

Privacy Policy

Last Updated: 3 September 2025

At Wefi, we prioritize the safeguarding of your personal data and respect your right to privacy. This Privacy Policy defines how we gather, handle, and safeguard your personal data, specifically referring to any information pertaining to an individual through which the User can be distinctly identified. All our data processing activities are in strict compliance with prevailing data protection laws of Canada (including Federal Personal Information Protection and Electronic Documents Act ("PIPEDA") and provincial statutes). Additionally, in order to follow best market practices in our business, we voluntarily follow the fundamental principles of Regulation (EU) 2016/679, known as the General Data Protection Regulation ("GDPR").

This Privacy Policy serves to assure our Users of the integrity and security measures we employ in handling their Personal Data. We are steadfast in our commitment to uphold the trust you place in us when sharing your data.

For the purposes of this Privacy Policy, unless explicitly stated otherwise, all terms shall bear the meanings attributed to them in our Terms and Conditions.

It is pertinent to highlight that this Privacy Policy is primarily intended for our Users and potential customers. Should you be an employee, contractor, or service provider affiliated with Wefi Payments Limited and/or S.R.L., the processing of your Personal data will be governed by your employment or contractual agreement, or in line with our distinct policies. For more details or to access these policies, please reach out to us using the contact information provided in the subsequent contact section.

I. DEFINITIONS

For the purposes of this Privacy Policy, the following terms shall have the meanings set forth below:

Audio Data refers to the data which includes complete voice recordings of calls that you either receive from us or initiate with us.

Company (or "Wefi", "we", "us" or "our") refers to Wefi Payments Limited and/or S.R.L.

Contact Data refers to information used to get in touch with you.

Content Data refers to information you share or upload, such as images, videos, or other materials.

Financial Data refers to information related to payments or purchases, such as payment details or related records.

Identity Data refers to information that identifies you personally.

KYC Data (Know Your Customer) refers to information collected to confirm your identity.

Location Data refers to information about where you are when using our services, such as general regional or setting-related details.

Marketing and Communication Data refers to information about your preferences for receiving updates, promotions, or other communications.

Personal Data refers to any information that relates to you and could be used to recognize or identify you.

Privacy Policy refers to this document that explains how we collect, use, share, and manage your information.

Profile Data refers to information about your account, such as login details, interests, or feedback you provide.

Technical Data refers to information about how you access and use our services, such as device or system details.

Terms and Conditions refers to the agreement that sets out the rules and responsibilities between you and us.

Transaction Data refers to information about your activities with us, such as purchases, payments, or account interactions.

Usage Data refers to information about how you engage with our services.

User (or "you" or "your") refers to the individual or entity accessing the Website as the User.

Consequently, the terms "Your" and "Yours" should be interpreted in relation to You.

Website refers to the internet site located at wechain.ai, including all subdomains, subpages, and associated online platforms operated by Wechain.

II. WHO WE ARE

We are a platform, providing

- fiat services through:

Wefi Payments Limited: A registered money services business (number: M23563590) with the corporate number 2025535572, authorized by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), having its registered office Suite 2700, 225 - 6th, Avenue SW, T2P1N2, Calgary, Alberta, Canada.

- and all other services including cryptocurrency exchange (crypto to crypto), as well as technical services by:

S.R.L.: a company registered in Costa Rica with the corporate number 3-102-939581 having its registered office at: Province 01 San Jose, County 15 Montes De Oca, District One San Pedro, Los Yoses, Avenues Eight and Ten, Street Thirty-Nine, LY Center.

We are the controller and accountable for the Personal Data of the User shared with us during account registration or while availing any services offered through the wefi.co (together with its subdomains), all subdomains and all their respective pages ("**Website**").

Your privacy is of utmost importance to us, and we are committed to ensuring the safety of the data you provide. We have in place robust data protection standards and consistently review and

adapt them to ensure the security of user data and accounts. Your Personal Data is safeguarded by a combination of legal, administrative, and technical measures, all designed to uphold its privacy, integrity, and availability. Our approach to Personal Data protection is comprehensive, blending both organizational and technical strategies, and is informed by our yearly risk evaluations.

