

Privacy Policy

1. Simplified Summary of Key Points

Important Notice: This summary is intended to facilitate an understanding of the key provisions of this Privacy Policy. It does not constitute a separate contractual or legal instrument and does not replace the full text of this Privacy Policy. In the event of any discrepancy or conflict between this summary and any provision of this Privacy Policy, the full text of this Privacy Policy shall always prevail.

- The Application does not require you to use your real name or personal photograph to create an account. The pseudonym and avatar you select constitute the primary means by which you are presented to other users, subject to the Application's design and privacy settings.
- Account registration data, including your email address or other authentication methods, is used to manage your account, verify your identity, secure the Service, and perform related functions. Such data is not made visible to other users in the ordinary course of using the Application.
- Your full date of birth is not displayed to other users. Instead, a general age range or other general information determined by the Application's design may be displayed.
- The Application is designed to limit the retention of message content to the extent reasonably practicable, while taking into account circumstances that may require such content to be retained for longer periods for legal, security, technical, or operational reasons, as further described in this Privacy Policy.
- The Company may retain certain security or technical data, as well as moderation and reporting records, for longer periods than other types of data where necessary to protect the Application, prevent misuse or abuse, comply with legal obligations, or protect legitimate rights and interests.
- The Company may rely on service providers or technology partners to operate, develop, or protect the Application. Data may be processed or stored in different jurisdictions, subject to the implementation of appropriate measures to protect such data in accordance with Applicable Laws.
- Applicable Laws may grant you certain rights in relation to your Personal Data, including rights of access, rectification, deletion, and other rights. Such rights shall be exercised in accordance with the procedures, requirements, limitations, and exceptions set forth in this Privacy Policy and to the extent permitted or required by Applicable Laws.
- The Application is not intended for persons below the minimum age permitted to use the Application under the Terms of Use or Applicable Laws. If the Company determines that an account or data has been created or provided in violation of such requirements, the Company may take appropriate measures, including suspending or deleting the account or deleting the data associated with it, in accordance with this Privacy Policy and the Terms of Use.

By using the Application or continuing to use it, you acknowledge that you have read and understood this Privacy Policy and consent to the processing of your data in the manner and for the purposes described herein, to the extent permitted by Applicable Laws.

2. Introduction, Scope, and Relationship with the Terms of Use

2.1 Welcome and Nature of this Document

This document (the “Privacy Policy” or “Policy”) explains how Sigmarket Trading and Design llc (the “Company,” “we,” “us,” or “our”), in its capacity as the data controller or the entity responsible for processing data, as applicable, collects your Personal Data, technical data, operational data, and derived data associated with your use of the WellChat application (the “WellChat” or the “Application”), your creation of an account, or your use of any of its services or features. It further explains how such data is used, processed, stored, protected, disclosed, retained, or deleted, as well as the rights you may have under Applicable Laws and the mechanisms for exercising such rights.

This Policy shall be read together with all other legal documents governing the use of the Application, including the Terms of Use, and any additional policies, notices, consents, or terms that may be published or adopted from time to time. Each such document shall be deemed complementary to the others and shall be interpreted in a manner that gives effect to their common purpose.

Unless the context otherwise requires, references to “Data” shall include all Personal Data and non-personal data, technical data, statistical data, derived data, and anonymized or pseudonymized data, to the extent permitted by law.

2.2 Relationship with the Terms of Use

This Policy forms an integral and inseparable part of the WellChat Terms of Use. Your acceptance of the Terms of Use, creation of an account, or continued use of the Application or any of its services shall constitute your express consent to this Policy and to all processing activities described herein, to the extent permitted by Applicable Laws.

In the event of any conflict between this Policy and the Terms of Use with respect to any matter relating to the processing of Personal Data, the provisions of this Policy shall prevail solely to the extent of such conflict, while all other provisions of the Terms of Use shall remain in full force and effect and shall continue to be binding.

2.3 Scope of Application

This Policy applies to all persons who use or interact with the Application in any manner, whether they are registered or unregistered users, subscribers to free or paid services, applicants seeking to create an account, persons communicating with the support team, persons submitting reports, or beneficiaries or users of any service or feature provided by the Application, to the extent applicable to the nature of their use.

This Policy also applies to all processing activities carried out by the Company or by any of its service providers or contractors who process Data on its behalf in accordance with this Policy or pursuant to instructions issued by the Company.

Differences in nationality, place of residence, location from which the Application is used, or any other personal circumstance shall not affect the applicability of this Policy, except to the extent that Applicable Laws require otherwise.

2.4 General Principles of Data Processing

In processing Data, the Company adheres to the principles it considers appropriate for providing the Service in a secure and effective manner and in accordance with Applicable Laws, including, without limitation, the following:

Collection of Data that the Company reasonably considers necessary to provide, develop, or secure the Service, or to fulfill its legal or contractual obligations.

Processing of Data for the purposes described in this Policy, or for any purposes that are compatible with, related to, or otherwise permitted by law.

Implementation of appropriate organizational and technical measures to protect Data in a manner proportionate to its nature and the level of risk associated with it.

Retention of Data for no longer than the Company considers necessary to achieve the purposes of processing, comply with legal obligations, or protect legitimate rights and interests, in accordance with the provisions of this Policy.

Periodic review of processing methods and security measures in a manner appropriate to technological and regulatory developments.

Nothing in these principles shall be construed as restricting the Company's right to carry out any other processing that is permitted by law or that is required or reasonably necessary by the nature, security, or operation of the Service.

