

SharedOut Privacy Policy

Effective Date: 20th June 2026

I. Preamble and Applicability

Greetings and welcome to SharedOut! (hereinafter referred to as the “**SharedOut**” or or “**Platform**”). This is the Privacy Policy (“**Policy**”) that applies to all products and services provided to you by SharedOut (collectively referred to as “the **Services**”). In the event that a specific product or service provided to you is accompanied by a separate privacy policy or similar legal document, such separate document shall prevail.

The Platform is maintained by Aishin Tech Pte Ltd. (Company Registration No. 201701719W), a private limited company incorporated under the laws of the Republic of Singapore with its registered office address at 21 Merryn Terrace S298427 (“**Company**”, “**we**,” “**our**” or “**us**”).

To provide the Services to you (“**you**” and “**your**”), during your registration, login, browsing, and use of the Platform’s services or tools we will, based on this Policy, collect, store, use, process, transmit, disclose, and delete relevant data. This Policy describes:

- What Personal Data we collect;
- Why and how it is collected’
- How it is used, protected, and shared (with third parties if relevant); and
- How you may exercise your rights concerning your Personal Data.

We place great importance on protecting your personal data and privacy rights. The Platform is committed to handling your personal data appropriately in accordance with Singapore’s Personal Data Protection Act 2012 (“**PDPA**”) and other relevant laws and regulations.

During your registration, login, browsing, and use of the Platform’s services or tools we will, based on this Policy, collect, store, use, process, transmit, disclose, and delete relevant data.

This Policy does not apply to services provided to you by other third parties. The processing and protection of your information by such third parties shall be governed by their respective privacy policies or similar documents. We assume no responsibility for the privacy practices or the collection, use, or disclosure of personal data by any third party. Where the Services involve or integrate third parties (including but not limited to Google Cloud, Firebase and Stripe), the applicable terms and conditions and privacy policies of such third parties shall apply directly between you and the relevant third party.

Before clicking “Agree” and starting to use the Platform’s services, please carefully read through this Policy. By clicking to agree or by using the services, you consent to the collection, storage, use, disclosure and other uses and processing of your personal data by us in accordance with this Policy and you are deemed to have understood and accepted all terms of this Policy. In addition to this Policy, we may also, under certain circumstances, inform you of the purposes and scope of our collection, use, and disclosure of your personal data through instant notifications (including pop-up windows, page prompts, etc.) and feature update notes. These instant notifications and feature update notes constitute an integral part of this Policy and hold equal validity. Should you have any questions, comments, or suggestions regarding the content of this Policy, feel free to contact us via the contact information provided at the end of this Policy.

This Policy applies only to individual users (whether accessing the Platform on their own behalf, or on behalf of other individuals or corporate entities) and not to corporate users.

II. Terms and Definitions

- a) Platform Entity/Platform: Refers to the SharedOut Mobile App Platform, including its website, client applications, and all future iterations of service formats.
- b) Personal Data: Refers to information, whether factual or not, relating to an identified or identifiable natural person, provided that: (a) the identifiable natural person can be identified, directly or indirectly, from the very information, in particular by reference to an identifier

such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that identifiable natural person; or (b) the identifiable natural person can be identified by combining the information with other information which the organization possesses or is likely to have access to.

- c) Corporate Client Information: Refers to the organizational details, contact information, business contracts, project description, etc., provided when the registered entity is a company, partnership, or institution.
- d) Log Information: Includes access time, user ID, dialog ID, dialog content, as well as IP address, browser type, language preference, and access date and time.
- e) De-identification: Refers to the process of processing personal data so that it cannot be used to identify a specific natural person without additional information.
- f) Anonymization: Refers to the process of processing personal data so that a specific natural person cannot be identified with it, and the data cannot be restored to its original state.
- g) Cookie: Refers to the Cookies and similar device identification technologies commonly used on the Internet. When you use our services, we may employ relevant technologies to send one or more Cookies or anonymous identifiers to your device to collect, identify, and store information about your access and use of the products.