We maintain strict confidentiality regarding our Users' private information. Such information will only be shared upon receiving the User's written consent, unless mandated by law, necessary for identity verification, or essential for fulfilling our contractual obligations with the User. Personal Data processing is carried out by our dedicated team. All Personal Data is securely stored, both electronically and physically, according to applicable law.

III. DATA USAGE

We may collect, use, store, and transfer various types of data about you, categorized as follows:

- **Identity Data**
- **Contact Data**
- **Financial Data**
- **Transaction Data**
- **Content Data**
- **Technical Data**
- **Profile Data**
- **Usage Data**
- **Marketing and Communication Data**
- **KYC data (Know your customer)**
- **Location Data**
- **Audio Data**

Aggregated data encompasses data that is statistical or demographic. This type of data is derived from your Personal Data but is not considered as such under the law since it doesn't reveal your identity, either directly or indirectly. For instance, we might use your Usage Data to determine the percentage of users engaging with a particular feature on the Website. However, if this aggregated data, when combined with other data, identifies an individual, we will treat it with the same care as Personal data according to our policies. We ensure that your data is processed with integrity, transparency, and fairness, always keeping the intended purpose of data collection in mind. We also adhere to principles like data minimization, accuracy, and limited data storage.

We primarily collect and process Personal Data for the following reasons:

- To perform its contract with you;
- To comply with its legal obligations; and/or
- To safeguard its legitimate interest.

If you don't provide the necessary data when asked, it might hinder our ability to offer you certain services. In such cases, we might have to terminate a service you're using. We'll inform you if such a situation arises. It's crucial for us that the data we have on you is up-to-date and accurate. Kindly inform us of any changes in your data during our association.

The User should be aware that we will store data related to the User's account and transactions. This data might be referenced in case of any disputes between us and the User. It's the User's responsibility to keep us updated with accurate data. While we make efforts to ensure the data's accuracy and occasionally review the information you provide, we might not always be able to do so without your assistance. The User should recognize that we don't bear any obligation or liability due to any such reviews or inspections of the data.

IV. HOW IS YOUR PERSONAL DATA COLLECTED

We use different methods to collect data from and about you, including through:

Direct Interactions. Most of the data we collect comes directly from you. You provide us with your Identity, Contact, and Financial Data online via the Website and/or by filling in online forms and/or by corresponding with us by emails or otherwise. This can be done when you:

- Create an account on our platform.
- Engage with our services.
- Purchase our products or services.
- Subscribe to our updates or publications.
- Opt to receive marketing materials.
- Provide feedback or request notifications about new products or updates.
- Reach out to us with inquiries or other requests.

Automated Technologies or Interactions. In the course of utilizing our Services, your device automatically transmits its technical specifications to us. The Locale (a combination of parameters setting regional preferences such as residence country, time zone, and interface language) is utilized to enhance service quality within the Website. We employ information such as IP addresses, cookie files, browser and operating system details, access timestamps, and requested page addresses to optimize the performance of the Website. This data is also used to monitor user behavior, thereby improving the efficiency and user-friendliness of our Services.

We employ web analytics tools and cookies to track the Website's performance and the sources of user engagement. This practice is aimed at refining our marketing strategies and providing users with an enhanced browsing experience.

You have the option to cease such data transmissions at any time (within the extent feasible and as per our legal obligations) by submitting a request using the contact details provided below, using the registered email address associated with your Account. We will endeavor to address your request within 30 business days.

Cookies and Automatic Data Collection Technologies: A cookie is a small data unit, frequently including a unique identifier, sent from a website's computer to your device's browser and stored on your device's hard drive to monitor site usage. Your browser settings permit a website to access only the cookies it has sent, safeguarding your privacy. This practice is commonly used by many websites to track online traffic patterns.

Stored cookies may outline a user's path on our site, anonymously identifying repeat visitors and highlighting popular pages. However, to preserve user privacy, personal details such as names and emails are not stored. While cookies are an industry standard widely used by major websites, it is possible to configure your browser to reject cookies from this site or even to delete cookies automatically or manually. However, please be aware that such actions may limit your access to all the functions provided on the Website.