2.5 Updates to this Policy

The Company may amend, replace, update, or supplement this Policy at any time, including as a result of the development of the Application, the introduction of new services or features, engagement of new service providers, compliance with legal or regulatory requirements, or the improvement of protection or operational standards.

The updated version shall become effective as of the date specified by the Company. The Company may notify users of such updates through any means it deems appropriate, including within the Application, by email, through notifications, or by publishing the updated version within the Application or on the Website.

Your continued use of the Application after any amendments become effective shall constitute your acceptance of such amendments, to the extent permitted by Applicable Laws, without prejudice to any rights or additional consents that the law may require to be obtained in particular circumstances.

3. Definitions

For the purposes of this Policy, and in addition to the definitions set forth in the Terms of Use, which shall be read together with this Policy, the following terms shall have the meanings assigned to them below:

- **Personal Data:** Any data relating to an identified or identifiable natural person, whether directly or indirectly, by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to that person's physical, physiological, genetic, psychological, economic, cultural, or social identity.
- **Processing:** Any operation or set of operations performed on Personal Data, whether by automated means or otherwise, including collection, recording, organization, storage, alteration, retrieval, use, disclosure, transfer, or deletion.
- **Data Controller:** The entity that determines the purposes and means of the Processing of Personal Data, which, for the purposes of this Policy, is the Company.
- **Processor:** Any party that Processes Personal Data on behalf of the Data Controller and in accordance with its instructions, including cloud infrastructure providers and payment service providers.
- **Pseudonymization / Hashing:** A Processing operation that transforms Personal Data so that it can no longer be attributed to a particular person without the use of additional information that is kept separately and securely, such as a one-way hash function. Data pseudonymized or hashed in this manner remains Personal Data for legal purposes and shall not be considered fully anonymized data.
- **Full Anonymization / De-identification:** A Processing operation that removes from Data all elements that could link it to a particular person in an irreversible manner, such that the Data cannot reasonably be re-linked to that person by any reasonably available means. Only upon achieving such a state shall the Data fall outside the definition of "Personal Data."
- **Special Category Data / Sensitive Data:** A special category of Personal Data subject to heightened protection or sensitivity under Applicable Laws, including, for example, racial or

ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning a person's sex life or sexual orientation.

- **Device Fingerprint:** Any unique identifier generated from characteristics of your device, including device type, operating system, Application version, or other technical characteristics, for the purposes of recognizing or distinguishing the device over time without relying on a direct personal identifier.
- **Cross-Border Transfer:** The transfer of Personal Data from one country to another, whether by directly storing such Data on servers located in another country or by enabling access to such Data from that country.
- **Competent Supervisory Authority:** The governmental or quasi-governmental authority legally authorized to supervise or monitor compliance with data protection laws in a particular jurisdiction.

4. Data Controller Identity

The entity responsible for controlling your Personal Data is Sigmarket Trading and Design LLC, officially registered under Commercial Registration No. 189962 in the State of Qatar, with its registered office in Doha, Qatar. This means that the Company is the entity that determines the purposes for which your Data is Processed and the means by which such Processing is carried out, and is legally responsible for compliance with this Policy and Applicable Laws.

5. Categories of Personal Data We Collect

Depending on the nature of the Service you use, the method by which you create your account, the features you activate, and the technical means used to provide, develop, or protect the Service, the Company may collect, Process, store, and use Personal Data, technical data, operational data, and derived data relating to you, whether collected directly from you, from your device, from authentication service providers, from infrastructure providers, or generated as a result of your use of the Application.

The Data we may collect includes, without limitation, the following:

5.1 Registration and Account Data

When you create an account, we may collect the following Data depending on the registration method you choose:

- Your email address when registering by email, which may be used for identity verification, account management and recovery, sending security and administrative notifications, and other operational purposes related to the Service.
- When registering through third-party authentication services (such as Apple or Google, or any other provider supported in the future), we may receive identifiers, authentication tokens, verification data, or identification information provided by the relevant service provider to authenticate your identity, without accessing your password for your account with that provider.
- An encrypted or hashed copy, or any other technically derived representation of identification data, used to detect duplicate accounts, prevent misuse or abuse, perform security verification, and prevent circumvention of security and protection systems.
- Internal account identifiers.
- Timestamps relating to account creation, the most recent login, the most recent activity, and records of certain essential account-related operations.
- Any additional verification data that may become necessary in the future for compliance purposes, platform protection, or fraud prevention.

5.2 Profile Data

We may collect the Data you choose to add to your profile, including, without limitation:

- Pseudonym.
- Date of birth or Data necessary to verify your age category.
- Calculated age range.
- Gender.
- Country of residence.
- Languages.
- Interests.
- Avatar, profile image, or similar identifying elements.
- Privacy settings and preferences.
- Any additional Data you choose to provide as part of your profile or that the Company may introduce in the future as part of the Service's features.

Some of this Data may be displayed to other users depending on the Service's settings, while other Data may remain internal and not be visible to users.

You acknowledge that certain essential Data, including your date of birth, may become non-editable once it has been verified or otherwise established, whether for security, regulatory, or operational reasons, and the Company may implement any technical mechanism it considers appropriate to achieve this purpose.

5.3 Communications Content

We may Process messages, textual content, and any media or Data exchanged through the Application to the extent necessary to provide and secure the Service, detect misuse or abuse, enforce the Terms of Use, and comply with legal obligations.

The Service is designed so that the retention of message content is limited in duration to the extent reasonably practicable, while taking into account circumstances that may require such content to be retained for longer periods, including reports, investigations, disputes, compliance with Applicable Laws, or the protection of the rights of the Company, users, or third parties.

