PageMind Data Processing Agreement

Last updated: 2026-07-24

1. Status and application

This Data Processing Agreement (“DPA”) is a public contractual template. It does not take effect merely because it is published.

It applies only when:

1. INAI and a customer have entered into a written agreement for PageMind (the “Principal Agreement”);
2. INAI processes personal data on that customer’s behalf as a processor; and
3. the Principal Agreement incorporates this DPA or the parties sign an equivalent version.

Customer-specific processing, delivery, security, location and transfer details must be identified in the Principal Agreement, an order form or an executed annex before the relevant processing begins.

This public template does not describe or publish an infrastructure, supplier, model or sub-processor inventory.

2. Parties and roles

The “Customer” is the entity identified in the Principal Agreement. The “Processor” is:

> **INAI**
> Société par actions simplifiée à associé unique (SASU)
> Registered with the RCS Lille Métropole under number **987 977 386**
> Registered office: **142 rue d’léna, apt. 21, 59000 Lille, France**

For processing covered by this DPA:

- Customer acts as controller or as a processor acting for another controller; and
- INAI acts as Customer’s processor or sub-processor, as applicable.

Each party remains responsible for the obligations that data-protection law assigns to its role.

3. Definitions

“Applicable Data Protection Law” means the GDPR and other binding data-protection law applicable to the processing.

“Customer Personal Data” means personal data processed by INAI on Customer’s behalf under the Principal Agreement.

“Data Subject”, “personal data”, “processing”, “controller”, “processor” and “personal data breach” have the meanings given by Applicable Data Protection Law.

“Sub-processor” means another processor engaged by INAI to process Customer Personal Data for the agreed PageMind service.

4. Processing details

The Principal Agreement or an executed annex must define the processing details required by Article 28 GDPR, including:

- subject matter and purpose;
- nature of the operations;
- duration;
- categories of personal data;
- categories of data subjects; and
- Customer’s documented instructions.

The parties do not assume that special-category data, criminal-offence data or children’s data is included. Such data may be processed only where the written agreement expressly identifies it, establishes a lawful basis and defines additional safeguards.

Customer must not submit data beyond the agreed scope.

5. Documented instructions

INAI will process Customer Personal Data only:

- on Customer’s documented instructions;
- as needed to perform the Principal Agreement; or
- where Union or Member State law requires processing, in which case INAI will inform Customer before processing unless the law prohibits that information.

INAI will promptly inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Law. INAI may suspend the affected instruction while the parties address the issue.

6. Confidentiality and authorised persons

INAI will ensure that persons authorised to process Customer Personal Data:

- are bound by confidentiality obligations;
- receive access only where needed for the agreed work; and
- process the data only under applicable instructions.

Customer is responsible for controlling its own users, credentials, source data and permissions.

7. Security

INAI will implement technical and organisational measures appropriate to the risk as required by Article 32 GDPR.

The measures applicable to a specific PageMind arrangement must be documented in the Principal Agreement or an executed security annex. They may address, as relevant:

- access control and authentication;
- confidentiality and personnel access;
- transmission and storage protection;
- separation and minimisation;
- logging and traceability;
- vulnerability and change management;
- availability, backup and recovery;
- incident management; and
- deletion or return.

This public template does not claim a particular hosting model, provider, data-centre location, encryption implementation, backup cycle, recovery objective, certification or audit result.

Customer acknowledges that security obligations are shared. Customer must use PageMind lawfully, protect its access methods, restrict submitted data and review outputs before consequential use.

8. Sub-processors

Customer grants INAI general authorisation to engage a Sub-processor only where one is actually used for Customer Personal Data under the executed arrangement.

Where Applicable Data Protection Law requires it, INAI will:

- provide the required identity, location and processing-function information directly to Customer through the contractual notice channel;
- impose data-protection obligations no less protective than the relevant obligations in this DPA; and
- remain responsible for the performance of its processor obligations.

The notice method and any reasonable objection mechanism will be stated in the Principal Agreement. This public template does not publish an empty, hypothetical or private provider list.

9. International transfers

The executed agreement must identify processing locations and transfers where legally relevant.

If Customer Personal Data is transferred to a country outside the European Economic Area in a manner governed by Chapter V GDPR, INAI will use a permitted mechanism, such as:

- an adequacy decision;

- approved standard contractual clauses with any required supplementary measures; or
- another mechanism permitted by Applicable Data Protection Law.

INAI will provide Customer with information reasonably necessary to assess the applicable transfer mechanism, subject to protection of confidential and security-sensitive material.

10. Assistance to Customer

Taking account of the nature of the processing and the information available to it, INAI will provide reasonable assistance with:

- requests from Data Subjects;
- security obligations under Articles 32 to 34 GDPR;
- data-protection impact assessments and prior consultation where applicable; and
- information needed to demonstrate compliance with Article 28 GDPR.

Customer remains responsible for responding to Data Subjects and authorities in its role as controller unless the parties agree otherwise.

Assistance that materially exceeds the ordinary service may be subject to agreed fees where permitted by law and the Principal Agreement.

11. Personal data breaches

INAI will notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data.

The notification will provide information reasonably available to INAI that Customer needs for its legal assessment and notifications. Information may be supplied in phases where it is not available at once.

INAI's notice does not by itself constitute an admission of fault or liability.

12. Return and deletion

At the end of the relevant services, INAI will, at Customer's choice, delete or return Customer Personal Data and delete remaining copies, unless applicable law requires retention.

The practical method, scope and any limited backup handling must be defined for the actual delivery arrangement. INAI will not actively use retained data except for the legally permitted purpose.

13. Audit and evidence

INAI will make available information reasonably necessary to demonstrate compliance with this DPA.

Where required by Article 28 GDPR, Customer may request a proportionate audit or inspection. The parties will first use available documentation and remote evidence where those means are sufficient. Any further audit must:

- be reasonably scoped and scheduled;

- protect other customers, confidential information and system security;
- avoid unnecessary disruption; and
- comply with the Principal Agreement and Applicable Data Protection Law.

14. Customer obligations

Customer represents that:

- its instructions are lawful;
- it has provided required information to Data Subjects;
- it has an applicable legal basis;
- it will not submit data outside the agreed scope; and
- its users will comply with the Principal Agreement and acceptable-use rules.

Customer is responsible for the accuracy, quality and legality of Customer Personal Data and for deciding whether PageMind is appropriate for its intended use.

15. Conflict, liability and term

If this DPA conflicts with the Principal Agreement on the protection of Customer Personal Data, this DPA prevails to the extent of that conflict. Mandatory law prevails over both.

Liability is governed by the Principal Agreement except where Applicable Data Protection Law does not permit the relevant limitation.

This DPA remains in force for as long as INAI processes Customer Personal Data under the Principal Agreement.

16. Contact

Data-protection questions concerning this template may be sent to the inAi team at privacy@inai.world.

The signed Principal Agreement must identify the parties and the applicable contractual notice channel.