Third parties or publicly available sources. We may obtain Personal data concerning you through various means, including when you visit other websites that use our cookies or from third parties such as business partners (including affiliates participating in affiliate marketing programs), subcontractors providing technical, payment, and delivery services, advertising networks, analytics providers, and providers of search information.

User contributions. You may also contribute Content Data for us to publish or showcase in public sections of the Website, or to send to other Users or third parties. You assume the responsibility for submitting Content Data for publication or transmission, understanding that it carries some inherent risk. While you have the option to configure privacy settings for Content Data through your account profile, it's important to note that no security measures are entirely flawless or invulnerable. Moreover, we lack control over the behavior of other website users with whom you decide to share your Content Data. Therefore, we cannot ensure or promise that unauthorized individuals won't have access to your Content Data.

V. PURPOSE FOR WHICH WE WILL USE YOUR DATA AND ON WHAT LEGAL BASIS

We process the aforementioned data in accordance with the provisions outlined in the PIPEDA and relevant provincial statutes, subject to amendments over time. This processing is carried out to achieve the following objectives:

- (i) Fulfillment of Contractual Obligations: We process data to effectively fulfill our contractual commitments to the User and provide them with optimal service quality.
- (ii) Efficient Service Provision: Data processing supports the efficient delivery of our Services.
- (iii) Legal and Regulatory Compliance: We process data to adhere to legal and regulatory requirements.

Data processing is carried out on the following legal basis:

- Compliance with Legal and Regulatory Obligations.
- Execution of Contractual Commitments towards the User.
- Protection of Legitimate Interests: We process data when it aligns with our legitimate interests, provided that your interests and fundamental rights do not supersede those interests.
- Consent Basis: Data processing may occur based on your explicit consent.

Hereafter, we outline the various ways we intend to utilize your data, accompanied by the corresponding legal basis. In cases where applicable, we specify our legitimate interests as well.

Please be aware that data processing may rely on multiple legal grounds, contingent on the specific purpose for which your data is used.

-	PURPOSE ACTIVITY	TYPE OF DATA	LAWFUL BASIS FOR PROCESSING, INCLUDING BASIS OF LEGITIMATE INTEREST
a.	1. For account activation (to accept registration as a User). 2. To notify you about changes to our terms or privacy policy. 3. To communicate with you and provide you with secure identification, authentication and support services. 4. To confirm you are at the age of majority as recognized and declared by the laws of your jurisdiction. 5. To participate in features on the Website.	1. Identity Data 2. Profile Data 3. Contact Data 4. KYC data 5. Financial Data	1. Necessary to perform our contract with you 2. Necessary to comply with our legal obligations
b	1. To verify the accuracy of information provided by you regarding your location.	1. Profile Data 2. Location Data 3. Content Data 4. Usage Data	1. Necessary to perform our contract with you 2. Necessary to comply with our legal obligations
c	1. To ensure secure authentication, identification, and support services through social network protocols, utilizing links to your social network accounts for this purpose.	1. Technical Data	1. Necessary to perform our contract with you 2. Necessary to comply with our legal obligations
d	1. To process and fulfill your transactions and requests.	1. Financial Data 2. Transaction Data	1. Necessary to perform our contract with you 2. Necessary for our legitimate interest

e.	1. To administer and protect our business and Website, encompassing troubleshooting, data analysis, testing, system maintenance, support, reporting, and data hosting.	1. Identity Data 2. Contact Data 3. Technical Data 4. Content Data	1. Performance of our contract with you 2. Necessary to comply with our legal obligations 3. Necessary for our legitimate interests (take reasonable steps to ensure a safe and Trusting Environment, confirm that you do not use any ways to manipulate the Website, provision of administration and IT services, network security, to prevent fraud)
f.	1. To provide you with relevant Website content and advertisements, gauging the effectiveness of the served advertising. 2. To optimize the operation of the Website, monitoring user behavior to enhance the efficiency and usability of our services. 3. To enhance the customer experience, offering the best possible service.	1. Identity Data 2. Contact Data 3. Profile Data 4. Usage Data 5. Technical Data 6. Marketing and Communication Data	1. Necessary to perform our contract with you 2. Necessary for our legitimate interests
g.	1. To study customer usage patterns of our products/services, fostering development, business growth, and informing our marketing strategy.	1. Transaction Data 2. Content Data	1. Necessary for our legitimate interests (including statutory limitations provisions by applicable laws)
h.	1. To notify you about: - New services and/or products we may offer. - New developments and features of existing products/services to enhance your platform experience.	1. Identity Data 2. Profile Data 3. Contact Data 4. Technical Data 5. Usage Data 6. Transaction Data 7. Marketing and Communication Data	1. Necessary to perform our contract with you 2. Necessary for our legitimate interests (to study how customers use our products/services, to develop our products/services and grow our business)