5.4 Device and Technical Data

We may automatically collect technical Data associated with your devices and connection, including, without limitation:

- Device fingerprint or any similar technical identifier.
- Various device identifiers.
- Device type.
- Operating system and version.
- Application version.
- Internet Protocol (IP) address.
- Network Data.
- Performance Data.
- Crash logs.
- Diagnostic Data.
- Notification tokens.
- Service connection information.
- Any other technical Data reasonably necessary to operate, develop, or secure the Application.

5.5 Usage Data and Analytics

We may collect information regarding how you use the Application, including operational events, feature usage history, interactions, usage patterns, statistical measurements, analytical data, and derived data, for

purposes including improving the Service, developing features, analyzing performance, detecting malfunctions, measuring service quality, and preventing misuse or abuse.

Such Data may be Processed on an individual, aggregated, anonymized, or pseudonymized basis, depending on the nature of the purpose for which it is Processed.

5.6 Payment and Subscription Data

When you subscribe to paid services, we may receive from payment providers or app stores the Data necessary to manage your subscription, including its status, type, duration, platform, and identifiers necessary to verify the validity of the subscription, without receiving full payment card details unless such receipt forms part of a future service expressly introduced by the Company.

5.7 Support and Reporting Data

We may collect any information you provide when contacting technical support, submitting reports, requesting assistance, or participating in investigations relating to violations of the Terms of Use, including the contents of the report, attachments, timestamps, and technical identifiers associated with the report.

Such Data may be retained for longer periods than those applicable to other operational Data where necessary to protect the platform or users or to establish, exercise, or defend the Company's legal rights.

5.8 Communication Data and Preferences

We may record your preferences regarding the receipt of notifications, administrative messages, marketing communications, and engagement or promotional notifications, as well as your interactions with such communications, for the purposes of managing your preferences and improving the effectiveness of our communication methods.

5.9 Other Data

The Company may collect, create, derive, infer, or otherwise Process any other Data that is related to your use of the Service or reasonably necessary to operate, develop, or secure the Application, prevent fraud, verify identity, comply with Applicable Laws, enforce the Terms of Use, or protect the rights of the Company, users, or third parties, including derived data, statistical data, analytical data, technical data, operational data, and any new categories of Data that may become necessary as a result of future regulatory requirements or technological developments, to the extent permitted by Applicable Laws.

6. How We Collect Your Data

We may collect your Personal Data or other Data associated with your use of the Application from multiple sources, depending on the nature of your use of the Service, including, without limitation, the following:

6.1 Data You Provide Directly

We collect the Data that you choose or are required to provide when creating an account, using the Application, or communicating with us, including, without limitation:

- Registration and account creation Data.
- Profile Data.
- Data that you add or modify within the Application.
- Messages and content that you choose to share through the Application.
- Reports, complaints, and feedback that you submit.
- Technical support requests, inquiries, or correspondence.
- Responses to surveys, forms, or requests for communication.
- Any other information that you decide to provide to us while using the Service.

The provision of certain Data is optional, while other Data may be necessary to create an account, provide the Service, or perform the Terms of Use.

6.2 Data Collected Automatically

When you use the Application, we may automatically collect technical, operational, and analytical Data generated through your use of the Service, whether through the Application itself, operating systems, devices, analytics tools, infrastructure providers, or other technical means.

Such Data may include, without limitation:

- Device Data.
- Network connection Data.
- Device fingerprints and technical identifiers.
- Usage logs.
- Performance Data.
- Crash Data.
- Session Data.
- Operational events.
- Data relating to interactions with Application features.
- Statistical and analytical Data.
- Data derived from usage patterns.

Such Data may be collected automatically whenever you use the Application or interact with any of its services or features.

6.3 Data Received from Third Parties

We may receive Data about you from third parties where reasonably necessary to provide the Service, enforce or perform the Terms of Use, or fulfill our legal or security obligations.

Such third parties may include, without limitation:

- Login and authentication service providers.
- App stores.
- Payment service providers.
- Analytics service providers.
- Fraud prevention and risk management service providers.
- Notification service providers.
- Infrastructure and hosting service providers.
- Competent governmental, judicial, or regulatory authorities where required by law.
- Any other service provider or technology partner relied upon by the Company to provide, develop, or secure the Service.

We receive from such parties only the Data that is reasonably necessary to achieve the purpose for which it was collected, or that we are otherwise permitted by law to receive and Process.

7. Legal Bases for Processing

The Company Processes Personal Data on the basis of one or more legal bases recognized under Applicable Laws and regulations. A single Processing activity may rely on more than one legal basis simultaneously where legally permitted.

Such legal bases may include, without limitation, the following:

Legal Basis	Examples of Processing Purposes
-------------	---------------------------------

Performance of a Contract	Creating an account, providing the Service, operating the Application, matching users, exchanging messages, managing subscriptions, performing the Terms of Use, providing technical support, and processing account-related requests.
Legitimate Interests of the Company or Third Parties	Protecting the platform, preventing fraud, detecting unlawful activities, managing reports, enforcing the Terms of Use, developing services, improving performance, conducting analytics, measuring service quality, information security, protecting the rights of the Company, users, or third parties, risk management, and conducting audits and internal investigations.
Your Consent	Sending marketing communications or notifications, using Data in circumstances where the law requires your consent, or carrying out any other Processing to which you expressly consent. You may withdraw your consent where legally available to you, without affecting the lawfulness of Processing carried out before such withdrawal.
Legal Obligation	Complying with Applicable Laws and regulations, complying with orders or requests from competent authorities, maintaining legally required records, preventing money laundering or fraud, and fulfilling any other regulatory requirements where applicable.
Vital Interests	Protecting the safety or life of a user or any other person in emergency situations or where there is a serious and imminent risk, to the extent permitted by law.
Public Interest or Exercise of Official Authority	Where required or permitted under Applicable Laws, regulations, or decisions issued by competent authorities.

