

PRIVACY POLICY

Effective Date: May 15, 2026

1. INTRODUCTION

PMaaSHub, LLC (“Company,” “we,” “our,” or “us”) is committed to protecting your privacy. This Privacy Policy explains how we collect, use, disclose, and protect personal information when you access or use our website at www.PMAASHub.com and the services available through it (collectively, the “Platform”).

The Platform is an online marketplace that connects certified project management professionals (“Providers”) with businesses and individuals seeking project management services (“Customers”). By using the Platform, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with this Privacy Policy, do not use the Platform.

2. INFORMATION WE COLLECT

We collect the following categories of information:

2.1 Information You Provide Directly.

(a) *Provider Registration Data:* When a Provider registers as a Provider, we collect:

- Name
- Email
- Professional profile link
- Areas of expertise
- Methodology (Agile, Waterfall, Hybrid)
- Past projects showcase
- Availability

(b) *Customer Registration Data:* When a business or individual registers as a Customer, we collect your first and last name, company name, and email address.

(c) *Communications:* Messages, work descriptions, and other content submitted through the Platform’s internal chat and hour-submission tools.

2.2 Information Collected Automatically. When you visit the Platform, we may automatically collect:

(a) Log data, including your IP address, browser type and version, operating system, referring URLs, and pages visited;

(b) Device identifiers and usage data; and

(c) Session information, including time and duration of visits.

We use our own internal analytics tools to monitor Platform traffic and usage patterns.

- 2.3 Information from Third Parties. We may receive information from third-party service providers in connection with your use of the Platform, including from Stripe in connection with payment processing and from Supabase in connection with file storage. We do not receive or store payment card numbers, bank account numbers, or other sensitive financial data, that information is handled exclusively by Stripe.
- 2.4 Cookies and Tracking Technologies. We use cookies and similar tracking technologies to operate and improve the Platform. A cookie is a small file placed on your device when you visit a website. For more information about our use of cookies and your choices, please review our Cookie Policy. If you choose to decline non-essential cookies, some Platform features may not function properly.

Note Regarding Third-Party Tracking Pixels: If we deploy any third-party tracking pixels or similar technologies on the Platform (such as a Meta Pixel or analytics tags), we will obtain your consent through a cookie consent banner before any such technology collects data about your activity. You will always have the option to accept or decline such tracking. We will not activate any third-party pixel without a functional cookie consent mechanism in place.

3. HOW WE USE YOUR INFORMATION

We use personal information for the following purposes:

- 3.1 Account creation, verification, and management, including verifying Provider certifications;
- 3.2 Operating and improving the Platform and its features;
- 3.3 Facilitating connections, communications, and transactions between Providers and Customers;
- 3.4 Processing and recording payment transactions through Stripe;
- 3.5 Communicating with you about your account, the Platform, or your transactions, including sending service-related notices;
- 3.6 Monitoring and enforcing compliance with our Terms of Service;
- 3.7 Detecting, investigating, and preventing fraud, abuse, and unauthorized activity;
- 3.8 Analyzing Platform usage and traffic patterns using our internal analytics tools; and
- 3.9 Complying with applicable legal obligations.

4. SHARING OF INFORMATION

We do not sell your personal information. We may share your information only in the following circumstances:

- 4.1 Other Platform Users. Provider profile information (as discussed in Section 2.1(a)) is visible to registered Customers for the purpose of facilitating connections. Personal contact information is not shared with other users directly.

- 4.2 Service Providers. We share information with trusted third-party vendors who assist in operating the Platform, including:
- (a) Supabase — for secure storage of Provider documents;
 - (b) Stripe, Inc. — for payment processing; and
 - (c) Hosting and infrastructure providers.

These service providers are authorized to use your information only as necessary to perform services on our behalf and are required to protect it appropriately.

- 4.3 Legal Requirements. We may disclose your information if required by law, court order, or governmental authority, or if we believe disclosure is necessary to protect the rights, property, or safety of PMaaSHub, our users, or the public.
- 4.4 Business Transfers. In the event of a merger, acquisition, reorganization, or sale of all or substantially all of PMaaSHub's assets, your information may be transferred to the successor entity. We will provide notice if such a transfer occurs.
- 4.5 With Your Consent. We may share your information for any other purpose with your prior consent.

