during storage and transmission. Physical, electronic, and procedural safeguards are in place to ensure the protection of your personal data during collection, storage, and disclosure. Additionally, only those employees, agents, contractors, and other third parties with a legitimate business need to know are granted access to your personal information. In accordance with our security protocols, you may be required to provide identification to prevent unauthorised access to your account or wallet.

Our employees and third parties accessing your data are contractually obligated to maintain the confidentiality of your personal data.

We continually enhance our data security systems and exert every effort to prevent data breaches. In the event of a data breach, we are committed to promptly notifying users and the appropriate regulatory authority about the incident as well as taking all necessary measures to mitigate any adverse consequences.

For example, we have taken no less than the following measures:

- Designation of an individual in charge of supervising personal data management;
- Restricting access to personal data only to authorized employees;
- Securing data through encryption during storage and transmission;
- Establishing the protocol for deleting personal data after its retention period expires;
- Conducting internal checks to adhere to personal data security standards;
- Setting guidelines for accessing personal data within the data processing systems;
- Establishing the protocol for addressing data security breaches.

If you have a reason to believe that your interaction with us is no longer secure, please immediately notify us of the problem by contacting us via email: help@fintopio.com or Telegram bot [@fintopiohelp](https://t.me/fintopiohelp).

13. Our global data transfer, and storage/retention practices.

We operate globally and may transfer your personal information to individual sister and/or affiliated companies or third parties in locations around the world for the purposes described in this Policy. Wherever your personal information is transferred, stored, or processed by us, we will take reasonable steps to safeguard the privacy of your personal information. These steps may include implementing standard contractual clauses, where recognized by law, obtaining your consent, or other lawful means of transferring personal information.

We may transfer a portion of the information you provide to us to countries other than the European Economic Area (EEA), the United Kingdom, or your country of domicile. It is possible that these nations do not have data protection laws comparable to those of the United

Kingdom and the European Union. In instances where we transfer your information in this manner outside of your country of residence, the United Kingdom, or the European Economic Area, we implement suitable security measures to safeguard your privacy rights in accordance with the regulations specified in this Policy and data protection legislation. Contractual obligations are imposed on the recipient of your personal information as part of these procedures. Please utilise the contact information provided at the conclusion of this Policy to obtain further clarification regarding the safeguards we have implemented, as well as to request a copy of the pertinent documents or gain access to them.

In order to facilitate your ongoing utilisation of our Services, we store or retain your personal information for the duration necessary to accomplish the objectives outlined in this Privacy Notice, as well as as mandated by law, including but not limited to reinforcement of legal claims and compliance with anti-money laundering regulations, resolution of disputes and legal proceedings, or as otherwise advised to you.

Although retention requirements may differ across jurisdictions, the following section provides an overview of the customary durations for which we retain various components of your personal data.

For audit and crime prevention purposes, content that you publish on our website, including support desk comments, photographs, videos, and blog posts, may be retained after you terminate your account.

Data collected through analytics tools such as web page counters, cookies, and similar methods is retained for a maximum duration of one year starting from the date the relevant cookie was collected.

Obtain Contact For marketing purposes, personally identifiable information including your name, email address, and telephone number is retained continuously until either you (a) discontinue your subscription, or we (b) terminate your account. We will subsequently add your information to an unsubscribed list to prevent us from accidentally marketing to you.

To fulfil our legal responsibilities under financial or anti-money laundering legislation, we may retain Personally Identifiable Information (PII) beyond the account closure period, for the duration specified by such legislation.

14. How you can contact us with complaints and questions.

If you have any questions or complaints about this Policy or our handling of personal data, please contact us at any of the following:

- Telegram bot: [@fintopiohelp](#)
- Email: help@fintopio.com

After receiving the request, we will contact you to find out how we can help. If you have any complaints about how we process your personal data, we would always prefer that you contact us first.

Before responding to your request, we will take reasonable steps to verify the identity of the person making the request. If we have doubts about the identity of the person making the request, we may ask for additional information to confirm your identity. If we are still not in a position to identify you after having requested additional information, we may refuse to act on your request.