III. Types of Information We Collect

This Platform collects only the minimum data necessary to achieve service objectives, adhering to the principles of legality, legitimacy, and necessity. We will collect information under the following categories:

- a) Information Voluntarily Provided by Users
 - Registration Information: Personal data submitted during account registration, such as name, email address, and mobile phone number. For corporate clients, to the extent necessary for providing services, we may process relevant personal data including the position, contact number and other relevant personal data of your legal representative and designated contact person.
 - Real-Name Verification Materials: Personal credentials, ID photos, authorization letters, etc.
 - Information Required for Professional Services: The information you submit will be used by users to deliver services. Depending on the content of consultation, the personal data of involved parties may include, but not be limited to, names, nationality, place of residence, or other factual bases necessary for the service, as well as any supplementary documents or texts you upload (including but not limited to contracts, statements, correspondence, or case descriptions). We will obtain your consent for the provision, processing, and sharing of personal data prior to initiating specific consultation to facilitate further service delivery.
 - Feedback Information: When using relevant services, you may provide appropriate ratings for the Services and its related services. We will collect your feedback to optimize the service experience.
- b) Information Automatically Collected by the Platform
 - Log Information: Access time, IP address, browser type, and operating system.
 - Operational Behavior Data: Client access date and time, server access date and time, clicks, browsing, searches, AI module calling records, and other network information generated during your use of related services.
 - Cookies and Similar Technologies: Used for maintaining authentication status and preference settings.

c) Data Provided by Third Parties

We may obtain data related to you from third parties we collaborate with (e.g., third-party authentication service providers, payment platforms) for the purpose of identity verification, transaction processing, or other service-related functions.

IV. Purposes and Methods of Personal Data Use

We will only use your personal data in compliance with legal requirements and for the following legitimate purposes. We are committed not to use your personal data for any purposes unrelated to those listed below, unless we have obtained your prior consent or as otherwise stipulated by relevant laws.

a) Contractual Obligations

- a) Service Provision and Delivery: To fulfil any contractual obligations that exist between us and you, that is to say our Terms of Use; where We provide you with the basic functions or services of the Platform.

b) Legitimate Interest

- b) Registration and Identity Verification: To create and manage your account, verify the authenticity of your corporate or individual identity, and prevent fraudulent registrations or account impersonation.
- c) Payment and Settlement: To issue invoices, process payments, make settlements, and manage related fund transfers.
- d) Data Analysis and System Optimization: To improve services, optimize system performance, and enhance user experience. We use anonymized data only within necessary scope for algorithm optimization.
- e) Risk Identification and Platform Governance: To prevent, identify, detect, and investigate fraud, breaching, or other potentially risky behaviors, and to handle complaints, disputes, and security incidents.

c) Legal Obligations

- f) Compliance Assessment and Regulatory Obligations: To comply with applicable laws, regulations, regulatory requirements, and internal compliance policies, including but not limited to the obligations of Customer Due Diligence/Know Your Customer (“**CDD**”/“**KYC**”), sanctions screening, Anti-Money Laundering (“**AML**”), and Combating the Financing of Terrorism (“**CFT**”).

d) Consent

- g) Other Specific Purposes: With your explicit consent, we may use your personal data for other specific purposes, such as marketing communications, product update notifications, or participation in surveys. You may withdraw such consent at any time.
- h) In addition to the purposes for which you have consented to for our collection, use, and/or disclosure of your personal data as described in this Policy, and to the extent permitted by applicable data protection laws, we may also collect, use, and/or disclose your personal data without your consent as required by such laws, including for the following purposes: (a)

the legitimate interests of ours or of others; or (b) responding to lawful requests for regulation, investigation, arbitration, litigation, etc.

V. Sharing, Transfer, and Disclosure of Personal Data

a) Entrustment

We may entrust the collection, use, disclosure, and/or processing of your personal data to authorized partners (e.g., technical service providers, authorized partners) so that they may provide certain services or perform certain functions on our behalf and/or for the purposes stated in this Policy. We will only entrust the processing of your information for the purposes declared in this Policy. Authorized partners will only have access to the information necessary to perform their functions and must commit through contracts not to use the information for any other purposes beyond the scope of the entrustment. Should an authorized partner intend to use your information for a purpose not entrusted by us, your separate consent will be obtained.

b) Sharing

Except as set out below, we will never share your Personal Data for any purposes other than those strictly necessary for rendering the Services to you for your benefit.