5. COOKIES AND TRACKING TECHNOLOGIES

We use cookies to:

- 5.1 maintain your login session and Platform preferences;
- 5.2 track internal analytics and Platform performance; and
- 5.3 support any third-party advertising or analytics tools for which you have provided consent.

You may control cookie preferences through your browser settings or through the cookie consent banner displayed on the Platform. Disabling certain cookies may affect Platform functionality.

For detailed information about the types of cookies we use and how to manage them, see our Cookie Policy available on the Platform.

6. DATA SECURITY

We implement reasonable and appropriate technical and organizational measures to protect your personal information against unauthorized access, alteration, disclosure, or destruction. These measures include secure data transmission (SSL/TLS encryption), access controls, and third-party security standards for our service providers.

However, no method of transmission over the Internet or electronic storage is completely secure. We cannot guarantee the absolute security of your information. If you believe your account has been compromised, contact us immediately at info@PMaaSHub.com.

7. DATA RETENTION

We retain your personal information for as long as your account is active and as necessary to provide you with Platform services, comply with our legal obligations, resolve disputes, and enforce our agreements. Provider documents are retained in Supabase for as long as the Provider's account remains active. Upon account closure, we will retain only the information necessary to meet our legal, regulatory, and operational obligations.

8. YOUR RIGHTS

Depending on your location and applicable law, you may have the following rights with respect to your personal information:

- 8.1 Right to Access: the right to know what personal information we hold about you;
- 8.2 Right to Correction: the right to correct inaccurate or incomplete personal information;
- 8.3 Right to Deletion: the right to request that we delete your personal information, subject to certain exceptions;
- 8.4 Right to Restriction: the right to request that we limit our processing of your personal information in certain circumstances;
- 8.5 Right to Data Portability: the right to receive a copy of your personal information in a structured, machine-readable format;
- 8.6 Right to Object: the right to object to certain types of processing; and
- 8.7 Right to Opt Out of Sale: we do not sell personal information; however, if applicable law requires we offer this right, you may exercise it by contacting us.

To exercise any of these rights, submit a written request to info@PMaaSHub.com. We will respond to verified requests within the time period required by applicable law (generally 45 days, with a possible extension). We will not discriminate against you for exercising your privacy rights.

9. CALIFORNIA RESIDENTS — ADDITIONAL RIGHTS (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020 (collectively, "CCPA/CPRA").

- 9.1 Applicability. This section applies to residents of California and supplements the rest of this Privacy Policy. It is provided pursuant to the California Consumer Privacy Act of 2018 and the California Privacy Rights Act of 2020 (collectively, "CCPA/CPRA"). If you are a California resident, you have additional rights regarding the collection and use of your personal information.
- 9.2 Categories of Personal Information We Collect. In the preceding 12 months, we may have collected the following categories of personal information about California residents, from the sources listed, and for the business or commercial purposes described:

Category	Examples Collected by PMaaSHub	Source	Business/Commercial Purpose
Identifiers	Full name, email address, IP address, account name	Directly from you; automatically collected	Account creation and management; platform operation; fraud prevention
Personal information under Cal. Civ. Code § 1798.80	Name, employment history	Directly from you	Account creation; Provider vetting and verification
Commercial information	Transaction records, hour-submission records, payment history (via Stripe)	Stripe (payment processor)	Facilitating payments; platform operation
Internet or network activity	Browsing history on the Platform, pages visited, session duration, referring URLs, device type, browser type	Automatically collected	Internal analytics; platform performance monitoring; security
Professional or employment-related information	Resume, job title, industry, desired hourly rate, security clearance status (yes/no only)	Directly from you (Providers only)	Provider vetting, verification, and profile display
Education information (as defined under FERPA)	Project management certifications	Directly from you (Providers only)	Provider credential verification
Geolocation data	Approximate location inferred from IP address	Automatically collected	Geographic access restrictions; platform security
Inferences	Usage patterns and Platform engagement data drawn from the above categories	Automatically collected	Platform improvement; internal analytics

9.3 Categories of Personal Information Disclosed for a Business Purpose. In the preceding 12 months, we have disclosed the following categories of personal information to third parties for a business purpose:

- (a) Identifiers (name, email address, IP address) — disclosed to Supabase and hosting/infrastructure providers;
- (b) Professional or employment-related information (Provider profiles including title, industry, hourly rate, certifications, and security clearance status) — displayed to registered Customers to facilitate connections;
- (c) Commercial information (transaction and payment data) — disclosed to Stripe solely for payment processing; and
- (d) Internet or network activity — processed by our internal analytics tools and not disclosed to third-party ad networks.

