

PremInspect Privacy Policy

Effective Date: July 30, 2025

This Privacy Policy describes how PremInspect ("we," "us," or "our") collects, uses, processes, and shares your information when you use our Software as a Service (SaaS) product, PremInspect, accessible at **preminspect.tech** (the "Service"). We are committed to protecting your privacy and handling your data transparently and securely.

By using the Service, you agree to the collection and use of information in accordance with this Privacy Policy.

1. Information We Collect

We collect various types of information to provide and improve our Service to you.

1.1. Information You Provide Directly to Us

When you register for an account, configure inspections, or interact with our Service, you may provide us with the following personal information:

- **Account and Contact Information:** Your company name, your name and surname, email address, and cell phone number.
- **Billing and Payment Information:** Details necessary for processing subscriptions and payments.
- **User-Generated Content and Inspection Data:** As part of using PremInspect, you can upload various images and input data through custom workflow inspections. This includes:
 - **Images:** Any images you choose to upload, which may range from personal images, identity documents, and registration documents to general pictures related to assets or inspections. **Please note: We do not use any biometric processing on these images.**

- **Custom Workflow Inputs:** Data you configure and input into custom fields within your inspection workflows, such as rules for who does what, cost assignments, and other descriptive text or values. This data can vary widely based on your specific configurations.
- **Support and Feedback:** Information you provide when you contact us for support or submit feedback.

1.2. Information Collected Automatically

When you access and use our Service, we automatically collect certain information, including:

- **Usage Data:** This may include your device's Internet Protocol (IP) address, browser type and version, device type, operating system, unique device identifiers, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, and other diagnostic data.
- **Cookies and Tracking Technologies:** We use cookies, web beacons, and similar tracking technologies to monitor activity on our Service and store certain information. This helps us analyze user behavior and improve the Service.

1.3. Information from Third Parties

We may receive information about you from third-party services that we integrate with or utilize to provide our Service, such as:

- **Database and Hosting Providers:** Supabase (database) and Vercel (platform hosting).
- **Communication Services:** WhatsApp (for notifications), SendGrid (for emails and SMS).
- **Marketing and CRM Tools:** SendGrid or other CRM tools for sending out newsletters and marketing communications.

2. How We Use Your Information

We use the collected information for various purposes, primarily to provide, maintain, and improve our Service, and to communicate with you.

- **To Provide and Maintain Our Service:** This includes managing your account, enabling asset inspections, facilitating custom workflow creation and execution, and providing customer support.
- **To Improve and Personalize Your Experience:** We analyze usage patterns and feedback to enhance user experience, develop new features, and optimize existing functionalities.
- **To Communicate with You:** We use your contact information to send you service updates, important notices, and, with your consent, marketing communications and newsletters via WhatsApp, email, or SMS.
- **To Process Payments:** We use billing information to manage subscriptions and process payments securely.
- **To Ensure Platform Security and Prevent Fraud:** We use data to maintain the stability, integrity, and security of the PremInspect platform, including detecting and preventing fraudulent activities and unauthorized access.
- **To Comply with Legal Obligations:** We may process your information to fulfill regulatory requirements, respond to legitimate legal requests, and prevent fraud.
- **For Business Transfers:** In the event of a merger, acquisition, divestiture, or sale of assets, your information may be transferred as part of the transaction.
- **For Sale to Third Parties:** We may sell aggregated or anonymized data related to costs assigned to assets, if we develop a data pool that enables us to provide costing insights. This is the only type of data currently intended for sale. Any such sale will be conducted in compliance with applicable data protection laws, including obtaining necessary consent or providing opt-out mechanisms where required.

3. How We Share Your Information

We may share your information with the following categories of third parties:

- **Service Providers:** We engage third-party companies and individuals to facilitate our Service, provide the Service on our behalf, perform Service-related

services, or assist us in analyzing how our Service is used. These include:

- **Supabase:** For database services.
- **Vercel:** For platform hosting.
- **WhatsApp:** For sending notifications.
- **SendGrid:** For sending emails, SMS, and newsletters.
- **CRM/Newsletter Tools:** For managing client communications and newsletters.
- **For Business Transfers:** If PremInspect is involved in a merger, acquisition, or asset sale, your Personal Data may be transferred. We will provide notice before your Personal Data is transferred and becomes subject to a different Privacy Policy.
- **Law Enforcement and Legal Obligations:** We may disclose your Personal Data in the good faith belief that such action is necessary to:
 - Comply with a legal obligation.
 - Protect and defend the rights or property of PremInspect.
 - Prevent or investigate possible wrongdoing in connection with the Service.
 - Protect the personal safety of users of the Service or the public.
 - Protect against legal liability.

Important Note on User-Configured Data: When you use PremInspect's custom workflow features to collect data, including images, you (as the PremInspect client) act as the "data controller," determining the purpose and means of processing that data. PremInspect acts as a "data processor," processing this data on your behalf. You are responsible for ensuring you have the necessary legal bases and consents for any personal data you collect through your custom workflows, especially if it includes sensitive information or images of individuals. We recommend that you have a comprehensive Data Processing Addendum (DPA) in place with us to define the responsibilities of both parties.