i.	<p>1. To send direct marketing of our services, always within the scope of our legitimate interests.</p> <p>2. To deliver newsletters, push-messages, and calls, keeping you informed about new features, product/service developments, news, and comprehensive service offerings. Please note that we never use your data to promote third-party marketing material.</p>	<p>1. Identity Data</p> <p>2. Profile Data</p> <p>3. Contact Data</p> <p>4. Data that may be provided by you during your activity at the Website.</p> <p>5. Marketing and Communication Data</p>	<p>1. Necessary to perform our contract with you</p> <p>2. Necessary for our legitimate interests (to provide effective and personalized customer services to you and to update you in relation to our services that are available to you).</p>
j.	<p>1. To optimize the operation of the Website, enhancing efficiency and usability.</p> <p>2. To employ analytics tools for tracking Website performance and the marketing sources of our Users, aiming to optimize marketing expenses and provide an enhanced user experience.</p>	<p>1. Location Data</p> <p>2. Technical Data</p> <p>3. Usage Data</p> <p>4. Marketing and Communication Data</p>	<p>1. Necessary to perform our contract with you</p> <p>2. Necessary for our legitimate interests (to provide effective and personalized customer services to you and to update you in relation to our services that are available to you).</p>
k.	<p>1. To enable monitoring and training of our employees for your benefit.</p> <p>2. To safeguard interests in cases of disputes.</p> <p>3. To undertake fraud prevention measures.</p> <p>4. To enhance the quality of services provided to you.</p>	<p>1. Audio Data</p> <p>2. Content Data</p>	<p>1. Necessary to perform our contract with you</p> <p>2. Necessary to comply with our legal obligations</p> <p>3. Necessary for our legitimate interests</p>

If you are currently a Website User and we have a valid reason to engage with you, or if you have provided us with your consent, we will collect and manage your personal information to establish communication with you for support purposes, as well as to send you newsletters, push notifications, and calls to keep you informed about our latest features, updates, events, and the effective delivery of our complete range of services. Additionally, we will employ your data to forward marketing details related to our services, which we think could be of significance to you, through email or alternative means.

The Website is designed for adult users and does not target children. We are vigilant in avoiding the collection of data about minors. Since our services are exclusively available to individuals aged 18 or age of majority as recognized and declared by the laws of your jurisdiction, obtaining your birthdate is crucial for verifying the age of Users. Should we become aware of inadvertently or unintentionally gathering Personal data from someone under the age of 18 or the age of majority, we will promptly delete it. If you suspect that we have unintentionally collected data from or about someone under 18 years old or the age of majority, kindly reach out to us at support@wefi.co.

VI. OPTING OUT

If you wish to discontinue receiving marketing newsletters or sharing your data with third parties for marketing purposes, or if you prefer not to receive update notifications, you can send an email to support@wefi.com using the email address registered and associated with your Account. In your email, kindly request us to refrain from sending such promotional material or sharing your data for marketing purposes. Upon receipt of your email and request, we will ensure that advertising content ceases to be sent to you within 7 (seven) business days.

VII. DISCLOSURE OF DATA

We are committed to upholding confidentiality in matters related to Users and the assessments we gather. Data about you might be revealed under certain circumstances: (i) if there's a legal obligation; (ii) upon your explicit request for transaction processing or other services; (iii) as necessary for the fulfillment of our services within our contractual arrangement; and (iv) to safeguard our legitimate interests, following the guidelines of the PIPEDA and relevant provincial statutes that may change over time.

VIII. DATA RETENTION

We store your data for a duration that is reasonably necessary to fulfill the purposes for which it was gathered, covering the fulfillment of legal, tax, or accounting obligations. In instances where a complaint is received or if there is a reasonable expectation of potential litigation about our association with you, your Personal data may be retained for an extended period.