Service providers to whom we disclose personal information are contractually prohibited from using that information for any purpose other than performing services on our behalf and are required to protect it appropriately.

9.4 Personal Information We Do Not Sell or Share. We do not sell your personal information and have not done so in the preceding 12 months. We do not share your personal information with third parties for cross-context behavioral advertising purposes. We do not have actual knowledge that we sell or share the personal information of consumers under 16 years of age.

9.5 Your California Privacy Rights. California residents have the following rights under the CCPA/CPRA, as applicable:

- (a) *Right to Know (Disclosure).* You have the right to request that we disclose: the categories of personal information we have collected about you; the categories of sources from which personal information was collected; our business or commercial purpose for collecting, selling, or sharing personal information; the categories of third parties to whom we disclose personal information; and the specific pieces of personal information we have collected about you. You may request this information for the preceding 12-month period. You also have the right to request personal information collected beyond the preceding 12-month period to the extent required by applicable law, provided that doing so does not require a disproportionate effort on our part. Please note that we are not required to: (a) retain personal information collected for a single one-time transaction not ordinarily retained in the course of business; (b) re-identify or link data not maintained as personal information in the ordinary course of business; or (c) provide the specific pieces of personal information to you more than twice in a 12-month period.
- (b) *Right to Deletion.* You have the right to request that we delete personal information we have collected about you and direct our service providers to do the same. Upon receipt of a verifiable request, we will delete your personal information from our records, subject to the following exceptions. We may decline to delete your personal information if retaining it is

necessary to: (a) complete the transaction for which it was collected or otherwise perform our contract with you; (b) detect security incidents or protect against malicious, deceptive, fraudulent, or illegal activity; (c) debug to identify and repair errors that impair existing intended functionality; (d) exercise free speech or ensure another consumer's right of free speech, or exercise another right provided for by law; (e) comply with the California Electronic Communications Privacy Act; (f) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest where deletion would likely render the research impossible or seriously impaired; (g) enable solely internal uses reasonably aligned with your expectations based on your relationship with us; (h) comply with an existing legal obligation; or (i) otherwise use your personal information internally in a lawful manner compatible with the context in which you provided it.

- (c) *Right to Correction.* You have the right to request that we correct inaccurate personal information we maintain about you. We will use commercially reasonable efforts to correct the information as directed, taking into account the nature of the personal information and the purposes for processing it.
- (d) *Right to Opt-Out of Sale or Sharing.* As stated in Section 9.4, we do not sell or share personal information for cross-context behavioral advertising. There is currently no need to opt out. If our practices change, we will update this Privacy Policy and provide a "Do Not Sell or Share My Personal Information" mechanism on our homepage.
- (e) *Right to Limit Use of Sensitive Personal Information.* You have the right to direct us to limit our use and disclosure of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer. PMaaSHub does not currently collect or process sensitive personal information as defined under CPRA (Cal. Civ. Code § 1798.140(ae)). A security clearance indicator (yes/no) is collected for Provider vetting purposes only and is not used beyond that purpose. If our practices change, we will update this section accordingly.
- (f) *Right to Know About and Opt-Out of Automated Decision-Making.* You have the right to know whether we use automated decision-making technology, including profiling, in connection with decisions that produce legal or similarly significant effects on you, and to opt out of such processing. PMaaSHub does not currently use fully automated decision-making in connection with account approvals or other decisions that produce legal or similarly significant effects. Provider account approvals are reviewed and approved by a human administrator. If our practices change, we will update this section.
- (g) *Right to Access Information About Automated Decision-Making.* You have the right to request information about the logic involved in any automated decision-making processes we use and the potential consequences of those processes for you.
- (h) *Right to Non-Discrimination.* We will not discriminate against you for exercising any of your rights under the CCPA/CPRA. We will not: deny you goods or services; charge you different prices or rates; provide a different level or quality of goods or services; or suggest that you will receive a different price, rate, or quality of goods or services. We may,

however, offer a different price or level of service where that difference is reasonably related to the value provided to our business by your personal information, as permitted by applicable law.

