Sub-processor list for PageMind

Sub-Processor List and Engagement Principles for PageMind

Last updated: 2025-12-08

Version: 0.1
Last updated: [●]
Publisher: INAI SASU, 142 rue d'Iéna, 59000 Lille, France

---

1. Purpose and Scope of this Document

1.1 **Purpose**
This document describes the third-party service providers that INAI SASU ("**inAi**", "**we**", "**us**") may engage as **sub-processors** when providing the PageMind service ("**PageMind**") to its business customers ("**Customers**"). It also sets out the principles, safeguards, and notification mechanisms that govern our use of such sub-processors.

1.2 **Scope**
a) This document applies solely to PageMind, i.e. to the catalog operations automation and related services described in the applicable master agreement, order form, or online terms between inAi and the Customer (collectively the "**Agreement**").
b) It covers sub-processors that may process **Customer Personal Data** on our behalf for the purpose of delivering, securing, monitoring, supporting, or improving PageMind, in the role of processor as defined under the EU General Data Protection Regulation ("**GDPR**"). ([GDPR][1])
c) This document is intended to complement the **Data Processing Agreement** ("**DPA**") concluded between inAi (as processor) and the Customer (as controller). In the event of conflict between this document and the DPA or Agreement, the DPA and Agreement shall prevail.
d) This document does **not** apply to:

- Third-party systems that Customers choose to connect to PageMind on their own responsibility (e.g. their own PIM, MDM, or data warehouse), or
- Providers engaged directly by Customers as independent controllers or processors.

e) This document covers third-party providers that may process **Customer Personal Data** in connection with PageMind. Vendors that process only inAi's own HR, finance, or marketing data, or that process solely anonymised or aggregated technical data which does not relate to an identified or identifiable individual, are generally **not** treated as sub-processors for the purposes of this document.

1.3 **Contractual status**

This sub-processor list is provided primarily for transparency and to describe inAi's standard practices. By itself, it does not create new contractual rights or obligations. Where and to the extent the **DPA** or the **Agreement** expressly incorporates this document by reference, the rights and obligations described here shall apply between inAi and the Customer, subject always to the DPA and the Agreement. In case of conflict, the DPA and the Agreement prevail.
In the event of any inconsistency between this document and the DPA or Agreement regarding the engagement of sub-processors, the DPA and Agreement shall prevail.

---

2. Definitions

For the purposes of this document:

2.1 **"Controller", "Processor", "Sub-processor", "Personal Data", "Processing", "Supervisory Authority"** and **"Third Country"** shall have the meanings given in the GDPR. ([GDPR][1])

2.2 **"Customer"** means the legal entity that has entered into an Agreement with inAi for the use of PageMind and that qualifies as controller (or, where applicable, as processor on behalf of another controller) in respect of Customer Personal Data processed through PageMind.

2.3 **"Customer Personal Data"** means any personal data (as defined in GDPR) that is:

- Input into PageMind by the Customer or on its behalf (including via uploads, APIs, or integrations);
- Derived from such data as part of PageMind's processing (e.g., intermediate representations, embeddings, audit logs where these contain personal data); or
- Otherwise processed by inAi on behalf of the Customer for the purposes of providing PageMind.

2.4 **"Sub-processor"** means any third-party processor engaged by inAi who may have access to Customer Personal Data in order to support the provision of PageMind.

2.5 **"EU SCCs"** means the Standard Contractual Clauses adopted by the European Commission under Decision (EU) 2021/914 for the transfer of personal data to third countries. ([EUR-Lex][2])

2.6 **"EEA"** means the European Economic Area (EU Member States plus Iceland, Liechtenstein and Norway).

---

3. Roles and Responsibilities

3.1 **Customer as Controller**
In the context of PageMind, the Customer is typically the controller (or a processor acting on behalf of its own controller) with respect to Customer Personal Data. The Customer determines the purposes and means of processing such data (for example, which documents to upload, which product catalog schemas to use, and which users may access PageMind).

3.2 **inAi as Processor**
a) inAi processes Customer Personal Data solely on behalf of the Customer and in accordance with:

- The Agreement and DPA;
- The Customer's documented instructions as set out therein; and
- Applicable data protection law.
  b) inAi does not determine independent purposes for which Customer Personal Data is processed in the context of PageMind; the Customer remains responsible for defining the business purposes and essential means of processing.
  inAi will not use Customer Personal Data to train generally available foundation models or for unrelated analytics. Any limited use of Customer Personal Data that is necessary to **provide, maintain, secure and improve PageMind** (for example, to generate aggregated or de-identified statistics on service performance and reliability) will:
    - be carried out strictly in accordance with the DPA and the Customer's documented instructions; and
    - where technically and commercially feasible, rely on anonymisation, pseudonymisation, or other data minimisation techniques and will not involve attempts to re-identify data subjects.