The examples set out above shall not be construed as an exhaustive list of all circumstances in which Processing may occur. The Company may rely on any other legal basis recognized under Applicable Laws, or change the legal basis relied upon for a particular Processing activity where such change is lawful, without affecting the lawfulness of Processing carried out prior to such change.

8. Purposes of Data Processing

The Company Processes user Data to the extent necessary to operate, provide, maintain, develop, and continuously improve the Service, in accordance with the nature of the platform and its current and future features, and in compliance with Applicable Laws and general privacy principles.

The Company Processes Personal Data, technical Data, derived Data, and aggregated Data to the extent necessary and appropriate to operate, provide, maintain, secure, develop, improve, and personalize the Service, in accordance with the nature and characteristics of the platform, its current and future features, and to the extent permitted by Applicable Laws and regulations.

The purposes of Processing include, without limitation or restriction, the following:

8.1 Operation and Administration of the Service

This includes all Processing activities necessary to create and manage accounts, verify identity, enable login and authentication, and operate the Application's core functions, including search, matching, communication between users, management of settings, service levels, subscriptions, permissions, and account- or usage-related limitations.

8.2 Safety, Security, and Prevention of Misuse

Data may be Processed for purposes of protecting users and the security and integrity of the platform, including detecting unlawful, fraudulent, abusive, or otherwise prohibited activities; preventing misuse or abuse; investigating reports; enforcing security policies; and taking preventive or corrective measures, including the use of behavioral, technical, or automated analytical tools where necessary.

8.3 Communications and User Relationship Management

Data may be used to communicate with users regarding the Service or their accounts, including operational communications, verification and security messages, system notifications, technical updates, subscription management, technical support, and other administrative communications relating to the use of the Service.

Where permitted by Applicable Laws or the user's settings, the Company may also send marketing, promotional, informational, re-engagement, or similar communications.

8.4 Analytics, Service Improvement, and Development

Data may be used, whether individually, in aggregated form, in anonymized form, or in derived form, for purposes of analysis and statistical evaluation, understanding usage patterns, improving performance and stability, developing current and future features, improving search, matching, and recommendation systems, determining development priorities, and evaluating the user experience.

This may also include training, improving, testing, or operating algorithms and computational or statistical models, machine-learning models, or any current or future analytical or intelligent technologies.

8.5 Personalization and Advertising (Current or Future)

Data may be used to personalize the user experience within the Service, including ranking content, improving search results, and suggesting relevant matches, content, features, or experiences.

Data may also be used to provide, improve, measure, or manage promotional or advertising content within or outside the Service, including personalized or non-personalized advertising, in accordance with Applicable Laws, user settings, and any applicable rights to control or object to such Processing.

8.6 Subscriptions, Payments, and Billing Management

Data may be Processed to manage subscriptions and paid services, verify payment status, integrate with payment service providers or app stores, process billing, refunds, and renewals, and resolve related disputes or financial issues, where applicable.

8.7 Legal Compliance and Protection of Rights

Data may be Processed where necessary to comply with legal, regulatory, or judicial obligations; respond to official requests from competent authorities; enforce the Terms of Use; protect the rights of the Company, users, or third parties; or investigate, prevent, or manage disputes, including retaining or disclosing Data to the extent permitted or required by law.

8.8 Continuous Development and Evolution of Use

The purposes for which Data is Processed may change or expand as the Service evolves or as new features, technologies, products, or business models are introduced, including, without limitation, advanced analytics, personalization, advertising, recommendation systems, artificial intelligence, machine learning, or any similar current or future technologies.

Any such Processing shall remain within the limits permitted by Applicable Laws and shall be carried out consistently with the fundamental principles of this Policy, users' rights, and the Company's legal and regulatory obligations.

9. Sensitive Data and Information Shared by Users

The Service does not require users, as part of account creation or ordinary use of the Service, to provide us with Sensitive Personal Data or other Personal Data subject to heightened protection under Applicable Laws. Such Data is also not required for registration and does not constitute a core element of the user profile.

Certain information, preferences, or interests that a user voluntarily chooses to add to their profile or share while using the Service may contain indicators from which information of a personal or sensitive nature could be indirectly inferred. Providing or sharing such information is entirely voluntary and is based on the user's own decision and responsibility. We may Process such information to the extent necessary to provide the Service, operate its features, or improve the user experience, in accordance with this Policy.

A user may also voluntarily choose to share Personal Data or Sensitive Personal Data with other users through content they publish, messages, or any other means of communication within the Service. In such circumstances, the user is responsible for their decision to disclose such information, and the Company shall not be responsible for any use, republication, redistribution, or misuse of such information by persons with whom the user has chosen to share it, to the extent permitted by law.

We advise users not to share any sensitive, confidential, financial, or other information that they do not wish to disclose to others, unless they fully understand the nature of such disclosure and its potential consequences.

10. Minors' Data and Age Verification

Please read this section together with the "Age Eligibility" section of the Terms of Use, which sets out the requirements and eligibility conditions for using the Service.

The Service is intended solely for persons who meet the minimum age requirement specified in the Terms of Use. A user's age is determined based on the information provided by the user when creating an account, as the nature of the Service does not permit the independent or continuous verification of the actual age of every user. The user remains responsible for the accuracy of the information provided and for their representations concerning their age.

