PageMind Acceptable Use Policy (AUP)

Last updated: 2025-12-08

1. Purpose, Scope and Relationship with Other Terms

1.1. This PageMind Acceptable Use Policy ("**AUP**") sets out the rules and restrictions that apply to any access to and use of the PageMind service and its related modules and interfaces (together, the "**Services**"). PageMind is operated by INAI, a French société par actions simplifiée (SASU) with its registered office in Lille, France ("**inAi**", "**we**", "**us**").

1.2. This AUP forms part of, and is incorporated by reference into, the applicable agreement between inAi and the relevant customer entity (the "**Agreement**"), such as:

- online Terms of Service accepted on the PageMind website; and/or
- a signed Master Service Agreement, order form or pilot agreement.

1.3. **Relationship with the Agreement and other documents.** This AUP forms part of, and is incorporated into, the Agreement. In the event of any direct conflict between this AUP and the Agreement, the Agreement will prevail. For issues relating to the processing of personal data, the applicable data-processing agreement and privacy documentation will prevail over this AUP. In case of conflict between this AUP and the Documentation, this AUP will prevail.

1.4. This AUP applies to:

- the **Customer** that enters into the Agreement with inAi;
- all of Customer's employees, contractors and other persons to whom Customer grants access to the Services ("**Authorised Users**"); and
- any third party that uses the Services on Customer's behalf or under Customer's account.

1.5. Customer is responsible for ensuring that all Authorised Users and any other third parties acting under its control or on its behalf comply with this AUP. Any breach of this AUP by an Authorised User or third party is deemed a breach by Customer.

1.6. **Intended use; high-risk contexts.** The Services are intended solely for professional catalog and document workflows, primarily for retailers, brands and marketplaces that need to transform supplier files into catalog-ready, multilingual product data with traceability. The Services are not designed or intended for consumer use.

Customer must not use the Services in connection with:

a) employment or HR decisions about individuals (including recruitment, screening, promotion or dismissal);

b) creditworthiness, credit scoring or financial reliability of natural persons;
c) medical diagnosis, treatment, triage or any other health-care decision about individuals; or
d) other high-risk personal decision-making contexts where Applicable Law or good industry practice requires dedicated, specialised systems.

Additional restrictions on high-risk AI uses are set out in Section 7.6.

1.7. **Updates to this AUP.** We may update this AUP from time to time as described in Section 13 (Changes to this AUP). The then-current version will be made available on inAi's Legal Hub and/or via the Services interface. Subject to Section 13, continued use of the Services after the effective date of an update constitutes acceptance of the updated AUP.

---

2. Definitions

For the purposes of this AUP:

2.1. "**Agreement**" has the meaning given in Section 1.2.

2.2. "**Authorised User**" means any natural person who is authorised by Customer to access and use the Services on Customer's behalf (including employees, contractors and service providers) and who is permitted by inAi under the Agreement.

2.3. "**Customer**" means the legal entity that has entered into the Agreement with inAi for access to the Services (including any Affiliate named in an order form or statement of work, where applicable).

2.4. "**Customer Data**" means all data, documents, files, images and other content that Customer or its Authorised Users submit or upload into the Services (for example, supplier PDFs, spec sheets, spreadsheets, images of packaging) as well as any configuration information, templates or glossaries provided by Customer.

2.5. "**Derived Data**" means metrics, statistics, logs, run reports, anonymised patterns and other data generated by inAi through operation of the Services (for example, fill-rates, correction counts, anomaly flags, hashes and environment fingerprints), in each case excluding Customer Data and Outputs themselves. To the extent any Derived Data constitutes personal data, inAi will process such data in accordance with the Agreement, the applicable data-processing agreement and inAi's privacy documentation.

2.6. "**Documentation**" means the documentation, technical descriptions and FAQs that inAi makes available regarding the Services, including via the PageMind product page, FAQ and Legal Hub.

2.7. "**Harm**" means any damage, loss or risk of damage or loss, including personal injury, death, property damage, financial loss, reputational harm, regulatory or criminal exposure, compromise of security, or material disruption to systems or services.

2.8. “**Output**” means any content produced by the Services based on Customer Data and configuration, including but not limited to structured CSV/Excel files, QA lists, retry lists, run reports, compliance evidence packs, titles, descriptions and attribute values.

2.9. “**Services**” means PageMind and any related modules, including but not limited to:

- catalog ingestion and transformation flows (from supplier files to template-aligned CSV);
- translation, glossary enforcement and attribute normalisation flows;
- quality-assurance and retry mechanisms;
- compliance-oriented modules such as Verify.EU, to the extent enabled for Customer under the Agreement.