3.3 **Sub-processors engaged by inAi**
a) When inAi engages sub-processors, we do so solely for the limited purposes necessary to provide PageMind (hosting, compute, LLM inference, monitoring, support, etc.).
b) Under Article 28(2) GDPR, we will not engage another processor (sub-processor) without prior specific or general written authorisation of the Customer. ([GDPR][1])
c) Where the **DPA** provides that the Customer grants inAi a **general written authorisation** to engage sub-processors and establishes a right to object, this document and its updates describe how inAi will provide information on sub-processors and operationalise that mechanism (see section 11).

3.4 **Liability**
The allocation of liability between inAi and the Customer, including in respect of

sub-processors, is governed exclusively by the DPA and the Agreement. This document does not modify such allocation.

---

4. Data Types and Processing Operations Relevant to Sub-Processors

4.1 **Categories of data subjects**
Depending on the Customer's use of PageMind, Customer Personal Data may relate to:
a) Customer's employees, contractors, or other staff members who use PageMind (user accounts, workspace membership, audit logs);
b) Customer's suppliers' or partners' staff whose contact details or names may appear in supplier documents uploaded to PageMind;
c) Other identifiable individuals whose data may incidentally appear in the documents that Customer chooses to process (for example, names embedded in product manuals, certificates, or invoices).

PageMind is designed and marketed primarily for **B2B catalog data** (products, attributes, descriptions) and is **not** intended to systematically process special categories of personal data or large volumes of consumer data.

4.2 **Categories of Customer Personal Data processed by sub-processors**
Depending on the service provided, sub-processors may process some or all of the following data categories:
a) **Account and identification data** – user identifiers, usernames, email addresses, hashed passwords or authentication tokens, role or group membership.
b) **Contact and organisation data** – business contact details, employer, role, metadata that links users to workspaces or projects.
c) **Content data** – copies or representations of supplier files (PDFs, images, DOCX, CSV, etc.), intermediate text extracted via OCR, embeddings and structured representations that may sometimes contain personal data, and generated catalog outputs where personal data appears in source content.
d) **Technical and usage data** – IP addresses, device identifiers, browser type, timestamps, log entries, error traces, performance metrics, and other telemetry necessary for security, monitoring, and capacity planning.
e) **Support data** – information contained in support requests, screenshots, debug archives, and related logs shared when Customers seek assistance.

4.3 **Restricted categories of data**
a) PageMind is **not designed** for the intentional processing of:

- Special categories of personal data under Article 9 GDPR (health data, biometric identifiers for unique identification, political opinions, religion, etc.);
- Personal data relating to criminal convictions and offences;

- Children's data as a primary data set.
  b) Customers are responsible for ensuring that they do not upload such data unless:
- This is strictly necessary for their use case; and
- A valid legal basis and appropriate safeguards exist under applicable law.
  c) inAi reserves the right to take appropriate technical or contractual measures (including deletion, filtering, and suspension) if we reasonably believe that PageMind is being used in a way that materially increases risk to individuals' rights and freedoms beyond the intended B2B catalog context.
  d) inAi does not proactively monitor Customer uploads to detect special categories of personal data, criminal data, or children's data. However, if such use is brought to our attention or we reasonably suspect it based on available information (for example, in the course of support or incident handling), we may review relevant content solely as necessary to assess the situation and take appropriate measures as described above.

---

5. Principles Governing Engagement of Sub-Processors

5.1 **Equivalence of protection**
Before engaging any sub-processor, inAi will:
a) Execute a written contract with the sub-processor that imposes data protection obligations **at least equivalent in substance** to those set out in the DPA and in Article 28(3) GDPR, taking into account the nature of the services provided by the sub-processor. ([GDPR][1])
b) Require the sub-processor to process Customer Personal Data only on documented instructions from inAi and solely for the purposes of providing the contracted services.
c) Require the sub-processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where relevant and proportionate, measures such as encryption in transit, access control, and incident response procedures.

5.2 **Due diligence and risk assessment**
inAi conducts an **initial** and, where appropriate, **risk-based periodic** assessment of each sub-processor, taking into account: ([complydog.com][3])
a) The nature, scope, context, and purposes of processing;
b) The categories and volume of Customer Personal Data processed;
c) The geographical location(s) of storage and access, including any transfers to Third Countries;
d) The sub-processor's security posture (for example, certifications, publicly available or contractual security documentation, penetration test summaries, and incident response processes); and
e) The sub-processor's own sub-processing chain, where relevant.

inAi may rely on independent third-party audit reports, certifications, or similar attestations where direct audits would be disproportionate or not contractually available.

5.3 **Onward transfers and international data flows**
a) Where a sub-processor is located outside the EEA or where data access from a Third Country cannot be excluded, inAi will ensure that appropriate safeguards are in place under Chapter V GDPR, such as:

- EU SCCs (controller-to-processor or processor-to-processor modules, as applicable); ([EUR-Lex][2])
- Reliance on an adequacy decision of the European Commission (including, where applicable, the EU-US Data Privacy Framework); or
- Other lawful transfer mechanisms as permitted by GDPR.
  b) Where required under Chapter V GDPR and relevant supervisory guidance, inAi will perform and document a **transfer impact assessment (TIA)** to evaluate whether the laws and practices of the recipient Third Country may affect the effectiveness of the safeguards, and will implement supplementary measures where appropriate in light of that assessment.

