PageMind Data Processing Agreement (DPA)

Last updated: 2025-12-08

(DPA – GDPR ARTICLE 28)

This Data Processing Agreement ("DPA") forms part of and is incorporated into the master subscription agreement, terms of service, order form, or other written agreement governing the provision of the PageMind service between the parties (the "Principal Agreement").

BETWEEN:

1. The customer identified as such in the Principal Agreement ("Customer" or "Controller"); and
2. INAI, a French société par actions simplifiée à associé unique (SASU) with its registered office at 142 rue d'Iéna, apt. 21, 59000 Lille, France ("inAi", "Processor", "we", "us"),

each a "Party" and together the "Parties".

WHEREAS:

(A) Customer acts as a controller (or, where applicable, as a processor on behalf of a third-party controller) of certain Personal Data;
(B) Processor provides the PageMind software-as-a-service and related support and professional services, under which Processor will process Personal Data on behalf of Customer; and
(C) The Parties seek to implement a data processing agreement that satisfies the requirements of Article 28 of the GDPR and other Applicable Data Protection Law.

NOW, THEREFORE, the Parties agree as follows.

---

1. DEFINITIONS AND INTERPRETATION

1.1 In this DPA, the following terms shall have the meanings set out below:

(a) **"Applicable Data Protection Law"** means all data protection and privacy laws and regulations applicable to the Processing carried out under this DPA, including, where applicable, the GDPR and any national implementing or supplementary legislation, as amended from time to time.

(b) **“Controller”**, **“Processor”**, **“Personal Data”**, **“Data Subject”**, **“Processing”**, **“Personal Data Breach”**, **“Supervisory Authority”**, and **“Third Country”** have the meanings given to them in the GDPR.

(c) **“Customer Personal Data”** means any Personal Data in electronic form that is uploaded, submitted, provided or made available by or on behalf of Customer to Processor, or otherwise Processed by Processor on behalf of Customer, in connection with the PageMind Service under the Principal Agreement.

(d) **“EEA”** means the European Economic Area (being the Member States of the European Union from time to time, together with Iceland, Liechtenstein and Norway).

(e) **“PageMind Service”** means the catalog operations automation and related software-as-a-service offering branded “PageMind” (including the Verify.EU compliance module and any other PageMind-branded functionality) provided by Processor to Customer under the Principal Agreement, including associated support and maintenance.

(f) **“Sub-processor”** means another processor engaged by Processor for carrying out specific Processing activities on behalf of Customer in connection with the PageMind Service.

(g) **“Standard Contractual Clauses”** means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 adopted by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021 (including any successor decision), as amended, replaced or superseded from time to time.

(h) **“Technical and Organisational Measures”** means the technical and organisational measures implemented by Processor to protect Customer Personal Data in accordance with Clause 7 and Annex 2 of this DPA.

1.2 Capitalised terms not otherwise defined in this DPA shall have the meaning given to them in the Principal Agreement.

1.3 In case of conflict or ambiguity between any provision in this DPA and any provision in the Principal Agreement, the provision in this DPA shall prevail to the extent of such conflict with respect to the Processing of Customer Personal Data.

1.4 References to a statute or statutory provision include all subordinate legislation and guidance made under that statute or provision and any amendments or replacements thereof from time to time.

2. SCOPE, SUBJECT MATTER AND DURATION

2.1 This DPA governs Processor's Processing of Customer Personal Data on behalf of Customer in connection with the provision of the PageMind Service under the Principal Agreement.

2.2 The **subject matter** of the Processing is the Customer Personal Data described in Clause 4 and Annex 1 of this DPA.

2.3 The **duration** of the Processing shall be the term of the Principal Agreement, unless otherwise required by Applicable Data Protection Law or expressly agreed by the Parties in writing, and shall include any limited post-termination retention period specified in Clause 12 and Annex 2 for backups and logs.

2.4 **Roles.**
This DPA applies solely to Processing where Processor acts as a **processor** (or sub-processor) on behalf of Customer. This includes the processing of the content of Customer Data (e.g., supplier files, product attributes) for the provision of the PageMind Service.

Independent Controller Status: Processor acts as an independent **controller** solely regarding:
(a) Account management, billing, and contract administration; and
(b) The processing of **Service Data** (as defined in the Principal Agreement), such as technical logs, telemetry, and usage metrics, for security, fraud prevention, and product improvement purposes.