2.10. “**Verify.EU**” means the module of PageMind that, where available and configured, retrieves official product and energy-label information from relevant registries (such as EPREL) and generates compliance-oriented fields and evidence packs according to rules such as “no evidence, no publish”.

2.11. “**Workspace**” means a logical environment or project space within the Services that is associated with one Customer (or one Customer business unit) and that may contain Customer Data, Outputs, configurations, logs and Derived Data for that Customer.

2.12. “**Applicable Law**” means all laws, regulations, regulatory guidance and codes of practice that apply to Customer, its business, its use of the Services and the Customer Data and Outputs it processes (including but not limited to: data-protection laws such as the GDPR, consumer-protection and product-safety law, unfair commercial practices rules, labelling and energy-label obligations, export control and sanctions regimes, and sector-specific regulations).

---

3. Service Description and Role of PageMind

3.1. PageMind is designed as a **catalog operations automation** tool that converts messy supplier files (such as PDFs, Word documents, spreadsheets and images) into a clean, template-aligned, multilingual product spreadsheet (CSV/Excel) with per-row traceability, QA lists and run reports. It may also provide specialised compliance assistance through modules such as Verify.EU.

3.2. PageMind sits logically **before** Customer’s own Product Information Management (PIM), e-commerce or catalog systems: it does not itself act as a PIM, shop platform or database of record, but rather generates import-ready data that Customer may choose to load into its own systems. PageMind does not replace Customer’s PIM, MDM, ERP, e-commerce, content-management or regulatory systems.

3.3. The Services rely on machine learning, large language models and third-party infrastructure operated both by inAi and by selected cloud and AI vendors. Output quality

is influenced by the quality and completeness of Customer Data, the clarity of templates and glossaries, and the configuration of the Services. While the Services are designed to minimise hallucination and provide traceability, no automated system is infallible and Outputs may contain errors, omissions, inconsistencies or misclassifications, and may not be complete, current or suitable for any particular purpose.

3.4. **No professional advice.** PageMind and its Outputs do not constitute legal, regulatory, compliance or other professional advice. In particular, Verify.EU is a technical aid to support Customer's internal product-compliance workflows and evidence collection; it is not a substitute for Customer's own legal, regulatory or compliance assessment, nor a guarantee that Customer's catalog or product pages meet any specific legal or regulatory requirement.

3.5. Customer remains solely responsible for:

- deciding whether and how to use any Output;
- verifying that Output is accurate, appropriate and compliant before relying on it or publishing it;
- applying its own human review and quality-control processes at a level appropriate to the risk and regulatory context.

3.6. PageMind is not designed, tested or intended for:

- safety-critical systems (e.g. medical devices, aviation, nuclear, life-support, emergency response);
- making or automating decisions that create a high risk of Harm to individuals or the public without adequate human review;
- consumer-facing direct interaction, except where Customer has layered its own UI, workflows and safeguards over Outputs.

3.7. **Changes to the Services.** inAi may update, modify, improve or discontinue features of the Services, models, prompts and workflows from time to time, including to reflect technical progress or changes in Applicable Law. inAi does not intend to materially reduce the core functionality of the Services provided to Customer during a committed term. If inAi makes a change that materially reduces such core functionality for Customer during a committed term, inAi will provide reasonable notice and, where appropriate, discuss in good faith alternative solutions or the consequences under the Agreement.

---

4. Eligibility, Accounts and Authorised Users

4.1. **Business use only.** The Services are intended solely for use by businesses and organisations. Customer represents and warrants that it is not a consumer and that it acquires the Services for professional purposes only.

4.2. **Age and capacity.** Customer must ensure that all Authorised Users are at least 18 years old (or the age of legal majority in their jurisdiction, if higher) and have the legal capacity to use the Services on Customer's behalf.

4.3. **Account creation.** Customer may be required to create one or more accounts or Workspaces (e.g. via the PageMind interface or through an onboarding process). Customer must provide accurate and complete information for account creation and keep such information up to date.

4.4. **Access control.** Customer is responsible for:

- designating which individuals are Authorised Users;
- assigning appropriate roles and permissions to each Authorised User; and
- promptly revoking access for anyone who should no longer use the Services (for example, upon termination of employment or contract).

4.5. **Credentials.** Customer must ensure that all access credentials (usernames, passwords, API keys, tokens) used to access the Services are:

- kept confidential and not shared beyond the specific Authorised User to whom they are assigned (except where expressly permitted by inAi, e.g. for service accounts); and
- stored and transmitted securely, in line with Customer's security policies.

4.6. **Security incidents.** Customer must promptly notify inAi if it becomes aware of any:

- actual or suspected unauthorised access to the Services or to a Workspace;
- loss, theft or compromise of any credentials or access tokens; or
- misuse of the Services under its account.