As part of our commitment to enhancing user safety, particularly in light of the nature of the Service, which facilitates communication through pseudonyms, we implement operational measures intended to limit interactions between users who represent themselves as belonging to younger age groups and adult users. Such measures may include segregating users into designated age categories for purposes of search, matching, or other Service functions, depending on the design of the Service.

These measures constitute reasonable preventive measures intended to reduce risks and do not constitute a guarantee that violations, misuse, abuse, or circumvention through the provision of inaccurate information will not occur.

If we determine, or have reasonable grounds to believe, that a user does not meet the minimum age requirement or has provided inaccurate age information, we may take any action we deem appropriate, including requesting additional information, restricting the account, suspending it, terminating it, or deleting the Data associated with it, or retaining such Data as may be necessary where required or permitted by law or for security or regulatory purposes.

We also treat reports concerning the safety of minors, or suspected exploitation, harassment, or any conduct that may place minors at risk, as matters of high priority. We may take appropriate measures to protect users, including suspending or restricting accounts and cooperating with competent authorities where required by law.

If you believe that a person who does not meet the minimum age requirement has used the Service or provided us with their Personal Data, you may contact us through the contact methods specified in this

Policy. We will handle the report in accordance with our internal procedures, while retaining the right to request information necessary to verify the validity of the report before taking any action.

The implementation of the measures described in this section shall not constitute an acknowledgment or guarantee that the actual age of all users can be verified or that all instances of misuse, abuse, or circumvention can be prevented. Rather, such measures represent the reasonable measures we adopt to assist in protecting users and complying with applicable legal and regulatory requirements, taking into account the nature of the Service and the technical means available to us.

11. Automated Decision-Making and Algorithmic Systems

11.1 Algorithmic Systems for Search and Matching

The Company may use automated, semi-automated, or hybrid systems, including algorithms, statistical models, artificial intelligence or machine-learning technologies, and any similar current or future technological means, for purposes of operating the Application, improving the user experience, providing search and matching results, and managing certain functions of the Service.

Depending on the nature of the Service and the settings applicable from time to time, such systems may take into account one or more relevant factors, Data points, or indicators, including, without limitation, language, interests, age range, country of residence, gender, activity level, usage patterns, compatibility between users' preferences, and any other operational criteria that the Company considers appropriate for achieving the purposes of the Service.

The results generated by such systems are used as operational indicators intended to improve the ranking of search results, suggest users, or manage certain Application features. They do not constitute a guarantee, undertaking, or representation that any actual compatibility exists or that any communication or relationship between users will be successful, nor do they, by themselves, create any right or legal status for the user.

The Company retains full discretion to modify, develop, replace, or discontinue such systems, or any of their criteria, weighting, methodologies, or outputs, at any time and without any obligation to disclose their technical details, internal logic, or operational criteria, where the Company considers such action necessary to protect the security of the Application, prevent misuse or abuse, develop or improve the Application or its performance, or comply with legal or regulatory requirements.

11.2 Automated Systems for Detecting Violations

The Company may use automated or semi-automated systems and technologies to monitor, detect, assess, or limit activities, behavior, or content that may constitute a violation of the Terms of Use or Applicable Laws, or that may threaten the security of the Application or its users.

Such systems may rely on operational rules, technical indicators, behavioral patterns, statistical models, artificial intelligence, machine learning, or any other technological means that the Company considers appropriate.

The detection of a potential violation may result in automated operational or preventive measures, including rejecting a particular action or transaction, restricting certain functions, requiring additional verification, or taking any other temporary measure that the Company considers appropriate to protect the platform or its users. Such action shall not, in itself, be deemed a final decision or a decision having a material legal effect, unless Applicable Laws provide otherwise.

11.3 Automated Assessment of Reports and Moderation Procedures

The Company may use automated or semi-automated systems to assess incoming reports, prioritize them, estimate their level of severity, and support moderation and enforcement processes, based on a range of operational and security indicators and criteria determined by the Company from time to time.

Such systems may take into account, without limitation, the nature of the report, the history of relevant accounts, the frequency of violations, their severity, behavioral patterns, the reliability of previous reports,

and any other factors or indicators that the Company considers necessary to protect the safety of the platform or its users.

Where the Company considers a matter to involve heightened risks, threaten user safety or Application security, or require urgent action, automated or immediate measures may be taken, including temporarily suspending certain features, temporarily suspending an account, or imposing appropriate operational restrictions, before human review is conducted where the Company considers the nature of the circumstances to warrant such action.

At its sole discretion, the Company may subject any matter to human review before a decision is made, after a decision has been made, or while a decision is being implemented. The Company may also refrain from conducting human review where the law does not require it and the nature of the action or alleged violation does not warrant such review.

Where made available by the Company or required by law, a user may request a review of a decision in accordance with the mechanism set forth in the Terms of Use. The Company undertakes to consider such request in accordance with its internal procedures and in such manner as it considers appropriate. The submission or acceptance of a review request shall not, by itself, require the Company to cancel or modify the decision, compensate the user, or suspend the effects of the decision pending completion of the review, unless the Company determines otherwise or Applicable Laws require otherwise.

11.4 No Automated Profiling for Individualized Pricing Purposes

As of the date of issuance of this Policy, the Company does not use automated profiling systems intended to determine subscription prices or fees for services on the basis of an individual user's profile, behavior, or Personal Data.

Subscription and service prices are determined in accordance with the Company's applicable commercial policies, or those of app stores or payment service providers, or based on the applicable country, currency, pricing category, or other general commercial factors that do not rely on personalized profiling of the user.