For the avoidance of doubt, Processor shall not act as a Controller regarding the content of Customer Data unless such data has been fully anonymised such that it no longer constitutes Personal Data.

---

3. NATURE AND PURPOSES OF PROCESSING

3.1 Processor shall Process Customer Personal Data only for the following **purposes**, to the extent strictly necessary:

(a) to provide, operate and maintain the PageMind Service to Customer in accordance with the Principal Agreement, including:

(i) ingesting and reading files supplied by or on behalf of Customer;
(ii) extracting, structuring, transforming, translating, normalising and otherwise processing information contained in such files;
(iii) generating catalog-ready structured outputs, quality-assurance files, retry lists and compliance/evidence packs; and
(iv) providing associated dashboards, logs and reports;

(b) to provide **support services**, respond to incidents, troubleshoot bugs and address performance issues relating to the PageMind Service;

(c) to implement, monitor and improve **information security**, including detection and prevention of abuse, security threats or incidents;

(d) to generate and use **aggregated statistics and metrics** derived from the Processing of Customer Personal Data for statistical, analytical, service improvement, benchmarking and research purposes, provided that:
(i) such outputs are irreversibly anonymised such that they are no longer Personal Data; and
(ii) Processor does **not** use Customer Personal Data to train or improve the content-generation capabilities of any AI models shared with third parties or other customers; and

(e) to comply with **legal obligations** to which Processor is subject and to respond to lawful requests from public authorities, where such obligations or requests relate to Processing under this DPA.

3.2 The **nature of Processing** of Customer Personal Data by Processor includes, as applicable: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, analysis, translation, pseudonymisation, restriction, erasure and destruction, as necessary to achieve the purposes described in Clause 3.1.

3.3 Processor shall not Process Customer Personal Data for any purpose other than those permitted under this DPA, unless required to do so by Union or Member State law; in such a case, Processor shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

---

4. CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA

4.1 The **categories of Data Subjects** whose Personal Data may be Processed under this DPA typically include, to the extent included in files or data Customer provides to the PageMind Service:

(a) employees, contractors, representatives or contact persons of Customer;
(b) employees, contractors, representatives or contact persons of Customer's suppliers, brands, manufacturers, distributors and other business partners;
(c) individuals whose names or contact details may incidentally appear in documents supplied to PageMind (for example, authors, signatories or points of contact on product sheets or contracts); and
(d) any other Data Subjects whose Personal Data Customer chooses to include in materials uploaded or otherwise made available to the PageMind Service.

4.2 The **types of Customer Personal Data** Processed under this DPA may include, to the extent contained in Customer's input materials:

(a) identification and contact data (such as name, job title, role, employer, business email address, business telephone number, postal address);
(b) organisational data (such as department, region, business unit, role within the supplier or customer organisation);
(c) electronic identifiers embedded in documents (such as usernames, internal IDs, file metadata, timestamps); and
(d) any other Personal Data that Customer elects to submit to the PageMind Service in free-text fields, file contents or templates.

4.3 The Parties do **not anticipate** that Customer will deliberately submit **Special Categories of Personal Data** (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation) nor Personal Data relating to criminal convictions and offences in connection with the PageMind Service.

4.4 Customer shall be solely responsible for ensuring that:

(a) Customer does not intentionally include Special Categories of Personal Data or criminal-conviction data in materials uploaded to the PageMind Service, except where strictly necessary and subject to appropriate safeguards and a documented agreement between the Parties;

(b) Customer's use of the PageMind Service is configured in such a way as to avoid unnecessary inclusion of Personal Data (for example, by stripping or redacting personal contact blocks from supplier documents where feasible); and

(c) where Customer nevertheless submits Special Categories of Personal Data or criminal-conviction data, Customer has established an appropriate legal basis and complies with all additional requirements under Applicable Data Protection Law; and

(d) Customer's internal policies and procedures are designed to prevent the inclusion of Special Categories of Personal Data or criminal-conviction data in Supplier Materials and other inputs to the PageMind Service, except where strictly necessary and subject to a separate documented agreement as described in Clause 4.3, and Customer shall promptly notify Processor in writing if it becomes aware that such data are being Processed on a more than incidental basis.

4.5 Processor may, and in appropriate cases shall, delete, pseudonymise or restrict Processing of any Customer Personal Data that it reasonably believes to be excessive, irrelevant or unlawfully submitted to the PageMind Service, particularly where such data appears to include Special Categories of Personal Data or criminal-conviction data contrary to this Clause 4.