4.7. **Third-party access.** If Customer grants access to the Services to any third-party contractor, consultant or service provider, Customer:

- remains fully responsible for that third party's compliance with this AUP and the Agreement; and
- must ensure that appropriate contractual and security controls are in place with such third party.

4.8. **Pilot or beta access.** Where Customer accesses the Services in a trial, beta or pilot capacity (for example, under a PageMind private-beta or pilot agreement), the same eligibility and account rules apply. inAi may impose additional technical limitations or termination rights for pilots and betas, as set out in the relevant Agreement.

4.9. **Responsibility for account activity.** Except to the extent expressly stated otherwise in the Agreement, Customer is responsible for all access to and use of the Services under its accounts and Workspaces, including by Authorised Users and third parties acting on its

behalf, whether or not such access or use is authorised by Customer, and whether resulting from Customer's failure to protect access credentials or otherwise.

---

5. Customer Responsibilities and General Obligations

5.1. **Compliance with law.** Customer must ensure that its use of the Services, and the use of the Services by any Authorised User or third party under its control:

- complies with all Applicable Law; and
- must not use the Services in a manner that it knows or reasonably should know would cause inAi or any of its vendors or partners to be in breach of Applicable Law.

This includes, without limitation, compliance with:

- data-protection and privacy laws (such as GDPR);
- consumer-protection and unfair commercial practices law;
- product-safety, labelling and energy-label obligations (including EPREL-related obligations for energy-labelled products);
- export control and sanctions, including restrictions on dealing with listed persons or embargoed countries; and
- sector-specific regulations that apply to Customer's products or services;
- Customer acknowledges that inAi does not monitor, and has no obligation to monitor, Customer's compliance with Applicable Law and that Customer remains solely responsible for assessing whether its use of the Services and any Outputs is lawful in each relevant jurisdiction.

5.2. **Appropriate use context.** Customer must use PageMind only in contexts where:

- automated extraction, translation and transformation of supplier documentation into catalog-ready data is appropriate and lawful; and
- Customer has implemented an adequate human-in-the-loop review process before Outputs are relied upon or made public, especially for compliance-critical or safety-relevant fields.

5.3. **Responsibility for Customer Data.** Customer is solely responsible for:

- the legality, accuracy, completeness and integrity of all Customer Data it submits to the Services;
- ensuring that it has all necessary rights, licences and permissions (including from suppliers, licensors and data subjects) to upload Customer Data into the Services and to allow inAi and its subprocessors to process Customer Data in accordance with the Agreement and this AUP;
- ensuring that Customer Data does not infringe any third-party rights, including intellectual property, privacy, publicity or confidentiality rights.

5.4. **Responsibility for Outputs.** Customer is solely responsible for:

- reviewing Outputs generated by the Services;
- deciding whether and how to use, publish or rely upon any Output;
- ensuring that any published catalog content, product pages or other downstream use of Outputs complies with Applicable Law and Customer's own internal policies;
- implementing additional controls, validations and monitoring appropriate to the risk level of the use case.

5.5. **No reliance as sole source of truth.** Customer must not treat Outputs as a definitive or exclusive source of truth, especially for:

- legal or regulatory classifications;
- compliance-critical values (e.g. safety ratings, limits, hazard classifications);
- fields where Applicable Law requires specific official sources, accredited laboratories or notified bodies.

Where legal or regulatory obligations exist, Customer must ensure that it cross-checks Outputs against official or authoritative sources and applies appropriate professional judgement.

This Section 5.5 is consistent with and supplements Section 3 and Section 10 of the PageMind Terms of Service. In case of any doubt, Customer must follow the stricter interpretation.

5.6. **Data minimisation and personal data.** The Services are designed primarily for product- and catalog-related content and not for processing of large-scale or sensitive personal data. Customer must:

a) avoid intentionally uploading documents that primarily contain personal data about identifiable individuals (such as HR files, medical records, consumer complaints, CVs or identity documents), except where expressly permitted in the Agreement and applicable data-processing agreement; and
b) never use the Services to process special categories of personal data or personal data relating to criminal convictions or offences, unless this is expressly agreed in writing in the Agreement or a data-processing agreement and appropriate additional safeguards are in place.

Customer remains responsible for ensuring that it has a valid legal basis and appropriate transparency for any personal data included incidentally in Customer Data, in accordance with Section 8.

5.7. **Templates, glossaries and configuration.** Customer is responsible for:

- defining its own catalog templates, required fields and acceptable values;

- configuring allowed lists (e.g. for colours and sizes), glossaries, banned terms and other controls to reflect its internal rules and regulatory obligations;
- keeping such configuration up to date as its internal rules or Applicable Law change.