15. How to contact the relevant regulatory authorities.

We kindly request that you contact us directly with any concerns or inquiries you may have regarding our utilisation of your personal information. This will enable us to promptly attend to your concerns. Nevertheless, should you believe that your inquiries remain unresolved or need additional support concerning your rights or the management of your data, you are permitted to reach out to the appropriate regulatory bodies.

For concerns pertaining to our services within the United Arab Emirates, particularly in Dubai, please contact:

- UAE DATA OFFICE, affiliated to the UAE Cabinet.
- General Secretariat of the Cabinet,
- PO Box 899,
- Phone: 0097128887777,
- Website: <https://uaecabinet.ae/en>,
- Abu Dhabi, United Arab Emirates (UAE).

Given our global presence and the international nature of our services, we also have affiliated entities in different jurisdictions. Should your concerns pertain to services offered in these regions, you may contact the respective authorities:

For EU Residents:

If you are a resident of the European Union and have concerns related to data protection and privacy, you may wish to contact the relevant data protection authority within your country. Given our affiliated entities in Poland, we provide the contact details of the Polish data protection authority, which is part of the European Data Protection Board (EDPB).

- Office of the Personal Data Protection President (UODO)
- Address: **Stawki 2, 00-193 Warsaw, Poland**
- Telephone: **+48 22 531 03 00**
- Fax: **+48 22 531 03 01**
- Email: kancelaria@uodo.gov.pl
- Website: <https://uodo.gov.pl/en>

This authority is responsible for overseeing data protection laws and ensuring that the rights of individuals are protected in Poland. They provide guidance for individuals about their rights under the General Data Protection Regulation (GDPR) and can assist with concerns or complaints related to data processing activities.

For EU residents outside Poland, you can find the contact details of your national data protection authority on the European Data Protection Board's website: https://edpb.europa.eu/about-edpb/board/members_en

For residents of the Kyrgyz Republic, you can contact the Personal Data Protection Agency under the Cabinet of the Ministers of the Kyrgyz Republic.

- Address; **265a, Chui Ave., Bishkek, Kyrgyz Republic.**
- Contact Number: **+(996) 312 641 014,**
- Email Address: **info@dpa.gov.kg,**
- Postal Address: **720071.**

16. Privacy Notice for UK and EU residents.

This **Privacy Policy Notice** is specifically intended for individuals residing in the European Economic Area (EEA) and the United Kingdom (UK) and serves as a supplement to our Global Privacy Policy. This Notice is established in adherence to the General Data Protection Regulation (GDPR) requirements. Within the scope of this section, the term "Personal Data" is defined as per the General Data Protection Regulation (EU) 2016/679, which is incorporated into the legal frameworks of England, Wales, Scotland, and Northern Ireland by the European Union (Withdrawal) Act 2018. This Privacy Notice should be read in conjunction with our Global Privacy Policy.

Local Representative and Controller of Personal Information:

FINTOPIO FZ LLC is the controller of the personal information it collects; however, representatives and/or affiliates have been appointed in the European Union and the United Kingdom in adherence to relevant data privacy legislation.

The following are the contact details for our European Union representative:

- Company Name: **FINTOPIO SP. Z O.O.,**
- Address: **Grzybowska 2/29, Warsaw; Mazowieckie;**
- Postal Code: **00-131**
- Country: **Poland**

LEGAL BASIS FOR DATA PROCESSING

For those in the European Economic Area (EEA) or the United Kingdom (UK), our processing of your Personal Data is confined to specific, narrow purposes and is conducted only when there's a legitimate legal ground for processing, as defined by the relevant data protection regulations. The legal grounds we depend on for processing your Personal Data, when applicable, are outlined as follows:

- a) **Contractual Necessity:** Required for the fulfillment of a contract we have with you or to take preliminary steps at your behest before formalizing a contract.
- b) **Legal Compliance:** Essential for us to adhere to legal or regulatory obligations.
- c) **Legitimate Interests:** Important for the pursuit of our valid and lawful interests, with a careful balance against your rights to privacy and other fundamental rights and freedoms. This can encompass:
 - Ensuring the security of our systems, including fraud detection and prevention, within the bounds of the law,
 - Operation of our services,
 - Undertaking marketing, market research, and business development activities,
 - Handling internal administrative tasks within our group of companies,
 - Managing our interactions with you, for instance, by responding to your queries or requests,
 - Facilitating corporate transactions such as mergers, restructurings, acquisitions, and the transfer of assets,
 - Efficient management and provision of Fintopio services and associated activities,
- d) **Consent:** Based on your explicit consent.