Nothing in the foregoing prevents the Company from using analytics, statistical Data, aggregated or anonymized information, or other lawful analytical means to develop or improve its services, evaluate their performance, or design future commercial offerings, in accordance with this Policy and Applicable Laws.

12. Data Sharing and Disclosure

12.1 Sharing Data with Service Providers and Contractors

The Company may share Personal Data, technical Data, or operational Data with service providers, affiliates, contractors, or professional partners upon whom it relies to operate, develop, maintain, secure, or provide the Application and its Services, to the extent necessary to achieve the lawful purposes described in this Policy or the Terms of Use.

Such parties may include, without limitation:

- Cloud computing, hosting, and data center providers.
- Database, infrastructure, network, and backend service providers.
- Authentication, identity management, and user verification service providers.
- Notification, messaging, and communications service providers.
- Payment, billing, and subscription management service providers.
- App stores and application distribution platforms.
- Analytics, statistics, and performance measurement service providers.
- Cybersecurity, risk management, fraud prevention, and abuse prevention service providers.
- Device identification, technical identifier management, and detection of unauthorized or illegitimate accounts service providers.

- Artificial intelligence, machine learning, automation, and other similar operational technology service providers.
- Crash monitoring and technical diagnostics service providers.
- Services used to verify that a user is a real person.
- Technical support and customer request management service providers.
- Legal advisors, auditors, accountants, insurers, and other professional entities providing services to the Company.
- Any other service provider, contractor, or partner whose involvement is reasonably necessary to operate or develop the Application, comply with Applicable Laws, or protect the rights of the Company or its users.

Such parties may Process Data only to the extent necessary to perform the services for which they have been engaged, or to the extent permitted by the agreements entered into with them or by Applicable Laws, taking into account the nature of the legal relationship between such party and the Company.

12.2 App Stores and Payment Service Providers

When you subscribe to any paid Service, the Company may exchange with app stores, payment service providers, financial institutions, or billing providers the information necessary to verify the subscription, process payments, activate Services, prevent fraud, and fulfill accounting, tax, or regulatory obligations. The Company does not receive or retain full payment instrument information, unless this becomes part of a future Service introduced by the Company and permitted under Applicable Laws.

Payment processing activities carried out by payment service providers or app stores are subject to their respective independent policies and terms with respect to the Data they Process in their own capacity.

12.3 Disclosure to Governmental, Regulatory, and Judicial Authorities

The Company may disclose Personal Data or other relevant information to governmental, regulatory, judicial, security, law enforcement, or other competent authorities, whether inside or outside the applicable jurisdiction, where the Company considers such disclosure to be required or permitted under Applicable Laws, regulations, orders, judgments, or binding requests, or where reasonably necessary to:

- Comply with any legal or regulatory obligation.
- Implement or respond to orders, decisions, or requests issued by competent authorities.
- Protect or defend the rights of the Company, its affiliates, users, employees, or partners.
- Prevent or investigate fraud, abuse, crime, security violations, or any unlawful activity.
- Protect the safety of any person, property, the security of the Application or its users, or the public.
- Establish, exercise, or defend any legal right, claim, or judicial, arbitral, or administrative proceeding.

The Data disclosed shall be limited to what the Company reasonably considers necessary to achieve the relevant purpose or what is required by Applicable Laws or the competent authority.

12.4 Corporate Restructuring and Business Transactions

Personal Data may be transferred, shared, or made available as part of any merger, acquisition, sale, reorganization, restructuring, financing, investment, full or partial sale of assets or business, or any similar transaction involving the Company or its business.

In such circumstances, Data may be transferred to the successor entity, acquirer, investor, or entity resulting from such transaction, provided that its use continues in accordance with this Policy or pursuant to a new privacy policy of which users are notified where required by Applicable Laws.

12.5 Data Visible to Other Users

The Application displays to other users only the Data or information that the Service is designed to make available in accordance with its settings and functions, or that the user chooses to make available through the Application's features.

Depending on the design of the Service and applicable privacy settings, such Data may include a pseudonym, avatar or profile image, general age range, languages, interests, gender, country of residence, online or connection status, matching results or indicators, or other public information made available by the Application.

The Application does not provide other users with access to Data that is not intended for public or user-facing display, such as an email address, full date of birth, internal identifiers, Device Fingerprint, security or technical Data, or any other Data not intended for display, unless the user expressly consents to such access, or Applicable Laws or the nature of the Service require otherwise.

13. Cross-Border Transfers

Your Personal Data may be Processed or stored within or outside the country in which you reside, using service providers or technological infrastructure located in different jurisdictions, depending on operational requirements. In all cases, we seek to implement reasonable technical and organizational measures, consistent with applicable practices and standards, to protect your Data while it is being Processed, transferred, or stored.

14. Data Retention

14.1 Data Retention Principles

The Company retains Personal Data, technical Data, operational Data, and derived Data for the period it reasonably considers necessary to achieve the purposes for which such Data was collected, created, or Processed, or for the period required by Applicable Laws, regulations, regulatory or contractual requirements, or for as long as necessary to protect the legal rights or legitimate interests of the Company, its users, or third parties, whichever is longer.

The Company does not apply a uniform retention period to all categories of Data. Rather, the retention period may vary depending on the nature of the Data, the purpose for which it is Processed, its level of sensitivity, legal and regulatory requirements, security and operational needs, and the potential for disputes, legal claims, investigations, or judicial or regulatory proceedings to arise.