5.8. **Cooperation and feedback.** Customer must cooperate reasonably with inAi in the event of:

- investigation of potential misuse or security incidents related to Customer's account;
- pilot or beta projects where PageMind is being evaluated, including providing feedback and, where agreed, non-confidential performance metrics.

5.9. **Internal policies.** Customer must ensure that its own internal policies (for example, about AI use, data-protection, information security, compliance and procurement) permit the use of PageMind in the manner Customer intends. It is Customer's responsibility to obtain any necessary internal approvals (for example, from legal, compliance, DPO, information-security or works councils).

5.10. **Indemnity (conceptual placeholder).** Subject to the Agreement, Customer will be responsible for any claims, damages, fines or other liabilities suffered by inAi that arise from:

- Customer's breach of this AUP or the Agreement;
- Customer's unlawful use of the Services;
- Customer's failure to obtain necessary rights or consents for Customer Data or its downstream use of Outputs.

(The precise indemnity language, scope and limitations will be defined in the Agreement and should be reviewed with legal counsel.)

6. Permitted Use of the Services

6.1. **Intended business use.** Subject to the Agreement and this AUP, Customer and its Authorised Users may use the Services solely for Customer's internal business purposes, in particular to:

a) ingest and process supplier documentation (including PDFs, images, DOCX, spreadsheets and similar files) in order to generate catalog-ready, template-aligned product data and related reports;
b) translate and localise catalog content into supported languages under Customer-defined glossaries and terminology rules;
c) assist with the normalisation and validation of product attributes (such as colour, size and other technical specifications) according to Customer's allowed lists and templates;
d) generate QA lists, retry lists, run reports and evidence packs to support Customer's internal catalog-quality and compliance workflows;

e) where enabled, use Verify.EU or similar modules to assist with retrieving and cross-checking product and energy-label information from relevant registries (such as EPREL), subject to the Verify.EU-specific rules in this AUP.

6.2. **Authorised Users.** Only Authorised Users may access and use the Services. Customer must ensure that each Authorised User uses the Services solely:

a) on behalf of Customer and in the course of their professional duties; and
b) in accordance with this AUP, the Agreement and any Documentation provided by inAi.

6.3. **Limitations to intended scope.** The Services are designed for product- and catalog-related workflows, not for consumer use or general high-risk decision-making about individuals. Customer must not use the Services for purposes outside this intended scope, including any use that is prohibited under Section 7.

6.4. **Third-party integrations.** Where the Services provide connectors or export formats for PIM, e-commerce, marketplace or other third-party systems, Customer may use such integrations solely to move Outputs into Customer's own environments and solely in accordance with the applicable terms of such third-party systems. inAi does not grant any rights under, or assume any responsibility for compliance with, third-party terms.

6.5. **Benchmarks and testing.** Customer may perform reasonable tests and evaluations of the Services for its own internal purposes (including pilots, proof-of-concepts and QA). Customer must not publish or disclose to any third party any benchmark, performance test or evaluation of the Services (including comparisons with other products or services) without inAi's prior written consent. Customer must not access or use the Services in any way that would fall within the prohibitions set out in Section 7 (for example, using test runs as a vehicle to misuse infrastructure or infringe rights).

6.6. **Reservation of rights.** All rights in and to the Services not expressly granted to Customer under the Agreement are reserved by inAi and its licensors. No rights are granted by implication or estoppel.

---

7. Prohibited Content and Activities

Customer and its Authorised Users must not, directly or indirectly, use the Services, or permit the Services to be used, in any way that falls within any of the categories set out in this Section 7. Any such use constitutes a material breach of this AUP and the Agreement.

7.1. Illegal, harmful or offensive activities

Customer must not use the Services to:

a) violate any Applicable Law;
b) plan, commit, promote or facilitate any fraudulent, deceptive, criminal or otherwise unlawful activity;

c) create, store, distribute or promote content that incites violence, terrorism or violent extremism, or that is intended to threaten, harass or intimidate individuals or groups;
d) exploit or harm minors in any way, including by exposing them to inappropriate content or collecting their personal data in violation of child-protection laws; or
e) engage in or promote human trafficking, slavery or other serious human-rights abuses.

7.2. Infringement of intellectual property or confidential information

Customer must not:

a) upload or process any Customer Data that infringes any copyright, trademark, database right, trade secret or other intellectual-property or proprietary right of any person;
b) use the Services to copy, reconstruct or misappropriate third-party datasets, taxonomies, catalogues or confidential documentation in a manner that would violate contractual restrictions or trade-secret obligations;
c) upload supplier or partner documents where Customer does not have, and has not obtained, all necessary rights and permissions for such documents to be processed via the Services for catalog purposes; or
d) remove or alter any proprietary notices (including copyright and trademark notices) included in the Services or in Documentation.