We may share your personal data for the purposes outlined in this Policy in the following circumstances:

- **Sharing with Your Explicit Consent:** We will share your user information with other parties after obtaining your explicit consent. For example, upon your consent, sharing necessary personal data with users who are providing tools to you.
- **Necessary for Platform Operations and Compliance:** Sharing certain information with service providers for platform review, risk control, payment settlement, compliance support, etc.
- **Necessary for Fulfilling an Agreement to Which You Are a Party:** Sharing your information as required to establish or fulfill an agreement to which you are a party.
- **Compliance with Legal Obligations:** We may share your user information as required by laws and regulations, in response to litigation or arbitration proceedings, or upon lawful requests from administrative or judicial authorities.
- **Sharing with Partners for Jointly Provided Services:** For services jointly provided by us and our authorized partners, we may share your personal data with these partners. Such sharing is limited to lawful, legitimate, necessary, specific, and clearly defined purposes.

c) Transfer

To facilitate mergers, acquisitions, business asset transactions, or in connection with bankruptcy, dissolution, winding-up, or liquidation of us or other legal entities, we may disclose your user information to other organizations or individuals. We will follow lawful procedures and notify you in advance. All international transfers will comply with applicable data protection laws. Where required, safeguards such as Standard Contractual Clauses (“**SCCs**”) will be implemented to ensure your Personal Data is adequately protected throughout the transfer process.

d) Disclosure

We will only publicly disclose your user information under the following circumstances:

- With your explicit consent or based on your voluntary choice and on reasonable/legitimate grounds; or
- Where it is necessary to protect the personal and property safety of us, our users, or the public from infringement, we may disclose your user information in accordance with applicable laws or relevant agreements.

VI. Management of Personal Data

a) Access and Correction

- You can access and correct your basic information on this Platform via “Personal Center” → “Account Settings”. To access and/or correct other personal data, please contact us using the contact details provided in this Policy. To the extent permitted by applicable law, we will provide you with information regarding the use or disclosure of your personal data within the past year. When you request corrections, we will update the records accordingly and send the corrected data to third parties who have received your personal data within the past year (limited to those for whom the corrected information is necessary), ensuring that the corrected data remains necessary for any legal or business purposes.
- Changing or Withdrawing Consent
 - You may change or withdraw consent previously granted to us by managing the authorization status via [“Personal Center” – “Account Settings”].
 - You may also contact us using the details disclosed in this Policy to change or withdraw the scope of consent for our collection and processing of your personal data.
 - Upon your withdrawal of consent, we will cease processing the corresponding personal data. However, your withdrawal will not affect our processing of your personal data based on your previously given consent.
 - Please note that if you withdraw the consent for collection, use, and/or disclosure of all or part of your personal data, depending on the nature of the request, we may no longer be able to continue providing services to you, managing established contractual relationships, or fulfilling/concluding existing or potential agreements. This may result in the termination of any agreement you have with us and constitute a breach of your contractual obligations or commitments. In such cases, we expressly reserve all legal rights and remedies.

b) Process for Responding to the Above Requests

- For security reasons, you may be required to submit a written request or provide proof of identity. Before processing your request, we may require you to complete identity verification.
- To the fullest extent permitted by applicable law, we reserve the right to reject requests that:
 - Are not directly related to your identity;
 - Are repeated and lacking a reasonable basis;
 - Would require disproportionate technical resources (e.g., requiring the development of a new system or a fundamental change to existing processes);
 - Would infringe on the legitimate rights and interests of others; or
 - Are otherwise impracticable.
- If you are (i) unable to access or correct your personal data on this Platform, (ii) willing to change the scope of or withdraw your consent, close your account, or need to access, supplement, correct, delete, or copy any other personal data generated from your use of this Platform’s applications, or (iii) convinced that we have violated any laws, regulations, or agreements, you may contact us using the contact information published in this Policy.

c) Exceptions to Denying Access and/or Correction Requests

To the extent permitted and/or required by applicable law, we reserve the right to deny any request for access and/or correction, including but not limited to the following circumstances:

- Regarding Access Requests:
 - The request is repetitive or systematic, and granting it would unreasonably interfere with the organization's operations;
 - Providing access would impose an unreasonable burden or expense on the organization, or be manifestly disproportionate to the individual's interests;
 - The requested information does not exist or cannot be found;
 - The requested information is trivial;
 - The request is otherwise frivolous or harassing; or
 - The request concerns personal data protected by legal professional privilege, or the disclosure of such data would reveal confidential business information of the organization and, in the reasonable judgment of a reasonable person, could harm the organization's competitive position.
- Regarding Access and/or Correction Requests:
 - The request concerns advisory data retained solely for evaluation purposes;
 - The request relates to prosecution documents where not all related proceedings have been completed; and/or
 - The request relates to derived personal data.

d) Right to Data Portability

Pursuant to relevant provisions of the PDPA, you may request us to:

- Provide you with the personal data supplied to us in a structured, commonly used, and machine-readable format (e.g., JSON, CSV); or
- Transfer your personal data to another organization as per your instruction (where applicable and feasible).