5. INSTRUCTIONS AND RESPONSIBILITIES OF THE PARTIES

5.1 **Documented instructions.** Processor shall Process Customer Personal Data only:

(a) on the documented instructions of Customer as set out in this DPA and the Principal Agreement; and

(b) on any additional documented instructions that Customer may reasonably give from time to time where such instructions are consistent with the Principal Agreement and this DPA and are technically feasible.

The Parties agree that Customer's configuration and use of the PageMind Service (including selection of input folders, templates, languages and workflows) constitutes documented instructions for the purposes of this DPA.

5.2 **Notification of unlawful instructions.** If Processor considers that an instruction given by Customer infringes Applicable Data Protection Law, Processor shall inform Customer without undue delay. Processor shall not be obliged to provide legal advice. Pending resolution, Processor may suspend the relevant Processing. Customer remains solely responsible for the legality of its instructions.

5.3 **Customer responsibilities as Controller.** Customer shall be solely responsible for:

(a) determining the **lawful purposes and legal bases** for the Processing of Customer Personal Data and ensuring that such Processing is fair, lawful and transparent, including in relation to international transfers;

(b) providing all **necessary notices** to Data Subjects and, where required, obtaining any necessary **consents** or satisfying other conditions for the lawful Processing of Customer Personal Data, including its transfer to Processor and onward transfers to Sub-processors;

(c) ensuring that the **content, accuracy, quality and lawfulness** of Customer Personal Data and of the means by which Customer acquired such Personal Data comply with Applicable Data Protection Law;

(d) ensuring that Customer's use of the PageMind Service and Customer's instructions to Processor do not place Processor in breach of Applicable Data Protection Law; and

(e) where Customer acts as a processor on behalf of a third-party controller, ensuring that it is authorised under its agreement with such controller and under Applicable Data Protection Law to enter into this DPA and to give the instructions contained herein.

5.4 **No joint controllership.** The Parties acknowledge and agree that, with respect to the Processing of Customer Personal Data in connection with the PageMind Service, **Customer is the Controller** (or, where applicable, a processor acting on behalf of a third-party controller) and **Processor is a processor** only. Nothing in this DPA or in the Principal

Agreement is intended to create, or shall be construed as creating, a relationship of joint controllership between the Parties.

5.5 **Processor's reliance.** Processor is entitled to rely on the representations and warranties given by Customer in this DPA and the Principal Agreement. Processor shall have no liability (to the maximum extent permitted by law and subject to any limitations agreed in the Principal Agreement) for any Processing carried out in accordance with Customer's instructions that results in a breach of Applicable Data Protection Law, to the extent that such breach is attributable to Customer's acts or omissions, including Customer's failure to comply with Clause 5.3.

6. OBLIGATIONS OF THE PROCESSOR

6.1 **Compliance with documented instructions.** Processor shall Process Customer Personal Data only on documented instructions from Customer, as set out in this DPA, the Principal Agreement, and any additional written instructions that Customer may reasonably issue from time to time in accordance with Clause 5.1, except where Processing is required by Union or Member State law to which Processor is subject. In such a case, Processor shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

6.2 **No further use.** Processor shall not use Customer Personal Data for its own purposes or for the purposes of any third party, except: (a) as strictly necessary to perform the PageMind Service and related support in accordance with this DPA and the Principal Agreement; (b) to comply with legal obligations; or (c) as set out in Clause 3.1(d) in relation to aggregated statistics and metrics derived from the Processing of Customer Personal Data that do not enable identification of any Data Subject by Customer or any third party and do not disclose Customer's business secrets.

6.3 **Confidentiality.** Processor shall ensure that any person acting under its authority who has access to Customer Personal Data, including employees, agents, contractors and Sub-processors:

(a) is bound by an appropriate duty of confidentiality (whether statutory, professional or contractual); and
(b) Processes Customer Personal Data only on instructions of Processor and, in turn, only in accordance with Customer's documented instructions as described in this DPA.

6.4 **Records of Processing.** Processor shall maintain records of Processing activities carried out on behalf of Customer as required by Article 30(2) GDPR (to the extent applicable) and shall make such records available to competent Supervisory Authorities upon request, as required by Applicable Data Protection Law. Upon Customer's reasonable written request, Processor shall provide Customer with summary information regarding such records that is sufficient to demonstrate Processor's compliance with this DPA, subject to appropriate confidentiality protections.