Customer is responsible for ensuring that its agreements with suppliers and other data providers permit the use of their content within PageMind as described in the Agreement and this AUP.

7.3. Personal data and privacy

Customer must not use the Services in a way that violates data-protection, privacy or confidentiality laws, or that conflicts with the roles and responsibilities allocated in the Agreement, the applicable data-processing agreement or inAi's privacy documentation. In particular, Customer must comply with the personal-data usage rules in Sections 5.6 and 8 and must not intentionally use the Services to process special categories of personal data or personal data relating to criminal convictions or offences unless this is expressly permitted under those documents and appropriate safeguards are in place.

7.4. Security violations and network abuse

Customer must not:

a) access, or attempt to access, any data, account, system or resource related to the Services that it is not expressly authorised to access;
b) probe, scan, test, or attempt to probe, scan or test, the vulnerability of any inAi system or network without prior written permission from inAi (no unauthorised penetration testing);
c) interfere with, or attempt to interfere with, the proper functioning of the Services, including by engaging in any denial-of-service attack, overload, flooding, spamming or mail-bombing;

d) introduce malware, viruses, worms, Trojan horses, ransomware or other malicious code into the Services or into Customer Data uploaded to the Services; or
e) use the Services to attempt to gain unauthorised access to, or disrupt, any third-party system, network or service.

7.5. Misuse of the Services or infrastructure

Customer must not:

a) circumvent or attempt to circumvent any usage limits, quotas, security controls or technical restrictions implemented in the Services (including by creating multiple accounts or API keys solely to bypass such limits);
b) use the Services as a generic computing platform, LLM proxy or benchmarking tool for unrelated workloads, outside the catalog and document workflows contemplated by the Agreement and Documentation;
c) use free tiers, test accounts, credits or beta access to run workloads that are not reasonably related to evaluating or using the Services for permitted catalog-ops or document-ops purposes;
d) attempt to reverse engineer, decompile, disassemble or derive the source code, underlying models or non-public interfaces of the Services, except to the extent such restriction is prohibited by Applicable Law; or
e) use the Services, or any non-public information about the Services obtained through access to them, to design, train or operate a service that is substantially similar to or competes directly with PageMind in a manner that misuses inAi's intellectual-property or confidential information. For clarity, nothing in this AUP is intended to prevent Customer from independently developing products or services that compete with PageMind, provided such development does not involve misuse of the Services or inAi's intellectual-property or confidential information.

7.6. High-risk or prohibited AI uses

Without inAi's prior express written consent and a separately documented risk-management and compliance framework, Customer must not use the Services in connection with:

a) making, or materially supporting, decisions about the creditworthiness, credit scoring or financial reliability of natural persons;
b) recruitment, screening, ranking, promotion or dismissal of employees, workers or candidates, where Outputs are used as a decisive factor;
c) biometric identification, biometric categorisation or emotion recognition of individuals;
d) law-enforcement risk scoring, predictive policing, migration or border control decisions; or
e) any other use case that is classified as "high-risk" or prohibited under Applicable Law and for which PageMind is not explicitly designed or documented.

Customer must not use the Services to circumvent safeguards, monitoring or compliance obligations that apply to other AI systems or automated decision-making tools operated by or for Customer.

inAi may, without liability, refuse, suspend or terminate any use of the Services that it reasonably considers to fall within the categories described in this Section 7.6 or to create an unacceptable level of regulatory, security or reputational risk for inAi, its subprocessors or other customers.

7.7. Verify.EU and registry-linked misuse

Where Customer uses Verify.EU or any similar module:

a) Customer must not represent the Services, Verify.EU, or any Output as an official service, approval, certification or decision of the European Union, EPREL or any regulator;
b) Customer must not alter or present Outputs in a manner that falsely suggests that a value originates from an official registry when it does not, or that omits qualifiers or flags in a way that would make the Output appear more authoritative or definitive than it is;
c) Customer must not use Verify.EU in any way that violates the terms of use or access conditions of the relevant registries or APIs; and
d) Customer remains solely responsible for verifying that its energy-label and product-information obligations are met for each product in each jurisdiction where it markets that product, and may not rely on the Services as a substitute for such verification.

7.8. Misuse of Outputs and automation

Customer must not:

a) rely solely on Outputs, without appropriate human review, for legal, safety-critical or regulatory decisions where Applicable Law or good industry practice requires human judgement or additional validation;
b) represent to any third party that Outputs are guaranteed to be correct, current, complete or legally sufficient, or that PageMind assumes responsibility for compliance of Customer's catalog;
c) remove, conceal or ignore flags, warnings, traceability fields or other indicators inserted by the Services in a way that would reasonably mislead others about the reliability or provenance of Outputs;
d) implement fully automated "publish without review" workflows for Outputs in contexts that are compliance-critical, safety-relevant, or subject to specific regulatory obligations (including Energy Labelling), regardless of any internal risk assessment; or
e) use Outputs in any deliberate attempt to mislead regulators, consumers, partners or marketplaces as to the characteristics, performance or compliance of products.