In assessing the suitable duration for retaining your data, we evaluate factors including the quantity, type, and sensitivity of the data, the potential risks associated with unauthorized access or disclosure of the data, the objectives for processing the data, the feasibility of accomplishing those objectives through alternative methods, and the relevant legal, regulatory, tax, accounting, and other obligations.

We will retain your information for as long as is necessary (but not less than 5 years) to provide you with the services that you have requested from us or for as long as we reasonably require to retain the information for our lawful business purposes (such as to exercise our legal rights), or for as long as the law otherwise permits.

At the expiration of the data retention period, the data is erased by irreversible destruction, and we also inform all third parties, to whom the data was transferred, regarding such erasure and request the implementation of similar actions on their part.

IX. YOUR RIGHTS AND HOW TO WITHDRAW CONSENTS AND UNSUBSCRIBE

Identity Accuracy: We urge you to furnish us with accurate, up-to-date, and complete information about your identity. If there are any changes in your identification details, it's imperative to inform the Company within 7 calendar days of the occurrence of such changes. If you believe any of your data with us is inaccurate or incomplete, please reach out to our support

team at the contact details provided below.

Under the PIPEDA and relevant provincial statutes, you possess certain rights concerning your data. These rights can be intricate, and there might be exceptions. We recommend reaching out to us or relevant regulatory bodies for a comprehensive understanding of these rights. A brief overview of your rights includes:

A. Right to Access: You can request confirmation regarding whether we are processing your data. Additionally, you can request more specifics about the data we hold and our processing activities. You may also be entitled to receive a copy of this data.

B. Right to Rectification: If your data is incorrect or incomplete, you have the right to request its correction or completion.

C. Right to Erasure: You can ask us to delete your data if there's no valid reason for its continued processing. If you wish to delete your account and associated data, contact us using the details in the Contact Section below. However, there might be legal reasons preventing us from immediately erasing your data.

D. The right to restrict processing. You have the right to request the restriction of processing of your Personal data under the following circumstances:

(a) If the data is inaccurate.

(b) If the processing may be unlawful, but you wish to avoid data erasure.

(c) If you require us to retain the data even when it is no longer needed.

(d) If you've objected to our data usage, and we need to verify if there are overriding legitimate reasons to continue.

E. Right to Data Transferability: If our processing of your data is based on your consent and is done through automated methods, you're entitled to receive your data in a structured, widely recognized, and machine-readable format. This right might not be applicable if it negatively impacts the rights and freedoms of others or if it's technically infeasible.

F. The right to object. Depending on the legal foundation of the data processing, you have the right to object to the processing of your Personal data. It's important to note that there might be situations where our legitimate reasons for processing might necessitate continued processing despite your objection.

G. The right to withdraw consent. If our data processing activities are based on your consent, you have the authority to revoke that consent at any given time. This could be relevant for marketing activities or when sharing your data with third parties. If you decide to revoke your consent, we will cease to process your data, unless there's a legal or regulatory reason that mandates continued processing. Revoking your consent won't impact the legality of any processing that occurred prior to the revocation.

H. The right to complain to the data protection supervisory authority. We prioritize the protection of your data and strive to keep you informed about our processing activities. If you feel that our processing or protection of your data is inadequate, or if you have concerns about the information we've provided, we encourage you to reach out to us. We value your feedback as it helps us enhance our practices. If you wish to exercise any of your rights, please contact us.

To address your concerns or exercise your rights, please get in touch using the contact details provided in the Contact section below. When reaching out, please provide pertinent details, such as your full name and email address, to help us identify you. We aim to respond promptly to all inquiries.

For security reasons, we might request additional information to verify your identity and ensure that Personal data isn't disclosed to unauthorized individuals. We might also seek more details about your request to expedite our response.

While we strive to address all legitimate requests within a month, there are instances where it might take longer, especially if the request is intricate or if there are multiple requests. Should this happen, we'll keep you informed about the progress.

Please note that for requests deemed excessive or unreasonable, we might impose a nominal administrative fee. This also applies if you request additional copies of your data.