6.5 **Data protection by design and by default.** Taking into account the state of the art, the cost of implementation, the nature, scope, context and purposes of Processing, and the risks of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall implement appropriate technical and organisational measures designed to meet the principles of data protection by design and by default, including measures to ensure that, by default, only Personal Data which are necessary for each specific purpose of the Processing are processed.

6.6 **Security of Processing.** Processor shall implement and maintain appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk, including, as appropriate, the measures listed in Annex 2. In particular, Processor shall:

(a) protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to such data;
(b) ensure ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
(c) restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident, to the extent such data are stored by Processor; and
(d) regularly test, assess and evaluate the effectiveness of the Technical and Organisational Measures for ensuring the security of Processing.

6.7 **Changes to measures.** Processor may update or modify the Technical and Organisational Measures from time to time, provided that such updates or modifications do not result in a material degradation of the overall level of security and protection afforded to Customer Personal Data. On request, Processor shall provide a description of the then-current measures.

6.8 **Use of Sub-processors.** Where Processor engages Sub-processors as permitted under Clause 7, Processor shall ensure that such Sub-processors are contractually bound to comply with data protection obligations which are no less protective of Customer Personal Data than those imposed on Processor under this DPA, to the extent applicable to the nature of the services provided by the Sub-processor. Processor shall remain responsible towards Customer for the performance of its Sub-processors as set out in Clause 7.

6.9 **Assistance.** Processor shall provide reasonable assistance to Customer, taking into account the nature of the Processing and the information available to Processor, in order to enable Customer to fulfil its obligations under Applicable Data Protection Law, including obligations relating to data security, data protection impact assessments, prior consultations with Supervisory Authorities, and responses to Data Subject Requests, as further detailed in Clause 10. Such assistance shall be limited to the provision of existing information, documentation and tools made available as part of the PageMind Service and shall not require Processor to (i) implement changes to the PageMind Service for the benefit of a single Customer, (ii) carry out disproportionate manual analysis or searches of unstructured Customer files, or (iii) provide legal or regulatory advice.

6.10 **Restrictions on disclosure.** Processor shall not disclose Customer Personal Data to any third party except:

(a) to Sub-processors in accordance with Clause 7;
(b) as instructed or authorised by Customer; or
(c) where required to do so by Union or Member State law to which Processor is subject, in which case Processor shall (to the extent legally permitted) notify Customer of such requirement before making any disclosure.

---

7. USE OF SUB-PROCESSORS

7.1 **General authorisation.** Customer hereby grants Processor a general written authorisation to engage Sub-processors for the Processing of Customer Personal Data in connection with the PageMind Service, subject to the conditions set out in this Clause 7.

7.2 **Current Sub-processors.** As at the Effective Date of this DPA, Processor uses the categories of Sub-processors described in Annex 3 for the purposes set out therein. The specific Sub-processor entities engaged by Processor from time to time (including their locations and roles) are identified in Processor's then-current Sub-processor List, which is made available to Customer on request or by publication at a URL notified to Customer. Annex 3 and the Sub-processor List together form part of this DPA.

7.3 **Addition or replacement of Sub-processors.** Processor may appoint new Sub-processors or replace existing Sub-processors, provided that:

(a) Processor notifies Customer of the intended change (including the name, location and role of the Sub-processor) in advance by email or via an in-product notification or public sub-processor list update; and
(b) Customer has the right to object to such change on reasonable, documented grounds relating to the protection of Customer Personal Data, within the objection period specified in the notice (which shall not be shorter than thirty (30) days from notification, unless a shorter period is required for urgent operational reasons).

7.4 **Customer's right to object.** If Customer objects to a proposed Sub-processor within the applicable objection period, Customer shall provide Processor with a written explanation of its reasonable grounds for objection. The Parties shall discuss in good faith to resolve the objection, including by:

(a) Processor proposing alternative measures to address the objection;
(b) Customer agreeing to use the PageMind Service without the involvement of the relevant Sub-processor (for example by disabling a particular feature); or
(c) where no resolution is possible within a reasonable period and Customer's objection is based on reasonable, documented data protection grounds in accordance with Clause 7.3(b), allowing Customer to terminate the affected part of the PageMind Service on written notice. In such case, Customer shall be entitled, as its sole and exclusive remedy, to a pro-

rated refund of any fees prepaid specifically for the terminated portion of the PageMind Service in respect of the period after the effective date of termination; no refund shall be due in respect of services already performed.