7.9. Sanctions, export control and restricted parties

Customer must not use the Services:

a) in violation of any applicable sanctions, export-control or embargo laws, including those of the European Union, United Nations, United States or United Kingdom;
b) for or on behalf of any individual or entity that is listed on any applicable sanctions list or that is otherwise the target of sanctions; or
c) in any jurisdiction where the provision or use of the Services is prohibited by Applicable Law or would require inAi to obtain a licence that it does not hold.

If Customer becomes a sanctioned person or entity, or is owned or controlled by a sanctioned person or entity, Customer must immediately stop using the Services and notify inAi.

---

8. Data Protection and Privacy Usage Rules

8.1. **Roles under data-protection law.** The allocation of roles and responsibilities for personal data (for example, whether Customer is controller and inAi is processor, or inAi is an independent controller) is governed by the Agreement, the applicable data-processing agreement and inAi's privacy documentation. If there is any conflict between this AUP and those documents in relation to personal data, those documents will prevail. This Section 8 sets additional usage obligations for Customer and must be read consistently with them.

8.2. **Data minimisation.** Customer must use the Services in accordance with the principle of data minimisation. In particular:

a) Customer will only upload Customer Data that is reasonably necessary for the catalog and document workflows for which it uses PageMind;
b) Customer will avoid uploading files that primarily concern identifiable individuals (such as HR records, consumer complaints, medical reports, CVs, identity documents), unless clearly necessary and permitted by the Agreement and privacy documentation; and
c) Customer will configure templates, projects and Workspaces in a way that avoids unnecessary duplication of personal data.

8.3. **Lawful basis and transparency.** For any personal data included in Customer Data, Customer is responsible for:

a) establishing and documenting a valid legal basis for processing under Applicable Law;
b) informing data subjects appropriately about the processing of their personal data via the Services, including any relevant disclosures about transfers to inAi and its subprocessors; and
c) honouring data-subject rights (access, rectification, erasure, restriction, objection, portability) in accordance with Applicable Law and the Agreement.

8.4. **Restrictions on special categories and criminal data.** Unless expressly agreed in writing and accompanied by appropriate additional safeguards, Customer must not use the Services to process:

a) special categories of personal data; or
b) personal data relating to criminal convictions or offences.

If inAi reasonably believes that Customer is using the Services to process such data without appropriate safeguards, inAi may require Customer to cease such processing, suspend relevant functionality, or take other measures under Section 11.

8.5. **Cross-border transfers.** International transfers of personal data by inAi (including to subprocessors) are governed by the Agreement, the applicable data-processing agreement and inAi's privacy documentation (for example, use of approved transfer mechanisms and EU data-centre locations). Customer must not use the Services in a way that intentionally circumvents or conflicts with those transfer mechanisms (for example, by routing Customer Data from jurisdictions or entities that are clearly incompatible with the agreed transfer framework).

8.6. **Combination with other datasets.** Customer must not use the Services to combine Customer Data or Outputs with other datasets in a way that would:

a) re-identify individuals from anonymised or pseudonymised data; or
b) materially change the risk profile for individuals compared to the way PageMind is normally used (for example, turning product usage data into detailed consumer or employee profiles).

8.7. **Incidents and cooperation.** If Customer becomes aware of a security incident, data breach or other event involving Customer Data in the Services that may require notification to regulators or data subjects, Customer must:

a) promptly inform inAi via the channels indicated in the Agreement or Documentation; and
b) cooperate reasonably with inAi in investigating and mitigating the incident, consistent with the Agreement and applicable data-protection terms.

---

9. Fair Use, Rate Limits and Resource Consumption

9.1. **Usage limits.** The Services may include technical and contractual limits on usage, such as:

a) maximum number of documents or products processed per period;
b) rate limits on API calls or job submissions;
c) limits by plan or Workspace on concurrent runs, environments or features.

These limits may be defined in the Agreement, the Documentation, the user interface or any applicable order form.

9.2. **Compliance with limits.** Customer must comply with all such usage limits and must not attempt to circumvent them, including by:

a) creating multiple accounts, Workspaces or API keys solely to bypass limits;
b) scripting or automating calls in a way that ignores documented backoff or rate-limit headers; or
c) modifying or interfering with any client library or integration provided by inAi to remove limit-enforcement mechanisms.

9.3. **Fair use of shared resources.** Customer must use shared infrastructure (such as compute, storage, queues) in a manner that is fair and does not unreasonably degrade the experience of other customers. inAi may apply throttling, queueing, scheduling or other technical measures to protect overall service quality.