5.4 **Confidentiality and access control**
a) Sub-processors are required to ensure that any person they authorise to process Customer Personal Data is bound by confidentiality obligations and receives appropriate data protection training.
b) Access to Customer Personal Data is limited to personnel with a strict need-to-know for the performance of the relevant services and is subject to role-based access control and logging.

5.5 **Audit and oversight**
Where contractually feasible and appropriate to the nature of the service, inAi **seeks to**:

a) Receive and, where relevant, review information from sub-processors about their security and privacy controls (for example, ISO 27001 or SOC 2 reports, penetration test summaries, or security whitepapers);
b) Reserve contractual rights to rely on, or request access to, independent audit reports or other verification mechanisms, subject to reasonable notice and confidentiality restrictions; and
c) Require prompt notification of any actual or suspected personal data breach affecting Customer Personal Data, together with appropriate cooperation as described in the DPA.

---

6. Categories of Sub-Processors

The categories below, and the sub-processors listed in section 7, represent providers that **may** be involved in processing Customer Personal Data for PageMind. Not every Customer

or workspace will rely on every sub-processor; actual usage depends on configuration, selected features, and the evolution of inAi's infrastructure.

6.1 **Infrastructure and hosting providers**
Third-party providers that supply data centres, compute, storage, networking, and related infrastructure on which PageMind runs (e.g. public cloud or European IaaS providers).

6.2 **AI / Large Language Model (LLM) and ML providers**
Vendors that provide LLM and other ML inference services used by PageMind to perform OCR, structured extraction, translation/localisation, attribute normalisation, and text generation, where such services may process Customer Personal Data contained in documents or logs.

6.3 **Observability, logging, and monitoring tools**
Services used to collect and process technical logs, metrics, and traces in order to monitor performance, detect anomalies, and investigate incidents. Where possible, these tools operate primarily on metadata and pseudonymised content; however, limited personal data may appear in logs.

6.4 **Email, messaging, and notification services**
Providers used to send transactional emails and other notifications to Customer users (e.g. account creation, password reset, run completion notifications). These providers typically process user email addresses and limited message content.

6.5 **Support and ticketing platforms**
Helpdesk tools used to handle Customer support requests, which may contain personal data included in tickets, attachments, or debug logs.

6.6 **Business operations and billing tools**
Where PageMind contractual and billing processes are handled through external platforms (e.g. invoicing systems, CRM), limited Customer Personal Data (such as business contact details and billing contact information) may be processed.

6.7 **Security and anti-abuse tools**
Tools used for threat detection, DDoS protection, web application firewalls, spam filtering, and abuse detection. These tools may process IP addresses, device fingerprints, and log data, and may operate at the edge of the network.

---

7. Current Sub-Processor List for PageMind

The table below lists the third-party sub-processors that may process Customer Personal Data in connection with PageMind at the date indicated in the version history of this document.

- Not every Customer or workspace will use every sub-processor; some are used only for specific features or configurations, as indicated in the "Notes" column.

- The inclusion of a sub-processor in this list does not guarantee that it currently processes Customer Personal Data for a given Customer; it indicates that the provider **may** be used during the term of the Agreement.
- Before appointing any new sub-processor, inAi follows the principles described in section 5 and, where applicable, the notice and objection mechanism described in section 11.

The composition of the sub-processor ecosystem may change over time as inAi evolves PageMind's infrastructure and feature set. The presence or absence of a specific provider in this list does not guarantee that a particular feature will be available, or that a provider will be used for the entire duration of the Agreement.

The inclusion of a provider in this list does not guarantee that such provider will be used for the entire duration of the Agreement, nor that all listed providers are currently active at any given time.

7.1 **Infrastructure and hosting**

Sub-processor	Role / Service	Data Categories	Primary Processing Location(s)	International Transfers & Safeguards	Notes
[EU Cloud Provider A] (e.g. Scaleway / OVHcloud)	Primary infrastructure hosting for PageMind (compute, storage, networking, managed databases)	Content data, account data, technical and usage data, support data where stored in backups	EU/EEA (specific data centre regions to be specified)	Customer Personal Data is intended to be hosted in **EEA data centres** selected by inAi for PageMind workloads. Limited remote access from outside the EEA may occur for support, maintenance, or resilience purposes under the provider's standard terms. Where such access	Main EU VPC for PageMind workloads (production and staging)

Sub-processor	Role / Service	Data Categories	Primary Processing Location(s)	International Transfers & Safeguards	Notes
				involves a Third Country, appropriate safeguards (such as SCCs, adequacy decisions, and, where required, TIAs and supplementary measures) are used.	
[Global Cloud Provider B] (e.g. AWS, Azure, GCP)	Supplementary infrastructure, specialised services (e.g. GPU workloads, backup, or specific managed services)	Same as above where used	EU regions (e.g. eu-west-●, westeurope), plus any additional regions explicitly configured	If support or failover involves Third Country access, EU SCCs and/or adequacy decision (e.g. EU-US DPF) applied; TIAs and supplementary measures as needed	Used selectively where required for specific workloads or resilience