X. DATA SECURITY AND USAGE

Security Protocols: We've implemented strict security measures to safeguard your data against accidental loss, unauthorized access, modification, or disclosure. Moreover, access to your data is restricted. Only our employees, agents, contractors, and specific third parties with legitimate business requirements are granted access. They process your data strictly based on our instructions and are bound by confidentiality obligations.

Handling Data Breaches: In the unfortunate event of a suspected data breach, we have established procedures to address and manage such incidents. We are committed to notifying you and the appropriate regulatory body, in line with legal requirements.

Account Security Measures: Upon registering on our Website, you will be prompted to choose a unique username and password. It's crucial to understand that we will never solicit your password. Sharing your registration details, especially in public forums, is discouraged. We cannot be held accountable for unauthorized or improper use of your account details, especially if shared. If you ever suspect unauthorized access to your account, it's imperative to alert our support team immediately.

Infrastructure Security: Our commitment to your data's security is unwavering. All equipment dedicated to data processing is housed within secure data centers, ensuring optimal protection. We employ advanced network segmentation techniques and ensure that employee access to data is granted strictly based on role-specific requirements.

Threat Management: We are proactive in identifying and mitigating modern threats to data

security. Continuous monitoring, analysis, and response mechanisms are in place to ensure your data's protection against threats, vulnerabilities, and malware.

Data Recovery: In case of any disruptions affecting data accessibility, we have backup and recovery solutions ready to restore your data promptly. Critical databases operate in high availability mode to minimize potential downtimes.

Employee Training: We prioritize the security and confidentiality of your data. To ensure this, we closely monitor all actions of our employees who have access to your data within our systems. Access permissions are granted strictly based on a "need to know" principle. We conduct regular training sessions to ensure every employee is well-versed in our data security principles and practices.

Consequences of Not Providing Data: If you choose not to provide certain data, it might hinder our ability to fulfill our contractual obligations to you. This could lead to the cancellation of services you've availed from us. The data we have about you must remain accurate and up to date. Please inform us of any changes during your association with us.

Automated Decision-making and Profiling: We generally don't employ automated decision making in our business relationships. If we do, you'll be informed separately. We might use profiling to evaluate certain personal aspects, and you'll be informed if we do so. Optional data collection will always be indicated.

XI. OUR CONTACT DETAILS

Entity Responsible for Data Processing: The organization responsible for the processing of your data is Wefi. For any inquiries or communication, you can reach out to us at:

Wefi Payments Limited:

Address: Suite 2700, 225 - 6th, Avenue SW, T2P1N2, Calgary, Alberta, Canada.

Email: support@wefi.co

Data Protection Officer (hereinafter referred to as "DPO"): We have appointed a DPO who is tasked with overseeing matters related to this Privacy Policy. If you have specific questions or concerns about this policy or any data-related issues, you can contact our DPO at:

Wefi Payments Limited:

Address: Suite 2700, 225 - 6th, Avenue SW, T2P1N2, Calgary, Alberta, Canada.

Email: support@wefi.co

For us to efficiently process your requests, please ensure you contact us using the email address you have registered with us. We may also ask you to provide a valid form of identification to ensure the protection of the data we hold and to comply with our security obligations.

If you have any further questions or require more details about how we handle your data, feel free to contact us using the aforementioned details.

XII. LINKS TO EXTERNAL WEBSITES

Our Website may contain links that redirect to third-party websites. These external websites are not under our direct control. As such, we cannot assume responsibility or liability for the actions or policies of these third-party Websites, especially concerning data collection or disclosure. Before providing your data on any external website, it's essential to review their terms and conditions, and privacy policies.

XIII. UPDATES TO THIS PRIVACY POLICY

The most recent update to this Privacy Policy was on 3 September 2025. We hold the right to periodically make changes to this policy to ensure it accurately reflects our data collection and processing practices.

Should there be any updates, we will promptly publish the revised Privacy Policy on our Website. These changes will become effective immediately upon their posting on our site. This policy might also be supplemented by additional information from other relevant Terms and Conditions that pertain to the Website or your interactions with us.

For any feedback, comments, or inquiries, you may contact us using the contact details provided in the Contact section above.