In all cases, the Company may extend any retention period where reasonably necessary, including, without limitation, for purposes of complying with Applicable Laws, establishing, exercising, or defending legal rights, protecting the security of the Application or its users, investigating violations, misuse, or fraud, restoring Data, maintaining the integrity of systems, or complying with orders issued by competent authorities.

The following table sets out the Company's customary operational retention periods for certain categories of Data, subject to the exceptions set out in this Policy or the Terms of Use, or otherwise required by law.

Data Category	Retention Period and Notes
Message Content	The Application is designed so that message content is retained temporarily to the extent practicable. The Company aims to delete messages once their operational purpose has been fulfilled and, as a general maximum, ordinarily no later than 48 hours from the date of sending where the conversation has not been opened or where there is no need to retain the messages for a longer period. This is subject to backups, investigations, reports, legal, security,

	or technical requirements, and any other exception permitted by law or provided for in this Policy or the Terms of Use.
Account and Profile Data	Retained for the duration of the account's active status, and throughout any applicable period of suspension, deactivation, termination, grace period, recovery, or review associated with the account. Thereafter, such Data may be deleted or anonymized in accordance with the Company's customary procedures, unless retention is required or permitted by law or is reasonably necessary for legitimate security, operational, or legal purposes.
Email Address and Associated Identifiers	The email address, or any technically derived representation of it, is retained for as long as necessary to manage the account, verify identity, and prevent misuse. Certain identifiers, hashes, or derived Data may be retained for an additional period where reasonably necessary to prevent fraud, the recreation of violating accounts, or to protect the security of the Application.
Reports, Moderation, and Enforcement Records	Retained for as long as necessary to investigate violations, protect users, enforce the Terms of Use, establish, exercise, or defend legal rights, or comply with legal or regulatory obligations. Such records are subject to periodic review in accordance with the Company's internal policies.
Technical Identifiers and Device Fingerprint	May be retained for as long as necessary for security purposes, prevention of misuse or fraud, prevention of the recreation of violating accounts, or protection of the integrity of the Application. The retention period may vary depending on the nature of the matter and the relevant account history.
Usage and Analytics Data	May be retained for as long as necessary for statistical analysis, service improvement, performance measurement, fault detection, and product development. Thereafter, such Data may be retained in aggregated, anonymized, or otherwise non-directly-identifiable form.
Subscription and Financial Transaction Data	Retained for the period required by applicable accounting, tax, or regulatory laws, by payment service providers or app stores, or pursuant to any other applicable legal obligations.
Technical Support Requests and Correspondence	May be retained for as long as necessary to process requests, improve support quality, verify complaints, establish, exercise, or defend legal rights, and address recurring issues. Thereafter, such Data may be deleted, anonymized, or retained in a form that does not permit direct identification of the user, where appropriate.

14.2 Deletion or Anonymization of Data

Once the legitimate purpose for Processing Data has ended, and there is no legal, regulatory, contractual, security, operational, or judicial requirement or justification for continued retention, the Company may, as it considers appropriate, take one or more of the following actions:

- Delete the Data from operational systems.
- Anonymize the Data so that it is no longer capable of being linked to a specific user.
- Replace the Data with aggregated, pseudonymized, or anonymized Data.
- Retain the Data in archives or backups until the applicable technical retention cycle expires, where immediate deletion is not technically feasible.

Deletion of an account or Data does not necessarily result in the immediate removal of all copies from all systems, backups, audit logs, or technical archives. Certain copies may continue to exist temporarily until applicable backup cycles, restoration requirements, or statutory retention periods expire, provided that such copies are not used for operational purposes in a manner inconsistent with this Policy or Applicable Laws.

15. Data Security Measures

We implement reasonable and appropriate technical, organizational, and administrative measures designed to protect Personal Data against unauthorized access, use, disclosure, alteration, loss, or destruction, taking into account the nature of the Data, potential risks, and available technologies.

Depending on the nature of the Service, such measures may include the use of appropriate safeguards for Data while it is being transferred, Processed, or stored, restricting access to Data to authorized persons whose duties require such access, and implementing controls and procedures designed to protect the security of the Service and reduce the risk of misuse or abuse.

We may also use various security measures and technologies, including systems for detecting misuse or abuse, identity verification mechanisms, measures designed to limit automated or fraudulent activity, and other measures that we consider appropriate to enhance the security of the Service. We may update, replace, or develop such measures at any time without prior notice.

We are committed to applying the principle of data minimization in retention wherever operationally practicable, consistent with the requirements of providing the Service and our legal and security obligations.

Notwithstanding our implementation of reasonable measures to protect Data, no system, network, or electronic means can be guaranteed to be completely secure. Accordingly, to the extent permitted by law, we do not guarantee that the Service will be completely protected against all security risks or incidents.

16. Your Rights Regarding Your Personal Data

Subject to Applicable Laws and the technical design of the Service, you may access, review, and manage most of your Personal Data directly through your account settings. You may update or correct Data that is technically capable of being modified at any time. Certain Data, including age and gender, may not be editable after registration has been completed as part of security measures and procedures designed to maintain the integrity of the Service and verify user eligibility.

You may request the correction of Data that cannot be modified through your account, or request deletion of your account and Personal Data in accordance with this Privacy Policy and the applicable Data retention periods. Where the Processing of certain Data is based on your consent, you may withdraw such consent at any time, without affecting the lawfulness of any Processing carried out before the withdrawal.