7.2 **AI / LLM and ML providers**

Sub-processor	Role / Service	Data Categories	Primary Processing Location(s)	International Transfers & Safeguards	Special Conditions
[EU LLM Provider] (e.g. Mistral / other EU-based vendor)	LLM inference for structured extraction,	Content data (portions of supplier files and intermediate representations that may	EU/EEA data centres as described in the provider's documentation	inAi configures the service to use EU/EEA regions where this is supported. The provider's	Contractual "no training on Customer data" commitments; strict retention

Sub-processor	Role / Service	Data Categories	Primary Processing Location(s)	International Transfers & Safeguards	Special Conditions
	translation, and generation tasks for PageMind	incidentally contain personal data)		support or operations personnel may, in limited circumstances, access Customer Personal Data from outside the EEA for maintenance or troubleshooting; such access is governed by appropriate safeguards (for example, SCCs) under the provider's DPA.	limits; encryption in transit; access control
[Global LLM Provider 1] (e.g. OpenAI, Anthropic, etc.)	Additional LLM inference for tasks where non-EU models are selected by inAi or agreed in writing with Customer	Same as above (content data; possibly pseudonymised or minimised)	**Global / United States.** (Customer acknowledges that use of these specific models involves processing outside the EEA. Appropriate transfer mechanisms are in place).	Transfers governed by EU SCCs and/or adequacy mechanisms with TIAs and supplementary measures; use restricted to configurations explicitly agreed with Customer where required	Provider contracts and configuration must ensure: (i) no training on Customer data by default, (ii) limited retention, (iii) appropriate security and access controls. Default PageMind configuratio

Sub-processor	Role / Service	Data Categories	Primary Processing Location(s)	International Transfers & Safeguards	Special Conditions
					ns are designed to prioritise EU-based or EU-hosted LLM providers where technically and commerciall y feasible. This global provider is used only for specific features or configuratio ns where such use has been selected by inAi for technical reasons or expressly agreed with the Customer.

7.3 **Observability, logging, and monitoring**

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards	Notes
[EU Monitoring Provider]	Metrics, traces, and logs for infrastructur e and application performanc	Technical/usag e data; limited pseudonymise d identifiers; in rare cases, fragments of content data	Primary processing in EU/EEA data centres where available; limited	SCCs or other Chapter V mechanism s for any Third Country	Logging configuratio n aims to avoid storing raw document content;

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards	Notes
	e	appearing in logs	access from other regions may occur in line with the provider's standard infrastructure	access; log minimisation and retention limits; access restricted to authorised operations staff	access restricted to operations staff
[Global Error Tracking Provider]	Error reporting and exception tracking	Same as above	Primary processing in EU/EEA region where available; error telemetry may be routed or accessed from other regions as part of the provider's global infrastructure	SCCs and other Chapter V mechanisms as applicable; configuration aims to minimise sensitive payloads; access restricted to authorised personnel	Used to debug failures and improve stability; sensitive payloads minimised where feasible

7.4 **Email, messaging, and notification services**

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards
[Transactional Email Provider]	Delivery of transactional emails (account creation, password reset, run notifications)	User email addresses; message meta-data; limited message content	Primary processing in EU/EEA data centres where available; routing and delivery may involve other regions as part of the provider's global email	SCCs/adequacy for any Third Country routing; TLS in transit; DKIM/SPF for email integrity

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards
			infrastructure	

7.5 **Support, ticketing, and collaboration**

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards
[Support Desk Platform]	Ticketing and support management	Account/contact data; contents of support tickets; optional attachments that may include content data	Primary processing in EU/EEA data centres where available; support staff in other regions may access data for troubleshooting in line with the provider's standard support model	SCCs and TIAs if applicable; access restricted to authorised support staff; retention controlled by inAi

7.6 **Business operations and billing**

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards
[Billing / Invoicing Provider]	Invoicing, subscriptions, and payment collection for B2B customers	Billing contact details; organisation identifiers; invoice data	Primary processing in EU/EEA where offered; some processing or support access may occur from other regions in line with the provider's infrastructure	SCCs and/or adequacy for any Third Country access; encryption and access controls
[CRM Provider]	Management of leads and customer accounts	Business contact data; limited notes regarding relationship	As per provider's regional settings (with EU/EEA regions selected where available); some processing or support access may occur from other regions	SCCs/adequacy and internal access restrictions

7.7 **Security and anti-abuse**

Sub-processor	Role / Service	Data Categories	Location(s)	Safeguards
[Edge Protection / CDN Provider] (e.g. Cloudflare or similar)	DDoS protection, TLS termination, edge caching, WAF	IP addresses; HTTP request data; device and browser metadata; cookies where applicable	Primary processing in EU/EEA data centres where feasible, with delivery across a global edge network; routing, caching, or support access from other regions may occur in line with the provider's standard infrastructure	SCCs/adequacy as applicable; encryption in transit; configurable retention of logs; strict access control

8. International Data Transfers

8.1 **General approach**
a) inAi's preferred default is to keep processing of Customer Personal Data within the EEA using EU-based infrastructure and EU-hosted services where technically and commercially feasible.
b) However, due to the use of globally distributed networks, specialised AI providers, monitoring systems, and security services, certain processing operations may involve transfers of Customer Personal Data to Third Countries or remote access from such locations. While inAi aims to keep primary processing within the EEA where feasible, temporary or limited processing or access from outside the EEA may still occur under the safeguards described in section 8.2 (for example, in the context of support, disaster recovery, or use of global security networks).