- 9.6 How to Exercise Your California Privacy Rights. To exercise any of the rights described in this section, you or your authorized agent may submit a verifiable consumer request by: (a) emailing us at info@PMaaSHub.com with the subject line “California Privacy Rights Request”; or (b) visiting www.PMaaSHub.com and submitting a request through our privacy request form www.pmaashub.com/privacy-request. When submitting your request, please include your full name and email address associated with your account, a description of the specific right you wish to exercise, and sufficient information to allow us to verify your identity.

You may designate an authorized agent to submit a CCPA/CPRA request on your behalf. To use an authorized agent, you must provide the agent with written permission signed by you, and we may require you to verify your identity directly with us even when using an authorized agent. We may deny a request from an agent who does not submit proof of valid authorization.

- 9.7 Verification Process. We are required to verify the identity of any individual who submits a request to exercise rights under the CCPA/CPRA before we can fulfill the request. We will use personal information you provide in connection with your request to verify your identity against information we already maintain. Depending on the nature of your request, we may ask you to confirm personal information already associated with your account and/or provide additional identifying information. We will only use personal information submitted in connection with a verification request to verify your identity and fulfill the request. We will respond to verifiable consumer requests within 45 days of receipt. Where reasonably necessary, we may extend this period by an additional 45 days and will notify you within the initial 45-day period of the extension and the reason for it. We will not charge a fee unless your request is excessive, repetitive, or manifestly unfounded.
- 9.8 California Online Privacy Protection Act (CalOPPA). A link to this Privacy Policy appears conspicuously in the footer of our website and on all pages where personal information is collected, in compliance with the California Online Privacy Protection Act. Our Platform does not currently respond to “Do Not Track” (DNT) browser signals. We may collect information about your online activities on the Platform as described in this Privacy Policy.

10. EUROPEAN RESIDENTS — GDPR NOTICE

- 10.1 Applicability and Data Controller. This section applies to individuals accessing the Platform from within the European Economic Area (“EEA”), the United Kingdom (“UK”), or Switzerland (collectively, “European Residents”). It supplements the rest of this Privacy Policy and is provided in accordance with the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and, for UK residents, the UK GDPR as retained in UK law by the European Union (Withdrawal) Act 2018. PMaaSHub, LLC is the data controller responsible for your personal information for the purposes of applicable European data protection law. Our contact details are set out in Section 17 of this Privacy Policy.

10.2 Key Terms. For the purposes of this section: “Personal Information” means any information relating to an identified or identifiable individual. “Special Category Personal Information” means personal information revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person’s sex life or sexual orientation. PMaaSHub does not collect special category personal information. A security clearance indicator (yes/no) does not constitute special category personal information under the GDPR. If you voluntarily include such information in your resume upload, you do so at your own discretion; we will treat it confidentially and will not process it beyond what is necessary for the purposes described in this Privacy Policy.

10.3 Legal Bases for Processing. Under the GDPR, we may only use your personal information if we have a lawful basis for doing so. We rely on the following legal bases:

- (a) *Performance of a contract* — to create and manage your account; to facilitate transactions between Providers and Customers; to verify Provider credentials; and to process payments through Stripe;
- (b) *Legitimate interests* — to operate, secure, monitor, and improve the Platform; to detect and prevent fraud and unauthorized access; to conduct internal analytics; to enforce our Terms of Service; and to communicate with users about Platform-related matters. Our legitimate interests are operating and improving a secure and functional marketplace Platform, preventing fraud and misuse, and maintaining the integrity of the Provider verification process. We have assessed that our legitimate interests are not overridden by your interests, rights, and freedoms;
- (c) *Legal obligation* — to comply with applicable laws and regulations, including data breach notification obligations; and
- (d) *Consent* — where we have obtained your prior consent, for example for non-essential cookies and third-party tracking technologies (such as the Meta Pixel, where activated). Where we rely on consent, you have the right to withdraw that consent at any time without affecting the lawfulness of processing carried out prior to withdrawal. To withdraw consent for non-essential cookies, use the cookie preference tool on the Platform. For any other consent-based processing, contact us at info@PMaaSHub.com.