For reasons relating to security, privacy protection, and the integrity of the Service, we do not provide downloadable or portable copies of Data that is already made available to you through your account within the Application. We also reserve the right to refuse or restrict any request where fulfilling it is technically infeasible, may adversely affect the rights or privacy of others, may compromise the security

or integrity of the Service, is repetitive or abusive, or where the retention or Processing of certain Data is required or permitted by law.

To exercise any rights available to you, you may contact us through the contact methods specified in this Policy and provide the information reasonably necessary for us to process your request. To protect user accounts, we may require you to verify your identity before fulfilling any request. We will process the request within a reasonable period in accordance with Applicable Laws.

17. Cookies and Technical Tracking Identifiers

The Application may use technologies and technical identifiers that are necessary to operate the Service, improve its performance, and protect users, including identifiers required for account management, Service security, operation of essential features, delivery of notifications, storage of user preferences, analysis of Application performance, and other legitimate operational purposes.

Certain information may be stored locally on your device or Processed through services or technical providers that we use to provide and improve the Service, in accordance with this Policy.

You may control certain permissions and settings, including notification permissions and other permissions that your device's operating system allows you to manage. However, certain identifiers or technical Data may be necessary to operate the Application, protect its security and integrity, or prevent misuse or abuse. Accordingly, it may not be possible to disable or delete such identifiers or Data separately without affecting your ability to use certain Application or Service functions.

We do not use technologies or identifiers for purposes inconsistent with those described in this Privacy Policy. We may update or replace the technologies or technical means we use from time to time in order to operate, develop, or enhance the security of the Service, without affecting the fundamental principles set out in this Policy.

18. Data Breach Notification

We implement reasonable technical and organizational measures designed to protect Personal Data against unauthorized access, use, disclosure, alteration, loss, or destruction. However, no electronic system, transmission method, or storage mechanism can be guaranteed to be completely secure.

If a security incident occurs that may affect Personal Data, we will take such measures as we consider appropriate to contain and investigate the incident and mitigate its effects, and we will address any legal obligations applicable to us, including notifying competent authorities or affected users where required or appropriate under Applicable Laws and having regard to the nature of the incident.

The Service is designed around the principles of data minimization and retaining only the minimum Data reasonably necessary to provide and operate the Service, with the aim of reducing the potential impact of any security incident. However, we do not guarantee that any security incident will not occur, and nothing in this section constitutes a guarantee regarding the scope or categories of Data that may be affected in any particular incident, as this will depend on the nature of the incident and the technical circumstances existing at the time it occurs.

19. Amendments to this Policy

We reserve the right to amend, update, or otherwise modify this Policy at any time, including as a result of developing the Service, adding or modifying its features, changing our Data Processing practices, complying with legal or regulatory requirements, or for any other legitimate reason.

Where material changes are made that affect how your Personal Data is collected, used, or disclosed, we may notify you through the Application, by email, or through any other appropriate means of communication, where such notice is required or appropriate under Applicable Laws or in light of the nature of the change.

Your continued use of the Service after the amendments become effective constitutes acceptance of the updated Policy to the extent permitted by law. Where any amendment requires your express consent under Applicable Laws, such amendment will not apply to you until that consent has been obtained.

The “Last Updated” date of this Policy will be updated when any amended version is published.

20. Contact Information and Final Acknowledgment

20.1 Official Privacy Contact Information

If you have any questions, requests, or comments regarding this Policy, the Processing of your Personal Data, or the exercise of any rights that may be available to you under Applicable Laws, you may contact the Company through the following official channels:

Contact Purpose	Channel
Legal Name of the Company	Sigmarket Trading and Design llc
Registered Address	Doha, Qatar
Personal Data Protection Requests and Exercise of Rights	privacy@wellchatapp.com
Minors’ Safety Complaints	childsafety@wellchatapp.com
Reporting Potential Security Vulnerabilities	security@wellchatapp.com
Intellectual Property Complaints	ip@wellchatapp.com
General Technical Support	support@wellchatapp.com

The Company may update or replace the contact methods listed above from time to time. Publication of updated contact information within the Application, on the website, or through any other official communication channel shall constitute sufficient notice to users of such updated contact information.

20.2 Relationship Between the Privacy Policy and the Terms of Use

This Policy shall be read and interpreted as an integral and inseparable part of the Terms of Use of the “WellChat” Application and, together with the Terms of Use and any additional policies, notices, consents, or terms adopted by the Company, shall collectively constitute the contractual framework governing the relationship between the user and the Company with respect to the use of the Application and the Processing of Personal Data.

In the event of any conflict between the provisions of this Policy and the Terms of Use with respect to the Processing of Personal Data, the provisions of this Policy shall prevail solely to the extent of such conflict, while all other provisions of the Terms of Use shall remain in full force and effect.

20.3 Acknowledgment of Review and Consent

By creating an account, using the Application, or continuing to use any of its Services or features, you acknowledge that you have been provided with a reasonable opportunity to review this Privacy Policy, that you have read it or had the opportunity to do so before using the Service, and that you understand its nature and purpose. You further consent to the collection, use, Processing, disclosure, and retention of your Personal Data as described in this Policy, to the extent permitted by Applicable Laws.

You further acknowledge that your use of the Application is subject to this Policy and the Terms of Use as in effect at the time of your use, and that your continued use of the Application after any updates or amendments become effective in accordance with the mechanism set out in this Policy constitutes your acceptance of such updates or amendments, without prejudice to any additional requirements imposed by law for obtaining renewed or express consent in particular circumstances.

Nothing in this acknowledgment shall operate to deprive you of any rights that cannot lawfully be waived under Applicable Laws, nor shall it be interpreted in a manner inconsistent with any mandatory legal protection afforded to users under such laws.