8.2 **Safeguards for Third Country transfers**
Where such transfers occur, inAi will:
a) Rely on appropriate transfer mechanisms recognised under GDPR (e.g. SCCs, adequacy decisions such as EU-US DPF, or other lawful mechanisms); ([European Commission][4])
b) Perform TIAs where appropriate and, where necessary, implement supplementary technical and organisational measures (such as encryption, strict access control, and data minimisation);
c) Periodically, and in light of **material legal or regulatory developments** that become known to inAi in the ordinary course of its business, review its approach to international data transfers and make reasonable adjustments where necessary to maintain an appropriate level of protection.

8.3 **Customer options**
Where the then-current version of PageMind technically supports it and where commercially reasonable, inAi **may** offer configuration options that allow Customers to:

a) Restrict or disable the use of certain non-EU sub-processors (for example, specific LLM providers) for their workspaces; and/or
b) Select processing modes that aim to keep Customer Personal Data within the EEA, with any functional, performance, or cost implications documented in the relevant product documentation or Agreement.

Any such options, if available, are described in the applicable product documentation or agreed in writing between inAi and the Customer.

---

9. AI / LLM-Specific Safeguards

Given the particular sensitivities associated with AI and LLM providers, inAi applies additional controls when using such sub-processors: ([StartupSoft][5])

9.1 **No training on Customer data by default**
inAi's policy is to use AI/LLM providers whose enterprise offerings and configuration options allow inAi to ensure that Customer Personal Data submitted through PageMind is **not** used to train or improve the provider's generally available foundation models by default.

Accordingly, inAi will, by default:
a) Configure such services (via "Zero Data Retention" or Enterprise settings where available) so that prompts and outputs are not used for training; and
b) Avoid sending Customer Personal Data to AI/LLM services that do not offer a reasonable way to disable such training, **unless**:

- the Customer has given prior written instructions or consent for that specific use; and
- appropriate legal bases, safeguards, and transparency measures are in place.

Nothing in this section prevents inAi from using models that are trained on **other customers'** or public data, provided that Customer Personal Data from PageMind is not used to train those models without such explicit agreement.

Any exception to the default "no training on Customer data" position will always require a separate written agreement with the relevant Customer, which will describe the specific purposes, safeguards and legal bases for such training.

9.2 **Minimisation and redaction**
a) Where feasible, PageMind's orchestration layer minimises the amount of Customer Personal Data sent to LLM providers, e.g. by:

- Restricting prompts to relevant product segments;
- Redacting obvious personal identifiers where the task does not require them.
  b) For catalog-only use cases, PageMind can operate predominantly on product attributes and descriptions rather than on free-form personal data.

9.3 **Stability, logging, and auditability**
a) PageMind is designed so that key processing steps and configurations (including models used, configuration signatures, and environment fingerprints) are logged, enabling inAi and the Customer to **reconstruct and explain** how particular outputs were produced. While some AI outputs may inherently vary between runs, the underlying pipeline, inputs, and configuration can be traced for audit and troubleshooting purposes.
b) AI/LLM sub-processors are not given unrestricted access to such logs; they see only what is necessary for inference and stability of their service.

9.4 **High-risk use cases under AI regulation**
PageMind is not intended to be used as a high-risk AI system under the EU AI Act (e.g. for employment, credit scoring, or biometric identification). ([Artificial Intelligence Act][6])
If a Customer contemplates such use, this must be the subject of a separate written agreement and risk assessment, including a review of sub-processors and their specific obligations under applicable AI regulation.

The Customer is responsible for assessing whether its use of PageMind forms part of a system that qualifies as **high-risk** under the EU Artificial Intelligence Act or other sector-specific regulation, and for implementing any associated organisational and technical measures. inAi does not provide legal advice and does not assume the Customer's regulatory obligations as deployer or provider of a high-risk AI system, unless expressly agreed in a separate written agreement.

---

10. Security Measures Applied by Sub-Processors

10.1 **Baseline expectations**
Each sub-processor engaged by inAi must implement security controls that are at least industry-standard and appropriate to the risk, such as:
a) Encryption in transit (e.g. TLS) and at rest where applicable;
b) Logical separation of customer environments and data;
c) Access control based on least privilege with multi-factor authentication for privileged access;
d) Logging and monitoring of access to systems processing Customer Personal Data;
e) Regular vulnerability management and patching;
f) Incident detection, response, and notification procedures.