For the avoidance of doubt, if Customer’s objection to a Sub-processor is not based on reasonable, documented data protection grounds, any termination and refund rights shall be governed exclusively by the Principal Agreement, and no refund shall arise under this Clause 7.4.

7.5 **No automatic breach.** Customer acknowledges that an objection to a Sub-processor may prevent Processor from providing some or all of the PageMind Service features. Processor shall not be deemed in breach of the Principal Agreement or this DPA to the extent any non-performance is caused by Customer’s objection to a Sub-processor and Processor’s compliance with such objection.

7.6 **Flow-down of obligations.** Processor shall enter into a written agreement with each Sub-processor that imposes on the Sub-processor, in substance, the same data protection obligations as those set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of Applicable Data Protection Law.

7.7 **Responsibility for Sub-processors.** Processor shall remain liable to Customer for the performance of its obligations under this DPA, including where such obligations are performed by a Sub-processor, except to the extent any failure is directly attributable to Customer or to limitations imposed by Customer (such as an objection to a Sub-processor that results in restricted functionality).

---

8. INTERNATIONAL TRANSFERS

8.1 **Primary Processing locations.** Processor will Process Customer Personal Data primarily within data centres located in the EEA and/or other jurisdictions officially recognised by the European Commission as providing an adequate level of data protection under Article 45 GDPR, to the extent this is compatible with the PageMind Service architecture and Processor’s infrastructure.

8.2 **Transfers to Third Countries.** Where the Processing of Customer Personal Data involves a transfer to a Third Country (whether by Processor or a Sub-processor), Processor shall ensure that such transfer takes place only:

(a) to a Third Country in respect of which the European Commission has adopted an adequacy decision pursuant to Article 45 GDPR; or
(b) pursuant to appropriate safeguards in accordance with Article 46 GDPR, such as the Standard Contractual Clauses, including any supplementary measures that may be required in light of the case-law of the Court of Justice of the European Union and guidance

from Supervisory Authorities; or
(c) in any other circumstances permitted by Chapter V GDPR.

8.3 **Implementation of transfer mechanisms.** Where the Standard Contractual Clauses or other appropriate safeguards are used:

(a) Processor shall ensure that the relevant Sub-processors enter into the applicable module(s) of the Standard Contractual Clauses with Processor or, where required, directly with Customer;
(b) to the extent the Standard Contractual Clauses are incorporated by reference into this DPA or the Principal Agreement, they shall form an integral part thereof and shall prevail in the event of any conflict with the terms of this DPA or the Principal Agreement relating to international transfers; and
(c) Processor shall, upon Customer's reasonable request, provide copies of the relevant transfer mechanisms, redacted as necessary to protect business secrets or other confidential information.

8.4 **Changes in legal framework.** If a legal or regulatory change, court decision, or decision of a competent authority results in the mechanisms relied upon under Clause 8.2 no longer ensuring a lawful transfer of Customer Personal Data to a Third Country, Processor shall:

(a) promptly inform Customer;
(b) use commercially reasonable efforts to implement alternative lawful transfer mechanisms or supplementary measures; and
(c) where no suitable solution can be implemented within a reasonable time, be entitled to suspend or terminate the affected Processing and/or the affected portion of the PageMind Service, without this constituting a breach of the Principal Agreement or this DPA. In such case, Customer shall be entitled to a pro-rated refund of any prepaid unused fees for the affected portion as its sole and exclusive remedy, without prejudice to any mandatory statutory rights.

8.5 **Customer instructions.** Customer shall not instruct Processor to transfer Customer Personal Data to a Third Country without first verifying that appropriate safeguards or derogations are in place under Applicable Data Protection Law. To the extent Customer requires Processor to implement specific transfer mechanisms or supplementary measures beyond those ordinarily used by Processor, such additional requirements shall be agreed in writing and may be subject to additional fees.

---

9. SECURITY AND TECHNICAL AND ORGANISATIONAL MEASURES

9.1 **Security measures.** Processor shall implement and maintain the Technical and Organisational Measures described in Annex 2 and such other measures as Processor deems appropriate from time to time in light of the nature of the Processing, the information processed and the risks identified. These measures are designed to protect

Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, and to ensure a level of security appropriate to the risk.