10.4 How and Why We Use Your Personal Information. The following table sets out the specific purposes for which we process your personal information and our legal basis for each:

Purpose	Legal Basis
Creating and managing user accounts	Performance of contract

Verifying Provider credentials and certifications	Performance of contract; legitimate interests
Displaying Provider profiles to registered Customers	Performance of contract
Facilitating interview requests and communications between Providers and Customers via the Platform's internal chat	Performance of contract
Processing hour submissions and facilitating payment via Stripe	Performance of contract
Sending service-related notices and account communications	Performance of contract; legitimate interests
Preventing and detecting fraud, abuse, and unauthorized access	Legitimate interests; legal obligation
Monitoring and enforcing compliance with our Terms of Service	Legitimate interests
Conducting internal analytics and improving Platform performance	Legitimate interests
Complying with legal and regulatory obligations	Legal obligation
Using non-essential cookies and third-party tracking technologies (when activated)	Consent

The above table does not apply to special category personal information. We do not currently collect special category personal information. If we do so in the future, we will only process it with your explicit consent.

10.5 Promotional Communications. We may use your personal information to send you updates (by email) about the Platform, including notices about new features or service changes. We have a legitimate interest in communicating with users about the Platform and its services. Where consent is required by applicable law before sending marketing communications (for example, to users in the EEA), we will obtain that consent separately and clearly. We will never sell or share your personal information with third parties for their own marketing purposes. You have the right to opt out of receiving promotional communications at any time by: (a) emailing us at info@PMaaSHub.com; (b) using the “unsubscribe” link in any email communication we send; or (c) updating your account communication preferences on the Platform.

10.6 International Transfers. PMaaSHub is operated from the United States. If you access the Platform from the EEA, UK, or Switzerland, your personal information will be transferred to and processed in the United States. The United States does not have data protection laws

equivalent to those in the EEA or UK. We take the following steps to ensure that such transfers are made in compliance with applicable data protection law: where required, we rely on Standard Contractual Clauses approved by the European Commission (or equivalent UK mechanisms) when transferring personal information to third-party service providers based outside the EEA/UK. Our third-party service providers (including Stripe and Supabase) are required to process personal information in accordance with applicable data protection law and to implement appropriate technical and organizational safeguards. If you would like further information about the safeguards we have in place for international transfers, please contact us at info@PMaaSHub.com.

10.7 Retention Periods. We retain your personal information for as long as your account is active and as necessary to provide you with Platform services, comply with our legal obligations, resolve disputes, and enforce our agreements. Specifically:

- (a) Account information (name, email, etc.) is retained for the duration of your account and for a reasonable period thereafter to allow for dispute resolution and legal compliance;
- (b) Provider documents (resume, headshot, certifications) stored via Supabase are retained for the duration of your Provider account and deleted or anonymized upon account closure, except where retention is required by applicable law;
- (c) Transaction and payment records are retained as required by applicable tax, financial, and commercial record-keeping laws; and
- (d) Usage and log data collected automatically is retained for a limited period consistent with our legitimate interests in Platform security and analytics.

We will not retain your personal information for longer than is necessary for the purposes for which it was collected.

10.8 Your Rights Under the GDPR. In addition to the rights set out in Section 8 of this Privacy Policy, European Residents have the following specific rights under the GDPR:

- (a) *Right of Access*. You have the right to be provided with a copy of the personal information we hold about you and information about how we process it.
- (b) *Right to Rectification*. You have the right to require us to correct any inaccurate or incomplete personal information we hold about you.
- (c) *Right to Erasure (Right to Be Forgotten)*. You have the right to require us to delete your personal information in certain circumstances — for example, where it is no longer necessary for the purpose for which it was collected, where you withdraw consent (where processing is based on consent), or where you object to processing and we have no overriding legitimate grounds.
- (d) *Right to Restriction of Processing*. You have the right to require us to restrict our processing of your personal information in certain circumstances — for example, where you contest

the accuracy of the data while we verify it, or where you have objected to processing while we consider whether our legitimate grounds override yours.