10.2 **Certifications and independent audits**
Where available and relevant, we prefer sub-processors that can demonstrate their security posture via:

a) ISO/IEC 27001 certification or equivalent;
b) SOC 2 Type II reports or similar third-party audit reports;
c) EU cloud compliance frameworks or national schemes, where applicable.

10.3 **Alignment with inAi's security programme**
Sub-processor security controls must be compatible with inAi's own security and privacy architecture, including our EU-focused data residency approach, audit logging, and incident-handling workflows as described in our Legal and Security documentation.

---

11. Notification of New Sub-Processors and Right to Object

11.1 **General authorisation and updates**
a) Where and to the extent the **DPA** provides that the Customer grants inAi a **general written authorisation** to engage sub-processors in accordance with Article 28(2) GDPR, such authorisation is implemented in line with this section 11. If the DPA instead requires **specific authorisation**, the notice and objection mechanics in this section apply only to the extent they are consistent with that mechanism. ([GDPR Local][7])
b) This document (or an equivalent sub-processor list referenced in the DPA) will be maintained on an accessible webpage. inAi may update it from time to time to reflect additions, replacements, or removals of sub-processors.

11.2 **Notification mechanism**
a) For material changes, such as the addition of a new sub-processor that may process Customer Personal Data, inAi will provide advance notice to Customers by:

- Updating this document; and
- Sending an email or platform notice to the designated contact (where the Customer has opted in to such notifications),

within a reasonable notice period (**usually at least 30 days before** the sub-processor becomes active for PageMind workloads), where this is reasonably practicable and unless earlier use is required for urgent security, resilience, or continuity reasons as described below.
b) For emergency additions motivated by security, incident response, or continuity of service, inAi will notify Customers as soon as reasonably practicable thereafter.

11.3 **Customer right to object**
a) Within the notice period specified in the DPA (for example **30 days**), the Customer may object in writing to the engagement of a new sub-processor on reasonable, documented data protection grounds.
b) Upon receiving such an objection, inAi will:

- Discuss the objection in good faith with the Customer and attempt to identify a commercially reasonable alternative;

- Where no alternative is feasible without unreasonable cost or material degradation of the services, inform the Customer of any options available under the DPA and the Agreement (such as disabling relevant features, creating a separate processing environment, or allowing the Customer to suspend or terminate the **affected services** in accordance with the termination and refund terms already set out in the Agreement).
  c) Failure to object within the notice period shall be deemed to constitute acceptance of the new sub-processor.

---

12. Customer Responsibilities

12.1 **Lawful basis and transparency**
The Customer is responsible for:
a) Ensuring that it has a valid legal basis for processing Customer Personal Data through PageMind and for any instructions it issues to inAi;
b) Providing appropriate privacy notices and transparency information to data subjects, including disclosures concerning the use of processors and sub-processors.

12.2 **Data minimisation and appropriateness of uploads**
The Customer remains responsible for:
a) Uploading only such documents and data to PageMind that are necessary for the intended catalog operations use case;
b) Avoiding the upload of special categories of personal data or other high-risk data types except where strictly necessary and legally justified;
c) Ensuring that any personal data embedded in catalog materials is handled in accordance with applicable law and internal policies.

12.3 **Configuration and access management**
The Customer is responsible for:
a) Configuring access rights and roles for its users within PageMind;
b) Maintaining the confidentiality and security of authentication credentials;
c) Reviewing and responding to notifications about new sub-processors or changes in processing.

12.4 **Third-party integrations**
Where the Customer chooses to connect PageMind to third-party tools, APIs, or data sources under its own control, the Customer is responsible for:
a) Evaluating those third parties;
b) Entering into appropriate data protection agreements with them;
c) Ensuring that any data flows between PageMind and such third parties are lawful and consistent with the DPA.

12.5 **AI regulation and sector-specific obligations**
The Customer is responsible for:

a) Determining whether and how its use of PageMind is subject to specific regulatory frameworks (including, where applicable, the EU Artificial Intelligence Act and sector-specific product or consumer protection rules); and
b) Implementing any additional technical, organisational, or governance measures required by such frameworks in its own environment.

inAi does not provide legal advice and does not assume the Customer's obligations under such frameworks, except where expressly agreed in writing.

---

13. Record-Keeping and Demonstrating Compliance

13.1 **Records of processing**
inAi maintains internal records of processing activities relating to PageMind, including the categories of sub-processors engaged, in order to demonstrate compliance with Article 28 GDPR and related obligations. ([ISMS.online][8])

13.2 **Documentation and evidence**
Upon reasonable request and subject to confidentiality obligations, inAi may provide Customers with additional information reasonably necessary to demonstrate compliance with its obligations relating to sub-processors, including:
a) Links to sub-processor privacy and security documentation;
b) High-level summaries of TIAs;
c) Confirmation of the legal transfer mechanisms in place.

inAi is not obliged to disclose full TIAs, detailed security reports, or other documents where disclosure would infringe the rights or confidentiality obligations of inAi or its sub-processors.