9.2 **Scope of measures.** The Technical and Organisational Measures shall include, as appropriate:

(a) physical and logical access controls to Processing systems and facilities;
(b) role-based access management, authentication and authorisation procedures;
(c) encryption of Customer Personal Data in transit over public networks and at rest where appropriate;
(d) network security controls, including segmentation, firewalls and intrusion detection or prevention measures;
(e) logging and monitoring of access and key Processing actions, including PageMind run logs and evidence packs;
(f) backup, disaster recovery and business continuity measures, including regular backups, testing of restore procedures and defined recovery time objectives;
(g) procedures for regular testing, assessment and evaluation of the effectiveness of security measures; and
(h) measures to ensure the integrity and traceability of PageMind Processing, including configuration fingerprints, hashing of inputs and outputs, and environment signatures to support audits and reproducibility.

9.3 **Customer's security responsibilities.** Customer is responsible for:

(a) properly configuring and using the PageMind Service, including managing user accounts, access rights and authentication mechanisms (such as passwords, API keys or SSO);
(b) securing the devices, networks and systems it uses to connect to the PageMind Service;
(c) protecting its own copies of Customer Personal Data, whether stored locally, in its own systems, or in third-party systems outside Processor's control; and
(d) ensuring that any transmission of Customer Personal Data to Processor takes place over secure channels and in accordance with Customer's own policies and Applicable Data Protection Law.

9.4 **Security incidents and vulnerabilities.** Processor shall maintain processes to detect, respond to and mitigate security incidents and vulnerabilities that may affect Customer Personal Data. Where Processor becomes aware of a Personal Data Breach affecting Customer Personal Data, Processor shall handle such breach in accordance with Clause 11.

9.5 **No guarantee of absolute security.** While Processor will implement and maintain the Technical and Organisational Measures described in this DPA, Customer acknowledges that no information system can be guaranteed to be 100% secure. Provided Processor has complied with its obligations under this DPA, Processor shall not be liable for any damages resulting solely from security incidents or vulnerabilities that were not reasonably preventable given the state of the art, unless otherwise provided in the Principal Agreement or required by mandatory law.

10. DATA SUBJECT RIGHTS AND ASSISTANCE

10.1 **Data Subject Requests.** Taking into account the nature of the Processing and the information and tools available to Processor, Processor shall assist Customer, insofar as this is reasonably possible, by appropriate technical and organisational measures for the fulfilment of Customer's obligations to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR (including rights of access, rectification, erasure, restriction of Processing, data portability, objection, and not to be subject to automated individual decision-making), primarily by making available the self-service functionalities, logs and documentation described in this Clause 10.

10.2 **Forwarding of requests.** If a Data Subject or third party contacts Processor directly with any request or complaint relating to Customer Personal Data, Processor shall not respond to such request or complaint except:

(a) to confirm that the request relates to Customer and that Processor is not authorised to respond directly; or
(b) where Processor is required by Applicable Data Protection Law to respond, in which case Processor shall, to the extent legally permitted, inform Customer of such requirement and provide a copy of any response.

Processor shall promptly forward any such request or complaint to Customer without undue delay.

10.3 **Customer responsibility.** Customer shall be responsible for:

(a) evaluating whether and how to respond to any Data Subject request relating to Customer Personal Data;
(b) providing, where appropriate, the response to the Data Subject; and
(c) ensuring that any response complies with Applicable Data Protection Law.

10.4 **Assistance with responses.** Upon Customer's written request, Processor shall provide reasonable assistance to Customer, insofar as this is possible and taking into account the nature of the Processing and the information available to Processor, by:

(a) making available and explaining the self-service tools and configuration options that Customer can use to search, retrieve, correct or delete Customer Personal Data within the PageMind Service;

(b) providing high-level information on the categories of Customer Personal Data Processed by Processor and on the relevant systems, locations and retention periods; and

(c) providing copies of logs or other existing records that specifically relate to Customer's use of the PageMind Service and are reasonably necessary to support Customer's response to a particular Data Subject request, provided that Processor shall not be required to (i) create new tools, interfaces or reports, (ii) carry out manual, file-by-file review of Supplier Materials or other unstructured content, or (iii) reconstruct historical Processing beyond what is available in existing logs, reports and backups. For the avoidance of doubt, Processor shall not be required to perform manual, file-by-file review of Supplier Materials or other unstructured Customer content, to develop bespoke tools or interfaces, or to undertake any activity that would amount to consultancy or professional services beyond what is expressly agreed and, where applicable, separately remunerated.