9.4. **Abnormal or abusive patterns.** If inAi reasonably detects abnormal or abusive usage patterns (for example, sudden spikes consistent with scraping, load testing or non-catalog workloads):

a) inAi may temporarily throttle or suspend the relevant jobs, users or Workspaces; and
b) inAi will, where reasonably practicable, notify Customer and work with Customer to understand and address the issue.

9.5. **Upgrading and capacity planning.** Where Customer's legitimate, permitted usage grows beyond the levels contemplated by its current plan or order:

a) inAi may request that Customer upgrade to a more suitable plan or conclude a new order reflecting such usage; and
b) until such upgrade is agreed, inAi may apply reasonable interim limits to ensure stability and predictability of the Services.

9.6. **Prohibition on stress-testing without consent.** Customer must not use the Services for deliberate stress-testing, load testing or resilience testing of inAi's infrastructure, except:

a) as reasonably incidental to normal business usage; or
b) where explicitly agreed in writing in advance with inAi (for example, as part of a coordinated test).

---

10. Third-Party Services, Subprocessors and Data Sources

10.1. **Subprocessors and vendors.** The Services may rely on third-party providers, including cloud infrastructure providers, AI model vendors and monitoring or logging services. The list of subprocessors for personal data, where required by law, is described in the relevant data-processing documentation or on inAi's Legal Hub.

10.2. **No privity with third parties.** The Agreement and this AUP do not create any contractual relationship between Customer and inAi's subprocessors or vendors. Customer's rights and remedies in relation to the Services are solely against inAi, subject to the Agreement.

10.3. **Compliance with third-party terms.** Where the Services provide integrations, connectors or exports to third-party services (such as PIMs, e-commerce platforms or registries), Customer must:

a) use such third-party services in accordance with their applicable terms and conditions; and
b) not configure or use the Services in a manner that causes, or is reasonably likely to cause, Customer or inAi to breach those third-party terms.

10.4. **External registries and official sources.** For modules such as Verify.EU that connect to official or semi-official registries:

a) Customer acknowledges that such registries are operated by third parties and that inAi does not control their content, availability or accuracy;
b) Customer must respect any access, usage or attribution requirements imposed by such registries; and
c) Customer must not use the Services to scrape, systematically harvest or redisplay registry data in ways that are not contemplated by the Agreement or that would violate registry terms.

10.5. **Customer's own third-party processors.** If Customer engages its own third-party processors, consultants or service providers to use Outputs, integrate PageMind with other systems or operate catalog workflows:

a) Customer remains fully responsible for such third parties' compliance with this AUP and the Agreement; and
b) Customer must ensure that its contracts with such third parties are consistent with the restrictions and responsibilities described in this AUP.

---

11. Monitoring, Investigation and Enforcement

11.1. **Monitoring of use.** inAi may monitor use of the Services, including via logs, metrics and automated tools, for the purposes of:

a) ensuring security, stability and performance of the Services;
b) detecting, preventing and responding to actual or suspected violations of this AUP or the Agreement; and
c) generating aggregated statistics and Derived Data for service improvement, capacity planning and reporting, as described in the Agreement and privacy documentation.

Monitoring will be conducted in a manner that is proportionate and consistent with Applicable Law and inAi's privacy commitments.

11.2. **Review of Customer Data.** inAi does not routinely review the substance of Customer Data. However, inAi may access and review limited portions of Customer Data where reasonably necessary:

a) to operate, maintain, secure and improve the Services in accordance with the Agreement, the applicable data-processing agreement and inAi's privacy documentation;
b) to investigate a suspected violation of this AUP or the Agreement;
c) to respond to a security incident or technical problem affecting the Services; or
d) to comply with a valid legal request or order from a competent authority.

Any such access will be restricted to personnel with a need to know and handled in accordance with applicable confidentiality and data-protection obligations. For clarity, nothing in this AUP shall be interpreted as imposing on inAi any general obligation to monitor Customer Data, Outputs or Customer's use of the Services.

11.3. **Reporting and escalation.** If inAi becomes aware of suspected misuse or breach of this AUP, inAi may:

a) inform Customer and provide relevant details, to the extent permitted by law;
b) request additional information from Customer; and
c) require Customer to take specific remedial actions (for example, removing certain Customer Data, disabling certain users, or modifying configurations).

11.4. **Enforcement measures.** Without limiting any other rights or remedies under the Agreement or at law, inAi may, in its reasonable discretion and depending on the severity and nature of the issue:

a) issue warnings or instructions to Customer regarding non-compliant use;
b) temporarily suspend or restrict access to the Services for specific users, Workspaces, features or the entire account;
c) remove, disable access to, or request removal of Customer Data or Outputs that appear to violate this AUP or Applicable Law;
d) refuse to process or complete specific jobs or tasks that inAi reasonably believes to be non-compliant; and/or
e) terminate the Agreement or relevant orders in cases of serious, repeated or wilful violations.