---

14. Amendments to this Document

14.1 **Unilateral updates by inAi**
inAi may update this document from time to time to:
a) Reflect changes in its sub-processor ecosystem;
b) Reflect changes required by law, regulation, or guidance from supervisory authorities;
c) Clarify language or improve transparency, provided such changes do not materially reduce the level of protection afforded to Customer Personal Data.

14.2 **Notification of material changes**
Material changes relating to sub-processors that process Customer Personal Data will be communicated in accordance with section 11 (Notification and Right to Object) and the DPA.

14.3 **Versioning**
Each version of this document will indicate its **version number** and **last updated date**. inAi may keep previous versions available upon request or via an archive for audit and compliance purposes.

---

15. Contact and Further Information

15.1 **Data protection contact**
Questions or concerns regarding this document, inAi's use of sub-processors, or PageMind's data protection practices may be addressed to:

INAI SASU – Data Protection
142 rue d'Iéna, 59000 Lille, France
Email: privacy@inai.fr (data protection contact)

15.2 **Supervisory authority**
Nothing in this document limits the rights of data subjects or Customers to lodge a complaint with a competent supervisory authority or to seek other remedies available under applicable law.

Annex A – Sub-processor Data Sheet Template

This Annex provides a standard template for documenting each Sub-processor engaged in connection with PageMind. The template may be completed and maintained internally by inAi and, where appropriate, made available to Customers subject to confidentiality obligations.

This Annex is primarily an **internal governance tool**; it does not, by itself, create contractual rights or obligations for Customers unless expressly incorporated into the DPA or Agreement.

A.1 Identification

1. **Legal name of Sub-processor:**
2. **Registered address:**
3. **Registration number / corporate ID (if available):**
4. **Website / main contact URL:**
5. **Contractual counterparty (if different from above):**

A.2 Role and Services

1. **Category (as per Section 6 of this document):**
    - ☐ Infrastructure and hosting
    - ☐ AI / LLM / ML provider
    - ☐ Observability, logging, monitoring
    - ☐ Email, messaging, notifications
    - ☐ Support and ticketing
    - ☐ Business operations and billing
    - ☐ Security and anti-abuse
    - ☐ Other (specify): _____
2. **Description of services provided:**
    - Concise description of what the Sub-processor does for PageMind (e.g. "Provides managed compute and storage for production workloads", "Provides LLM inference for attribute extraction and translation", etc.).
3. **Is this Sub-processor mandatory for use of PageMind?**
    - ☐ Yes, used by default for all Customers
    - ☐ No, used only for specific features or configurations (describe): _____
4. **Dependent modules / features:**
    - List of PageMind components or features that rely on this Sub-processor (e.g. "core ingestion pipeline", "Verify.EU module", "run notification emails").

A.3 Data Processing Details

1. **Categories of data subjects affected:**
    - ☐ Customer employees / users
    - ☐ Supplier employees / contacts appearing in documents
    - ☐ Other individuals whose data is contained in uploaded documents (describe): _____
2. **Categories of Customer Personal Data processed:**
    - ☐ Account and identification data (e.g. usernames, email addresses, user IDs)
    - ☐ Contact and organisation data (e.g. business contact details, role, company)
    - ☐ Content data (e.g. copies or excerpts of supplier files, extracted text, embeddings)
    - ☐ Technical and usage data (e.g. IP addresses, logs, request metadata, telemetry)
    - ☐ Support and ticketing data (e.g. contents of support tickets, attachments)

- ☐ Other (specify): _____

3. **Nature and purpose of processing:**
    - Short narrative describing why this Sub-processor processes Customer Personal Data (e.g. “hosting and storage”, “inference on text segments for translation and extraction”, “delivery of transactional emails”).
4. **Frequency of processing:**
    - ☐ Continuous (always on for PageMind workloads)
    - ☐ Event-driven / occasional (e.g. only on support requests, specific batches)
5. **Retention periods under Sub-processor’s control (if known):**
    - Working data: _____
    - Logs / telemetry: _____
    - Backups: _____
    - Notes (e.g. deletion SLAs, configurable retention): _____

A.4 Locations and International Transfers

1. **Primary data centre / processing locations:**
    - Country/Region #1: _____
    - Country/Region #2 (if applicable): _____
2. **Potential access from Third Countries:**
    - List any countries outside the EEA from which staff or systems may access Customer Personal Data (e.g. for support or maintenance): _____
3. **Transfer mechanism(s) for Third Country access:**
    - ☐ EU SCCs (processor-to-processor)
    - ☐ Adequacy decision (specify): _____
    - ☐ Data Privacy Framework participation (if US; specify status): _____
    - ☐ Other mechanism / derogation (describe): _____
4. **Summary of Transfer Impact Assessment (TIA) outcome (internal note):**
    - Risk rating (low/medium/high): _____
    - Key supplementary measures (e.g. encryption, minimisation, access restrictions): _____

A.5 Security and Compliance

1. **Relevant certifications or attestations (if any):**

    ☐ ISO/IEC 27001
    ☐ SOC 2 Type II
    ☐ Other (e.g. local cloud certification, specific schemes): _____
    ☐ None disclosed
2. **Key security measures (summary):**