- (e) *Right to Data Portability.* Where our processing of your personal information is based on your consent or the performance of a contract, you have the right to receive the personal information you have provided to us in a structured, commonly used, and machine-readable format, and to transmit that data to another controller where technically feasible.
- (f) *Right to Object.* You have the right to object at any time to our processing of your personal information where we rely on legitimate interests as our legal basis. We will cease processing unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or where the processing is for the establishment, exercise, or defense of legal claims. You also have the right to object at any time to processing of your personal information for direct marketing purposes, including profiling carried out in connection with direct marketing.
- (g) *Right Not to Be Subject to Automated Individual Decision-Making.* You have the right not to be subject to a decision based solely on automated processing — including profiling — that produces legal effects concerning you or that similarly significantly affects you. PMaaSHub does not currently make any such fully automated decisions; Provider account approvals are reviewed and made by a human administrator.
- (h) *Right to Withdraw Consent.* Where we process your personal information based on your consent (for example, for non-essential cookies), you have the right to withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of any processing we carried out prior to the withdrawal.

10.9 How to Exercise Your GDPR Rights. To exercise any of the rights set out in Section 10.8, please email us at info@PMaaSHub.com with the subject line “GDPR Data Subject Request” and provide: (a) sufficient information to identify you, such as your full name and the email address registered to your account; (b) proof of your identity if reasonably required; and (c) a description of the right you wish to exercise and the information to which your request relates. We will respond within 30 days of receipt. We may extend this period by a further two months where the request is complex or we have received a high volume of requests, and we will notify you of any extension within the initial 30-day period. We will not charge a fee for responding to your request unless it is manifestly unfounded or excessive.

10.10 Right to Lodge a Complaint. You have the right to lodge a complaint about our processing of your personal information with your local supervisory authority. If you are based in the EEA, this is typically the data protection authority in the EU member state where you habitually reside, where you work, or where the alleged infringement occurred. A list of EEA supervisory authorities is available at: https://edpb.europa.eu/about-edpb/about-edpb/members_en. If you are based in the United Kingdom, you may contact the Information Commissioner’s Office (ICO) at: <https://ico.org.uk>. We would appreciate the opportunity to address your concerns before you contact a supervisory authority, and we invite you to contact us first at info@PMaaSHub.com.

10.11 EU/UK Representative. As PMaaSHub is a US-based company that may process the personal information of individuals in the EEA and UK, we are assessing whether Article 27 of the GDPR requires us to appoint a representative in the EU and/or UK. If required, we will update this section with our representative's contact details. If you have questions in the interim, please contact us directly at info@PMaaSHub.com.

11. CHILDREN'S PRIVACY

The Platform is not directed to children under the age of 13 (or 16 where required by applicable law). We do not knowingly collect personal information from children under the applicable minimum age. If we become aware that we have collected personal information from a child without parental consent, we will take steps to delete that information promptly. If you believe we have inadvertently collected information from a child, contact us at info@PMaaSHub.com.

12. FLORIDA RESIDENTS

We comply with the Florida Information Protection Act ("FIPA") and other applicable Florida and federal privacy and data security laws. In the event of a data breach affecting Florida residents, we will provide notification as required by FIPA.

13. GEOGRAPHIC RESTRICTIONS AND INTERNATIONAL USERS

The Platform is not available to residents of Iran, North Korea, Syria, Cuba, Crimea (Ukraine), or the Province of Quebec (Canada). If you access the Platform from outside the United States (excluding restricted jurisdictions), your information may be collected and processed in the United States, where data protection laws may differ from those in your home country. By using the Platform, you consent to the transfer and processing of your information in the United States.

14. DO NOT TRACK

Our Platform does not currently respond to "Do Not Track" (DNT) signals from browsers. We may collect information about your online activities on the Platform as described in this Privacy Policy.

15. LINKS TO THIRD-PARTY SERVICES

The Platform may contain links to or integrations with third-party websites or services, including Stripe and Supabase. This Privacy Policy does not apply to those third parties. We encourage you to review the privacy policies of any third-party services you use in connection with the Platform.

16. UPDATES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time. When we make material changes, we will post the updated policy on the Platform with a revised Effective Date. We may also notify you by email or through a notice on the Platform. Your continued use of the Platform after the updated policy is posted constitutes your acceptance of the changes.

17. CONTACT US

If you have questions, concerns, or requests related to this Privacy Policy or our privacy practices, please contact us at:

PMaaSHub, LLC

Email: info@PMaaSHub.com

Website: www.PMaaSHub.com