Where consent serves as the legal basis, you are entitled to withdraw your consent at any moment, which won't affect the legality of any processing carried out prior to withdrawing your consent.

PERSONAL DATA COLLECTION

Personal Data pertains to information that can identify or is linked to an individual. Our methods of collecting personal information through our services are detailed below, with further insights available in our Global Privacy Policy.

- a) **Direct Collection from Users:** When you engage with our platforms, including websites, social media channels, mobile apps, online ads, or marketing and sales communications, we gather data. This also applies when you purchase our products or services. The collected data encompasses names, email addresses, phone numbers, along with various demographic and contact details.
- b) **Data Acquired from External Sources:** While using our services, we gather the following information from external entities:
- c) **Service Integrations:** Information about you is received through integrations with services you choose to connect with, like linking accounts from other service providers, including other cryptocurrency platforms, to your Fintopio account and/or wallet.
- d) **Third-Party Login:** When you access our services using login credentials from third parties (such as Google), we obtain information made available through your privacy settings with that third party.
- e) **Information from Public Sources:** We also collect information about you from publicly accessible sources when you use our services. These sources include:
 - Social Media,
 - Google search,
 - Blockchain,
 - Public digital address.

Please be aware that the information we have directly obtained from you may be combined with information we have obtained from other sources or from publicly accessible sources.

- f) **Passive Collection from Individuals:** We employ third-party technologies to passively gather data from individuals who visit our websites or interact with our emails. Through the use of cookies and similar tracking mechanisms, we automatically obtain:
 - IP address,
 - device type,
 - links clicked,
 - browser type,
 - pages viewed,
 - date and time of visit,
 - operating system version,
 - unique device identification numbers,
 - number of times you return to our website.

For information on how to manage your cookies preferences, please see our Online Privacy Notice or visit www.aboutcookies.org.

- g) **Information Integration:** We merge data acquired from external sources with the information we already possess. Additionally, we amalgamate details from an individual's profile with responses obtained through surveys.

STORAGE AND RETENTION OF PERSONAL DATA.

Fintopio retains and processes Personal Data only for the duration necessary to fulfill its operational and legal obligations. Personal Data is either deleted or made anonymous when it's no longer needed for its original purpose. The retention period for your information varies based on its type, the reason for its collection, and whether the information has been de-identified. In determining the retention period, we consider the legally required minimum retention time, industry recommendations, and other legal duties. Moreover, you have the right to request the deletion of your Personal Data as outlined in the Section on the "Rights of Data Subjects" below.

We might be obligated to keep your Personal Data to:

- uphold rights.
- settle disputes; and
- abide by legal requirements.

RIGHTS OF DATA SUBJECTS.

We are committed to ensuring that you are fully cognizant of your data protection rights as outlined by the GDPR. Each user is entitled to the following rights:

1. **The right to access:** You are entitled to request us for copies of your Personal Data.
2. **The right to be informed:** You possess the right to receive clear information about how your Personal Data is being used.
3. **The right to rectification:** You have the right to ask us to amend any data you deem inaccurate. Additionally, you can request the completion of data you believe is incomplete.
4. **The right to erasure:** You can request the deletion of your Personal Data from our records, subject to specific conditions.
5. **The right to restrict processing:** Under certain conditions, you have the option to request that we limit the processing of your Personal Data.
6. **The right to object to processing:** You have the right to oppose the processing of your Personal Data by us, under certain circumstances.
7. **The right to data portability:** Under certain conditions, you have the right to request that we transfer the data we have collected about you, to another organization, or directly to you.
8. **The right to not be subject to automated decision-making:** You have the right not to be subjected to a decision solely based on automated processing if it significantly affects you legally.

Upon receiving a request, we will have one month to respond. For requests that are particularly complex or numerous, we may extend this period. Should an extension be necessary, we will inform you within one month, explaining the reasons for the delay. If you wish to exercise any of these rights, please reach out to us at our email: help@fintopio.com, with the subject line "**GDPR Request**".