11.5. **Emergency suspension.** inAi may immediately and without prior notice suspend or restrict access to the Services where:

a) inAi reasonably believes that such action is necessary to protect the security, integrity or availability of the Services or of third-party systems;
b) inAi reasonably suspects that use of the Services is causing, or is likely to cause, material Harm to any person; or
c) inAi is required to do so by Applicable Law or by a competent authority.

Where reasonably practicable, inAi will inform Customer of the reasons for such emergency suspension and will work with Customer in good faith to restore compliant use.

11.6. **Law-enforcement and regulatory requests.** inAi may cooperate with law-enforcement agencies, regulators and other competent authorities in connection with

investigations of suspected illegal activities involving the Services, subject to Applicable Law and, where possible, reasonable efforts to notify Customer, except where such notification is prohibited.

---

12. Reporting Abuse, Security Issues or Violations

12.1. **Reporting channels.** Customer and third parties may report suspected abuse, violations of this AUP, or security vulnerabilities relating to the Services using the contact details specified in the Documentation or on inAi's website (for example, dedicated "abuse@" or "security@" email addresses).

12.2. **Information to include.** When reporting a suspected violation or security issue, reporters should provide sufficient detail to enable inAi to understand and assess the issue, including:

a) a description of the behaviour or content in question;
b) relevant dates, times and time zones;
c) any known account identifiers, Workspaces or job IDs; and
d) where applicable, steps to reproduce a technical issue or vulnerability.

12.3. **Good-faith security research.** inAi encourages responsible, good-faith reporting of security vulnerabilities. Reporters should:

a) avoid accessing more data than is strictly necessary to demonstrate a vulnerability;
b) not intentionally degrade the performance or availability of the Services; and
c) give inAi a reasonable opportunity to remediate issues before publicly disclosing them.

Any public bug-bounty or vulnerability-disclosure programs operated by inAi may set additional rules or channels for such reports.

12.4. **No retaliation for good-faith reports.** inAi will not take adverse action against Customer or a reporter solely for making a good-faith report of a suspected vulnerability or AUP violation, provided that the reporter's own actions remain within the boundaries of Applicable Law and this AUP.

---

13. Changes to this AUP

13.1. **Right to update.** inAi may update this AUP from time to time to reflect:

a) changes to the Services or to inAi's infrastructure;
b) changes in Applicable Law, regulatory guidance or industry standards; or
c) the need to address emerging forms of misuse or new risks.

13.2. **Notification.** inAi will make the updated AUP available via its Legal Hub or other central location and will indicate the date of the latest update. For changes that materially

broaden the types of prohibited uses or materially increase Customer's obligations, inAi will provide reasonable notice to Customer (for example, by email or in-product notifications). For these purposes, a change will be considered to "materially broaden" prohibited uses or "materially increase" Customer's obligations if it introduces new categories of prohibited use or new affirmative duties for Customer (for example, new configuration, reporting or audit obligations) beyond those reasonably necessary to maintain security, comply with Applicable Law or reflect changes to the Services that do not reduce Customer's existing rights.

13.3. **Effective date.** Unless otherwise specified in the notice, updates to this AUP will take effect on the date indicated as the "last updated" date. Continued use of the Services after that date constitutes Customer's acceptance of the updated AUP.

13.4. **Objections.** If Customer reasonably objects to an update that materially and adversely affects it, Customer may, within the notice period specified, notify inAi in writing. The parties will discuss in good faith; if they cannot reach a mutually acceptable solution within a reasonable time, Customer's sole and exclusive remedy will be to exercise any applicable termination and exit rights set out in the Agreement, and the version of this AUP in force immediately before the relevant update will continue to apply to Customer until such termination takes effect.

---

14. Governing Law, Jurisdiction and Contact Details

14.1. **Governing law and jurisdiction.** This AUP is governed by the same law and jurisdiction specified in the Agreement (for example, French law and the competent courts designated therein). Any dispute arising from or in connection with this AUP will be subject to that jurisdiction, without prejudice to mandatory rights of regulators or other authorities.

14.2. **Contact details.** Questions or concerns about this AUP may be addressed to inAi using the contact information provided in the Agreement or on inAi's website, including:

- registered office and corporate identity details as set out in the legal notices; and
- designated contact channels for legal, privacy, security and support matters.

14.3. **Hierarchy.** In case of inconsistency between this AUP and any other document referenced in it, the hierarchy provisions of the Agreement apply.