    - Data at rest encryption: ☐ Yes ☐ No ☐ Unknown
    - Data in transit encryption (TLS): ☐ Yes ☐ No ☐ Unknown
    - Role-based access control: ☐ Yes ☐ No ☐ Unknown
    - Multi-factor authentication for privileged access: ☐ Yes ☐ No ☐ Unknown
    - Logging and monitoring of access to Customer Personal Data: ☐ Yes ☐ No ☐ Unknown
3. **Incident and breach handling:**

    - Contractual obligation to notify inAi without undue delay in case of personal data breach: ☐ Yes ☐ No ☐ Unknown
    - Typical notification timeframe (if stated): _____
4. **Audit and inspection rights:**

    - Mechanism for audits (e.g. third-party reports, on-site audits, questionnaires): _____
    - Frequency and conditions of access to audit materials: _____

A.6 AI / LLM-Specific Controls (where applicable)

(Complete only for AI / LLM / ML Sub-processors.)

1. **Type of models used:**

    ☐ Foundation LLM (general purpose)
    ☐ Task-specific/NLU model
    ☐ OCR / vision model
    ☐ Other (specify): _____
2. **Use of Customer Personal Data for training:**

    - Provider's default position:

        ☐ No training on customer data by default
        ☐ Training by default with opt-out
        ☐ Training by default with no opt-out

- Configuration chosen by inAi: _____

3. **Retention of prompts and outputs:**
    - Stated maximum retention period: _____
    - Ability to configure shorter retention / no retention: ☐ Yes ☐ No
4. **AI-specific documentation available:**

    ☐ Model cards / transparency reports
    ☐ Safety and risk documentation (e.g. alignment, misuse policies)
    ☐ Copyright / content provenance statements
    ☐ None provided / not applicable

A.7 Contractual Terms with inAi

1. **Date of initial engagement:** _____
2. **Key contractual documents:**
    - Data processing agreement or addendum: ☐ Yes ☐ No
    - Security schedule / annex: ☐ Yes ☐ No
    - AI-specific addendum (if any): ☐ Yes ☐ No
3. **Pass-through of obligations:**
    - Confidentiality obligations: ☐ Aligned with inAi DPA ☐ Additional ☐ Weaker (requires mitigation)
    - Assistance obligations (e.g. data subject rights, DPIAs): ☐ Adequate ☐ Needs monitoring
4. **Renewal / termination terms relevant to data:**
    - Term and renewal conditions: _____
    - Data deletion/return obligation on termination: _____

A.8 Risk Assessment and Status (Internal Use)

1. **Overall risk level:**

    ☐ Low
    ☐ Medium
    ☐ High
2. **Key identified risks:**

---

3. **Mitigating measures implemented by inAi:**
    - Technical (e.g. minimisation, encryption, segregation): _____
    - Organisational (e.g. limited features, restricted access, compensating controls): _____
4. **Next review date:** _____
5. **Owner at inAi (name/role):** _____

Annex B – Sub-processor Change Log (Template)

This Annex provides a suggested structure for recording historical changes to the Sub-processor ecosystem. It may be maintained as an internal register and, where appropriate, summarised for Customers.

This Annex is intended as an **internal change log template**. It may be maintained by inAi for record-keeping purposes and, where appropriate, summarised for Customers, but it does not itself form part of the Agreement unless expressly referenced therein.

Version	Effective Date	Type of Change	Sub-processor(s) Affected	Category	Description of Change	Customer Impact / Actions	Notes
0.1	[dd/mm/yyyy]	Addition	[Name]	Hosting	Added as primary EU infrastructure provider for PageMind production workloads	Customers notified by email on [date]; objection window [X] days	—
0.2	[dd/mm/yyyy]	Replacement	[Old] → [New]	LLM	Replaced legacy LLM provider with new EU-based LLM provider for attribute extraction	No config change required for Customers; optional opt-out available	—

Version	Effective Date	Type of Change	Sub-processor(s) Affected	Category	Description of Change	Customer Impact / Actions	Notes
0.3	[dd/mm/yyyy]	Removal	[Name]	Logging	Retired legacy logging service, no longer processes Customer Personal Data	No impact; service disabled and data deleted per contract	—
0.4	[dd/mm/yyyy]	Location change	[Name]	Hosting	Added new EU region; disabled non-EU region for PageMind workloads	Data residency improved; no action required	—
0.5	[dd/mm/yyyy]	Policy change	[Name]	LLM	Provider changed data-retention defaults; configuration updated to maintain “no training” and minimal retention	Customers informed; technical configuration verified	—

For each entry, inAi should ensure that:

1. The **Type of Change** is clearly indicated (Addition, Replacement, Removal, Location change, Policy change, etc.).
2. The **Description of Change** is specific enough to understand what has been modified in practice.
3. The **Customer Impact / Actions** column clearly states whether Customers need to take any action or whether the change is transparent, and how the right to object has been offered (where applicable).

4. The **Notes** field is used to reference internal tickets, TIAs, or approval records, without exposing confidential information.