USE OF COOKIES.

Cookies are diminutive text files deposited by your browser onto your computer or mobile device. They fulfil various roles, aiding in seamless navigation across web pages and potentially enhancing the overall website experience. Cookies can be "persistent" or "session-based" depending on their lifespan and may originate from us directly ("first-party" cookies) or from third parties acting on our behalf ("third-party" cookies).

Fintopio and its affiliated service providers deploy cookies to gather details on your web browsing patterns over time and across different web pages. At Fintopio, cookies are utilized to:

- Manage and provide our services,
- Assess usage of our services and discern trends,
- Monitor your web navigation history,
- Enhance the functionality and user-friendliness of our services.

For more detailed information, please refer to our Cookies Policies at ([include link](#)).

INTERNATIONAL DATA TRANSFERS.

Fintopio FZ LLC is located in Dubai, the United Arab Emirates (UAE). We use data hosting services providers operating within the UAE to store the information we collect from our users. In situations where we need to transfer your Personal Data outside of the EEA or the UK, we ensure compliance with GDPR by employing recognized cross-border transfer mechanisms. Where necessary by law, we safeguard such international transfers of your Personal Data using suitable legal frameworks to ensure adequacy. Typically, we rely on Standard Contractual Clauses approved by regulatory authorities to guarantee that Personal Data receives an adequate level of protection when transferred outside the EEA or the UK to jurisdictions lacking comparable data protection standards.

For further details on international data transfers or to request a copy of the Standard Contractual Clauses, please reach out to us at help@fintopio.com with the subject line "GDPR Request." Additionally, as outlined in Section 6, "Sharing Personal Data with Third Parties," we may share your Personal Data with third parties under specific circumstances.

EXTERNAL WEBSITES' PRIVACY POLICIES.

Our website may include links to external websites and services. It's important to note that our privacy policy is applicable solely to our own website. Therefore, if you navigate to another website or service via a link, we encourage you to review their privacy policy.

UPDATES TO THIS POLICY.

We reserve the right to modify or update this Privacy Notice as necessary in the future. Any changes will be promptly reflected on our website. The effective date of the latest update to this notice will be clearly indicated at the top of this page. In the event of significant changes to this Privacy Notice, we will either highlight the updates on our website or directly inform our clients via email.

ENGAGING WITH REGULATORY AUTHORITIES.

If you have a complaint or believe that Fintopio has not adequately addressed your concerns or may have violated your rights, you are encouraged to contact the data protection authority in your country of residence, work, or where you believe an infringement may have occurred.

GET IN TOUCH WITH US.

For any inquiries regarding this privacy notice or our privacy practices, please feel free to reach out to us. You can email us at help@fintopio.com, using the subject line “**GDPR Inquiry.**”

17. Privacy Notice for EMEA Residents.

This privacy notice is pertinent to residents of Middle Eastern, African, and non-EU European countries and should be considered an integral part of our Global Privacy Policy.

Usage of Your Personal Data and Your Rights:

Engaging with Fintopio's websites and/or platforms, whether by visiting, registering, or using any Fintopio products, services, web, or mobile applications, places your personal data under the jurisdiction of Fintopio FZ LLC, located at 5DMC, Dubai Media City, Dubai, UAE.

For users of Fintopio's services residing in the Middle East, Africa, or European countries outside of the EU, please note that your personal data is processed by **Fintopio FZ LLC**.

The primary use of your personal data is to furnish you with the Fintopio products and services you solicit. It may also be employed to adhere to legal mandates, or to cater to our legitimate interests, such as enhancing your user experience, improving our services, or identifying unlawful conduct. With your explicit consent, it might also be used for sending you promotional materials and offers.

You are entitled to several rights, including the right to access, modify, or delete your personal data, or to alter your marketing preferences (including retracting any previously granted consent at any moment) – our Privacy Policy provides further details on how to manage your marketing preferences or delete your account and/or wallet.

For any inquiries or concerns regarding data protection, our Data Protection Officer can be reached at: help@fintopio.com.

Should you wish to file a complaint regarding data protection, you have the authority to do so with your local Data Protection Supervisory Authority or with the designated authority in Dubai.