4. International Data Transfers

PremInspect is a SaaS platform that will be sold globally. As such, your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country, or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place, including the security of your data and other personal information. This may include reliance on Standard Contractual Clauses (SCCs) or other legally recognized transfer mechanisms where applicable.

5. Data Retention

We retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy, unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements).

We apply the following best practices for data retention:

- **Account and Billing Data:** Retained for the duration of your active account with PremInspect and for a period thereafter as required by legal and financial regulations (e.g., typically 7+ years for financial records).
- **Usage Logs and Analytics Data:** Typically retained for 12-24 months for product improvement and performance monitoring.
- **Inspection Records and Images:** Retained for as long as required by your client contract and any relevant industry-specific legal minimums.
- **Identity Documents and Personal Images (if uploaded by users):** Retained for the shortest period necessary to fulfill the specific purpose for which they were uploaded, and securely deleted thereafter, or upon your request, unless a legal obligation requires longer retention.
- **Legal Holds:** In cases of litigation, regulatory investigations, or other legal requirements, data deletion may be suspended to ensure relevant data is preserved.

Once the retention period expires, we will securely delete or anonymize your Personal Data using methods such as cryptographic erasure or permanent deletion, ensuring it is irrecoverably removed.

6. Data Security

We are committed to protecting the security and integrity of your data. Our platform is built using secure, modern web frameworks and hosted on reputable, industry-leading cloud infrastructure providers. All API routes and databases are secured with access control layers, encryption, and continuous monitoring.

Our security measures include:

- **Platform Architecture:** Our platform is built using secure, modern web frameworks and hosted on reputable, industry-leading cloud infrastructure providers. All API routes and databases are secured with access control layers, encryption, and continuous monitoring.
- **Authentication & Access Control:**
 - APIs are protected using short-lived, cryptographically signed JSON Web Tokens (JWTs), which expire every 15 minutes.
 - Refresh tokens are securely stored and valid for 7 days, enabling seamless session continuation while maintaining security.
 - Access is role-based, restricting system functionality according to user permissions, adhering to the principle of least privilege.
- **Data Encryption:**
 - **In Transit:** All data is encrypted using TLS 1.2 or higher to protect it during transmission.
 - **At Rest:** Sensitive data is encrypted using modern cryptographic standards (e.g., AES-256) when stored on servers or databases.
- **Audit & Monitoring:**
 - We log critical system events and monitor for unauthorized activity.
 - Regular internal reviews and automated alerting help us quickly identify and respond to potential threats.
- **Incident Response:** We maintain a structured incident response plan, including rapid detection, containment, user notification (if required by law), and thorough post-incident reviews.

7. Your Data Rights

Depending on your location and applicable data protection laws (such as GDPR,

CCPA, and POPIA), you may have the following rights regarding your Personal Data:

- **Right to Be Informed:** The right to know what personal data is collected, the purposes for its collection, and how it will be used and shared.
- **Right of Access:** The right to request and obtain a copy of your personal data held by us.
- **Right to Rectification/Correction:** The right to request corrections to inaccurate or incomplete personal data.
- **Right to Erasure ("Right to Be Forgotten"):** The right to request the deletion of your personal data under specific circumstances.
- **Right to Object to Processing:** The right to opt-out of or restrict certain data processing activities, particularly those related to direct marketing or profiling.
- **Right to Opt-Out of Sale/Sharing (CCPA):** If you are a California resident, you have the right to opt-out of the sale or sharing of your personal information.
- **Right to Data Portability (GDPR):** The right to request your data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller.

How to Exercise Your Rights:

You can exercise your rights by contacting us at privacy@preinspect.com. We will respond to your request in accordance with applicable law.

For notifications, marketing, and newsletters, we will provide clear opt-in/opt-out mechanisms, allowing you to control your communication preferences.

8. Children's Privacy

Our Service is not directed to individuals under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If you are a parent or guardian and you are aware that your child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from anyone under the age of 13 without verification of parental consent, we take steps to remove that information from our servers.

If users upload images that contain identifiable children, the PremInspect client (as the data controller) is responsible for obtaining explicit parental or guardian consent, especially given the stringent requirements under laws like POPIA, which strongly

advise against identifiable images of children due to heightened risks.

9. Changes to This Privacy Policy

We may update our Privacy Policy from time to time to reflect changes in our practices, legal requirements, or technological advancements. We will notify you of any significant changes by posting the new Privacy Policy on this page, and by email or a prominent notice on our Service, prior to the change becoming effective.

We recommend reviewing this Privacy Policy periodically for any changes.

10. Contact Us

If you have any questions about this Privacy Policy, please contact us by email:

reece@preinspect.tech

11. Information Officer / Data Protection Officer

Please note that an Information Officer or Data Protection Officer has not yet been appointed for PremInspect. We are aware that certain data protection regulations, such as POPIA (for South Africa) and GDPR (for the EU/EEA), may require the appointment of such a role to oversee compliance and handle data subject requests. We are working to address this requirement as part of our ongoing commitment to data privacy.