When processing your data portability request, we will adhere to the following principles:

- We will only process portability requests where permitted by applicable law and technically feasible.
- The right to data portability does not apply to exceptions specified in this Policy or by law (e.g., where it would compromise trade secrets, affect others' personal data, or involve data required by law to be retained, etc.).
- Your request must not unreasonably affect the rights and freedoms of others, or the security or stability of our systems.

We will respond within a reasonable time after receiving your request and inform you of the scope of data portability, the mode of transmission, and any potential limitations.

VII. Protection and Storage of Personal Data

- a) We attach great importance to your information security and endeavor to implement reasonable physical, electronic, and administrative measures to protect your user information. We safeguard user information against unauthorized access, disclosure, use, alteration, damage, or loss. For instance, we employ encryption technologies to enhance user information security; utilize trusted security mechanisms to prevent malicious attacks; implement access controls to ensure that only authorized personnel can access user information; execute reliable disaster recovery protocols and data backups; and conduct security and privacy training to enhance employee awareness of protecting user information.

- b) Despite having implemented reasonable and effective security measures in accordance with relevant laws and regulations, we cannot guarantee 100% security of information due to technological limitations and potential malicious attacks. Please understand that our systems and communication networks may be subject to factors beyond our control. Therefore, we strongly advise you to take proactive measures to protect the security of your personal data, such as using complex passwords, changing passwords regularly, and not disclosing your passwords or related personal data to others.
- c) In the unfortunate event of a user information security incident (leakage, loss, etc.), we will, as required by laws and regulations, promptly notify you of the situation of the incident and its potential impact, the measures we have taken or will take, suggestions for prevention and risk mitigation that you can adopt, and the available remedial measures. We will notify you promptly via email, letter, phone call, or push notification etc. If it is impractical to notify each individual information subject, we will issue a public announcement in a reasonable and effective manner.
- d) In the event that a product or service ceases operation, we will take reasonable measures to protect the security of your user information. This includes promptly ceasing further collection of user information; notifying users of the discontinuation of the product or service via separate notification or public announcement; and deleting or anonymizing the personal data we hold.
- e) Our servers are located in Singapore. To provide our services to you, we may transfer your personal data to other countries where we or our third-party service providers conduct business, and store and process it locally. We will ensure that any cross-border transfer complies with the relevant requirements of the PDPA, specifically ensuring that overseas recipients provide protection standards comparable to those required by the PDPA. This may include entering into legally binding agreements with overseas recipients to safeguard your personal data.
- f) During cross-border transfers, your personal data may be involved in the following business scenarios:
 - **Access by Overseas PMO Teams to Project Materials or Deliverables**
To ensure project management and delivery quality, PMO teams may require remote access to project-related materials, which may contain limited personal data. Access is strictly limited to business necessity and protected by stringent access controls.
 - **AI Model Retrieval and Operation**
During processes such as AI model inference, training, or optimization, models may require collaboration with overseas teams or system components to process data stored in Singapore.
 - **System Maintenance and Log Analysis by Technical Support Teams**
Global technical support teams may remotely access system logs and operational data for troubleshooting, repairs, and performance optimization. When personal data is involved, measures such as encryption and access controls will be implemented.
 - **Conducting Compliance Assessments or Due Diligence Services in collaboration with Third Parties through the Platform**
To deliver professional services, we may share certain personal data with overseas partners. These partners will only access such data to the extent necessary to perform their functions and must comply with contractual data protection obligations.

If you explicitly object to cross-border data transfers, you may choose to close your account or contact the Platform's Data Protection Officer (DPO) to exercise your relevant rights.

g) **Information Retention Period**

Generally, we will retain your personal data for as long as you use the Platform's applications to achieve the processing purposes described in this Policy, unless otherwise required by applicable laws and regulations or national regulatory documents.

