PageMind Security and Data Protection Overview

Last updated: 2026-07-24

1. Status of this document

This is a public, high-level overview of the security and data-protection boundary for PageMind. It is not a certification, audit report, warranty or service level.

PageMind's actual delivery model, data flows and safeguards depend on the version and arrangement agreed with the customer. Binding commitments exist only in the applicable signed terms, order form and data-processing agreement.

This public document does not publish or imply an application, supplier, model, email, domain, hosting or infrastructure-provider inventory.

2. Data responsibility

Customers remain responsible for deciding what data to submit to PageMind and for having the rights and lawful basis needed to use it.

Customers should:

- submit only data needed for the agreed purpose;
- avoid credentials, payment data and unrelated sensitive data;
- apply their own access, approval and export rules;
- review outputs before operational use; and
- report suspected unauthorised access or disclosure promptly.

Special-category data, criminal-offence data, children's data or other high-risk material must not be submitted unless the applicable written agreement expressly permits it and defines the necessary safeguards.

3. Access and confidentiality

Where INAI processes customer data for PageMind under a signed arrangement:

- access is limited according to the roles and purposes defined for that arrangement;
- people authorised by INAI are subject to confidentiality obligations;
- customer data is used to provide and protect the agreed service, not for an unrelated public purpose; and
- customer-specific access, deletion, return and assistance obligations are governed by the signed agreement.

The public Website does not expose a PageMind customer workspace or publish customer data.

4. Data minimisation and lifecycle

The applicable agreement should identify:

- the categories and purpose of processing;
- the customer and INAI roles;
- the delivery and processing locations, where legally relevant;
- retention, deletion or return criteria;
- any legally required recipient or transfer information; and
- the technical and organisational measures applicable to that customer arrangement.

This public overview does not invent fixed retention periods, data locations, backup schedules, recovery objectives or infrastructure controls for an arrangement that has not been executed.

5. Product outputs and human review

PageMind outputs may be incomplete or inaccurate. Customers must review outputs and source material before publication, procurement, compliance or other consequential use.

Security and privacy controls do not convert generated output into verified fact and do not replace customer approval, quality control or legal review.

6. Incident and legal obligations

If a signed customer arrangement applies, incident assessment, cooperation and any required notification are handled under that agreement and applicable law.

This public page does not promise an acknowledgement, investigation, remediation or update timeline.

7. Reporting a security issue

Potential PageMind security issues may be reported to the inAi team at security@inai.world.

A report should include, where safe:

- the affected version or function;
- reproduction steps;
- observed and expected behaviour;
- potential impact; and
- non-sensitive supporting material.

Do not send credentials, private keys, access tokens, customer data belonging to another party or destructive proof.

INAI does not promise a public bounty or public credit.

8. Related documents

- PageMind Terms
- PageMind Data Processing Agreement template
- PageMind Acceptable Use Policy
- Global Privacy Policy

Privacy questions may be sent to the inAi team at privacy@inai.world.