For comprehensive insights into how Fintopio collects and uses data, we recommend reading through our Global Privacy Policy.

DATA CONTROLLER:

Data Controller: **Fintopio FZ LLC**,
Location: 5DMC, **Dubai Media City, Dubai – UAE**.

18. The Definition of “Terms” used in this Policy.

“Platform” refers to the software provided by Fintopio, which includes any websites, telegram bot, pages, features, or content owned or operated by Fintopio, any web-application or mini app developed or made available by Fintopio, as well as any application programming interfaces (APIs) offered to users or third-party applications dependent on such APIs where users can manage virtual assets wallets and interact with blockchain networks. This also encompasses any other means Fintopio may designate in the future for accessing Fintopio Wallet Services.

“Fintopio Wallet” refers to a digital wallet provided by Fintopio where users can deposit, store, trade, Swap, send, and receive and withdraw virtual assets through third parties.

“Third-Party Services” refer to the Services related to virtual asset activities such as exchanging, swapping, buying, selling of virtual assets, on-ramp, off-ramp, and other services provided by third parties and accessible through or within Fintopio Wallet.

“Fintopio Wallet Services” refers to all the features, tools, materials, or services offered by Fintopio, including the Fintopio Wallet accessible through its website, the Telegram integrated Fintopio Bot, and/or mini-app, aimed at creating and managing digital wallets and facilitating interaction (depositing, storing, trading, Swapping, transferring, sending, receiving and withdrawing virtual assets) with blockchain networks through decentralized application (DApp) websites.

“Mini-app” refers to a smaller, lightweight application within the Fintopio ecosystem that provides specific functionalities related to Fintopio Wallet Services.

“Telegram integrated Fintopio Bot” refers to a specialized bot within the Telegram app that provides users access to Fintopio Wallet Services directly through the Telegram platform.

“User” refers to any individual or entity that uses or accesses the Platform or Fintopio Wallet Services or any other services provided by Fintopio.

“Virtual or Digital Assets” refers to a digital representation of value or rights that can be transferred and stored electronically, including virtual assets and tokens supported by the Fintopio Wallet.

“Non-Custodial Wallet” refers to a type of digital wallet where the user retains full control of their private keys and, therefore, full control over their funds. Fintopio Wallet is a non-custodial wallet.

“Cookies” refer to small fragments of data sent by our web server and stored on a user’s device. Cookies are stored when you visit the Website, and this allows us to help the Website work effectively. Cookies allow us to save your selected settings (e.g., language) and analyze Website traffic. You have the right to disable Cookies that you do not want to be used in the Cookie-banner on the Website. However, please note that you cannot disable Cookies that are necessary for the functionality of the Website.

“Device” refers to a device from which you use our Services. Devices include mobile devices, tablets, personal computers, consoles, etc.

“Device information” refers to technical information about your Device. Device information includes browser data and types of browser plug-ins, operating system and its version, information about the type and manufacturer of said Device, and the language set for the Device.

“Know Your Customer (KYC)” refers to the mandatory process undertaken by Fintopio via its affiliates and/or third-party services providers, to verify the identity of their clients. It is designed to ensure the authenticity of clients’ identity and assess potential risks of illegal activities for the business relationship.

“Personal data” refers to any information that can directly or indirectly identify an individual, like names and email addresses, location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions etc.

“Data processing” refers to any action performed on data, whether automated or manual, including collecting, recording, organizing, structuring, storing, using, and erasing.

“Data subject” refers to customers or site visitors whose data is being processed.

“Data controller” refers to the person who decides why and how personal data will be processed.

“Data processor” refers to any third party that processes personal data on behalf of a data controller.

“Aggregate Information” refers to information about groups or categories of website visitors, which do not identify and cannot reasonably be used to identify an individual user.

“Children” refers to individuals who we have identified are not of legal age to consent to the collection and processing of their personal information.

“IP Address” refers to the access point through which you enter the Internet and is typically controlled by your Internet Service Provider (ISP), or your company.

“Anonymous Information” refers to information that does not directly or indirectly identify, and cannot reasonably be used to identify, an individual user.

“Public Forums” refers to message boards, conversation pages, blogs, chat rooms, social community environments, profile pages, and other forums that do not have a restricted audience.