Upon your request to delete personal data or close your account, we will delete your personal data as soon as possible in accordance with applicable laws and regulations, unless a longer retention period is required by applicable laws and regulations or national regulatory

documents. However, in the following circumstances, we may adjust the retention period of personal data based on legal requirements:

- To comply with applicable laws, regulations, or other relevant provisions.
- To comply with the requirements of court judgments, rulings, or other legal procedures.
- To comply with requests from relevant government authorities or legally authorized organizations.
- We have reasonable grounds to believe it is necessary to comply with relevant laws and regulations.
- To fulfill relevant service agreements or this Policy, or to provide necessary protection for the public interest, or for the legitimate rights and interests of clients, [Company], other users, or employees, including their personal or property safety, etc.

After you terminate your use of the Platform's services, we will cease the collection and use of your personal data, unless otherwise stipulated in this Policy or permitted by applicable laws and regulations or regulatory authorities (to continue data retention and use).

VIII. Protection of Minors' Information

This service is intended solely for users aged 18 or older, or those who have reached the legal age of majority under applicable laws. However, given the limitations of existing technological means and business models, it is difficult for us to identify the personal data of minors during the account registration process. If you are the guardian of a minor and discover that we have unintentionally collected, used, or disclosed the minor's personal data, you may contact us using the contact information provided in this Policy. Upon completion of the necessary verification procedures, we will delete or anonymize the relevant information based on the actual circumstances.

IX. Advertisements

There may be advertisements of third party products and/or services displayed within this Platform. The Company shall not be responsible for your interactions with such third parties, including their platforms (if any), which are not subject to this Policy.

X. Updates and Modifications to This Policy

- a) To provide you with a better service experience, we will continuously improve our technologies. We may update this Policy and notify you via SMS or other appropriate means, keeping you informed of the latest version. However, we will not restrict your rights under this Policy without your explicit consent.
- b) In the event of significant changes, we will also provide more prominent notifications (including SMS, email, in-site pop-ups, or announcements on the Platform's homepage) to inform you of the relevant changes again and, where required by law or regulation, obtain your consent.
- c) Significant changes referred to in this Policy include, but are not limited to:
 - Major alterations to our service models, such as the purposes of personal data processing, the types of personal data processed, and the manner of personal data use.
 - Major changes to ownership or organizational structure, such as those resulting from business restructuring, bankruptcy, or mergers and acquisitions.
 - Changes concerning the primary recipients of personal data (entities with whom data is shared, transferred, or publicly disclosed).
 - Significant changes to your participation in personal data processing and the way you exercise related rights.
 - Changes made in response to the issuance and implementation of national policies or legal regulations.

By continuing to use the Platform after the Policy update, you acknowledge that you have fully read and accepted the revised terms. For these reasons, we encourage you to periodically review this Policy for the latest version.

XI. Dispute Resolution Mechanism and Governing Law

- a) This Policy shall be governed by the laws of Singapore.
- b) All disputes, controversies, or differences arising out of or in connection with this Policy shall first be attempted to be mediated and resolved internally between the Parties. The Parties hereto agree to participate in the internal mediation in good faith. The disputes, controversies or differences shall be referred within seven (7) days to the Singapore Mediation Centre ("**SMC**") in the event the internal mediation does not work. The Parties agree to participate in mediation in good faith and undertake to abide by the terms of any settlement reached. If the dispute cannot be resolved by mediation within sixty (60) days of the date that it is referred to mediation, then the dispute shall be submitted to the non-exclusive jurisdiction of the Courts of Singapore.

XII. Contact Information and Complaint Channels

To better protect your personal data, we have established a dedicated Cybersecurity and Personal Data Protection Department. If you have any questions or suggestions regarding this Policy or the protection of personal data during your use of the Platform's applications, you may send your claims and supporting materials to the following contact details. We will provide feedback as soon as possible upon receiving the relevant information:

- Data Protection Officer (DPO): Matthew Lee
- Email: support@sharedout.com.sg
- Customer Service Hotline: +65 8473 8285
- Address: 21 Merryn Terrace S298427

If you are dissatisfied with our response, particularly if you believe our processing of personal data has infringed upon your lawful rights and interests, and we have failed to provide a satisfactory solution or refused to make improvements after receiving your feedback, you may lodge a complaint or report with the relevant regulatory authorities.