PM Assist — Security and Data Protection Overview

PM Assist · security@pmassist.co.uk

Last reviewed: 28 July 2026

This overview describes the controls PM Assist operates. It is not a third-party audit report, and PM Assist does not currently hold SOC 2 or ISO 27001 certification. Where a control is planned rather than in place, it is not listed here.

Where your data is held

The application and database are hosted in Frankfurt, and document storage is in Stockholm. All customer data is stored in the EU.

Transfers outside the EU

When you ask a question, the relevant excerpts from your documents are sent to OpenAI in the United States to generate the answer. This is the only routine transfer of your content outside the EU. It is covered by OpenAI's Data Processing Addendum, which incorporates the EU Standard Contractual Clauses and the UK International Data Transfer Addendum.

Per-building data separation

Each building's data stays separate. Documents, chat history, and user accounts are isolated at the data layer through application controls designed to prevent cross-building access.

- Database queries are scoped to the active building
- Documents and chat history are separated per building
- User access is restricted to their assigned building
- Per-building controls reduce the risk of cross-building data access

Authentication and access control

PM Assist uses credential-based authentication with secure password hashing. Role-based access control is available on Starter plans and above.

- Passwords are hashed using bcrypt before storage
- Email verification required for new accounts
- Role-based access control (admin and member roles)
- Session management with secure, httpOnly tokens

Data storage and encryption

Documents and application data are stored with encryption in transit and at rest. File storage uses cloud infrastructure with server-side encryption.

- All traffic is encrypted via HTTPS/TLS
- Document storage uses server-side encryption (S3)
- Database connections use encrypted transport
- Sensitive fields (passwords, tokens) are hashed or encrypted

AI and data processing

When you ask a question, PM Assist sends relevant document excerpts to OpenAI's API to generate a response. Only the content needed to answer your query is transmitted.

- Only relevant document excerpts are sent to the AI provider — not entire files
- AI responses include source citations for verification
- Under OpenAI's standard API data usage policy, API inputs and outputs are not used to train their models. We do not currently hold a separate Zero Data Retention agreement

- AI-generated content should always be verified against source documents

Auditability and citations

Every AI-generated answer includes source citations referencing the original documents, pages, and sections. This supports verification, compliance workflows, and accountable decision-making.

- Source citations on every AI response
- Audit logging available on Pro and Enterprise plans
- Admin dashboard for user and tenant management
- Responses can be exported for compliance records

Operational controls

PM Assist includes server-side security headers and operational controls to protect against common web vulnerabilities.

- Content Security Policy (CSP) headers
- Clickjacking and MIME sniffing protection
- Strict referrer policy
- Rate limiting on authentication endpoints

Data retention and deletion

You retain ownership of all uploaded documents. Self-service account deletion and data export are available from your profile page. Automated daily cleanup enforces retention schedules without manual intervention.

- Account data retained until you delete your account (self-service or by request)
- Documents retained until deleted from the building they belong to
- Query logs automatically purged after 90 days
- Audit logs follow a tiered schedule: routine-event IPs scrubbed at 14 days, all PII scrubbed at 90 days, full records deleted at 180 days
- Expired authentication tokens purged daily; soft-deleted accounts hard-deleted after 30 days
- Self-service data export (JSON) available from your profile page

What happens when you delete your account

Account deletion is self-service, from your profile page, and takes effect immediately. It is confirmed with your password.

Removed immediately

- Your name, email address and password. The email is replaced with a non-routable placeholder so the account cannot be signed in to or recovered.
- Your chat and query history.
- Your building assignments — the record of which buildings you had access to.
- Documents and images you generated in the app, such as exported reports.
- All outstanding password reset, invitation and email verification tokens.
- The remaining account record is permanently deleted 30 days later by the daily cleanup job.

Retained, and why

- Audit log entries are kept, but stripped of personal content — the question, the answer, your IP address, your browser and your email are all removed. What remains is the action and its timestamp, which is what makes the log useful for investigating a security incident.
- Documents you uploaded stay with the organisation. They belong to the building, not to your user account, so that a colleague leaving does not take the building's O&M pack with them. To remove documents, delete them from the building before deleting your account, or ask us.

Billing

- If you are the last active member of your organisation, the subscription is cancelled immediately rather than at the end of the period, and the customer record held by our payment processor is deleted along with any stored payment method.
- If other people are still using the organisation, the subscription continues and they are unaffected. One person leaving does not cancel everyone's billing.
- If our payment processor cannot be reached at that moment, your deletion still completes and the cancellation is retried automatically. We do not make your erasure wait on a third party being available — but it does mean a cancellation can, rarely, lag the deletion by a short period.

Current limitations

- Accounts that sign in with Google and have never set a password cannot use self-service deletion, because deletion is confirmed with a password. Set a password from your profile first, or email us and we will action it.
- Master administrator accounts cannot be deleted from the profile page.
- The export is a JSON file covering your profile, organisation, building access, query history, audit records and generated documents. It does not include the original files you uploaded — download those from the building.

Shared responsibility

Security is a shared responsibility. We secure the application, infrastructure configuration, and data-layer controls we manage. Customers are responsible for user access management, password security, document selection, and internal governance of how the Service is used within their organisation.

Subprocessors

Regions marked with a specific data centre are infrastructure we configure and can evidence. Regions marked “EU regional setting” reflect the provider’s own regional configuration, which governs collection and initial processing; their terms permit processing elsewhere under the safeguards listed.

Service	Purpose	Region	Location
Vercel	Application hosting — runs the web application and its API	EU	Frankfurt (fra1)
Neon (PostgreSQL)	Application database — accounts, buildings, document metadata, chat history	EU	Frankfurt (eu-central-1)
Amazon Web Services (S3)	Document file storage — the PDFs and drawings you upload	EU	Stockholm (eu-north-1)
OpenAI	AI search and response generation — receives document excerpts and your question	US	United States
Stripe	Payment processing and subscription management	EU	European Union
Resend	Transactional email — verification, notifications, invitations	EU	European Union
Sentry	Error monitoring and application reliability	EU	European Union
Google Analytics 4	Product analytics. Consent-gated via Consent Mode v2; personal data is stripped before events are sent.	EU	EU regional setting
Google Ads	Conversion measurement only. Consent-gated via Consent Mode v2, cookieless — no advertising cookies, no remarketing or interest-based targeting.	EU	EU regional setting

Transfer safeguards

OpenAI: OpenAI's Data Processing Addendum, which incorporates the EU Standard Contractual Clauses and the UK International Data Transfer Addendum

Google Analytics 4: Google's Data Processing Terms, which incorporate the EU Standard Contractual Clauses and the UK International Data Transfer Addendum

Google Ads: Google's Data Processing Terms, which incorporate the EU Standard Contractual Clauses and the UK International Data Transfer Addendum