10.5 **Assistance with DPIAs and consultations.** Processor shall provide reasonable assistance to Customer, upon written request, in relation to:

(a) any data protection impact assessment ("DPIA") that Customer is required to carry out in relation to the Processing of Customer Personal Data via the PageMind Service; and
(b) any prior consultation with a Supervisory Authority regarding such Processing, to the extent required by Applicable Data Protection Law.

Such assistance shall be limited to providing available information about the Processing carried out by Processor, the Technical and Organisational Measures and the Sub-processors used. Any assistance under this Clause 10.5 that goes beyond Processor's standard security and product documentation may be subject to additional fees in accordance with Clause 10.6.

10.6 **Costs of assistance.** To the extent that assistance under this Clause 10 requires Processor to expend significant time or resources beyond what is reasonably included in the standard fees for the PageMind Service (for example, complex data extractions, bespoke documentation or participation in extensive regulatory consultations initiated by Customer), Processor may charge Customer for such assistance at its then-current professional services rates, provided that Processor notifies Customer in advance and Customer approves the additional work.

---

11. PERSONAL DATA BREACH NOTIFICATION

11.1 **Notification of Personal Data Breach.**
In the event of a Personal Data Breach affecting Customer Personal Data, Processor shall notify Customer without undue delay after becoming aware of the Personal Data Breach. Processor will use commercially reasonable efforts to provide such notification within seventy-two (72) hours of becoming aware of the breach, subject to the availability of sufficient information to confirm that a Personal Data Breach has occurred.

11.2 **Content of notification.** The notification referred to in Clause 11.1 shall, to the extent such information is available to Processor at the time of notification, include:

(a) a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and

approximate number of Personal Data records concerned;
(b) the name and contact details of the data protection contact or other contact point where more information can be obtained;
(c) a description of the likely consequences of the Personal Data Breach; and
(d) a description of the measures taken or proposed to be taken by Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide all information at the same time, Processor may provide the information in phases without undue further delay as it becomes available.

11.3 **Customer's responsibility for notifications.** Customer is responsible for determining whether it is required under Applicable Data Protection Law to notify the relevant Supervisory Authorities and/or affected Data Subjects of the Personal Data Breach. Processor shall not make such notifications on Customer's behalf unless expressly instructed to do so in writing by Customer or required by Applicable Data Protection Law.

11.4 **Cooperation.** Processor shall cooperate with Customer and take reasonable commercial steps as directed by Customer to assist in the investigation, mitigation and remediation of any Personal Data Breach, including by providing relevant logs, records and technical information, subject to reasonable limitations relating to security and confidentiality.

11.5 **No admission of liability.** Any notification or communication by Processor to Customer or to a Supervisory Authority or other third party in connection with a Personal Data Breach shall not be construed as an admission by Processor of fault or liability with respect to the Personal Data Breach or the underlying incident.

---

12. RETURN AND DELETION OF PERSONAL DATA

12.1 **Return or deletion at end of Processing.** Upon termination or expiry of the Principal Agreement or upon termination of the provision of the PageMind Service in whole or in part, Processor shall, at Customer's choice (communicated to Processor in writing within thirty (30) days of termination or expiry):

(a) return to Customer all Customer Personal Data Processed on behalf of Customer in the form of standard exports made available via the PageMind Service or by other reasonable means; or
(b) delete such Customer Personal Data in accordance with Clause 12.3.

If Customer does not provide instructions within such thirty (30) day period, Processor may delete Customer Personal Data in accordance with Clause 12.3.

12.2 **Customer's retrieval of data.** During the term of the Principal Agreement, Customer is responsible for exporting or otherwise retrieving its Customer Personal Data from the

PageMind Service as needed. Processor does not have an obligation to retain Customer Personal Data beyond the retention periods described in this DPA and the Principal Agreement.

12.3 **Deletion from active systems.** Subject to Clauses 12.4 and 12.5, Processor shall delete Customer Personal Data from its active systems and production databases within a commercially reasonable period following (a) Customer’s written request for deletion, or (b) the effective date of termination or expiry of the Principal Agreement, or (c) the end of any applicable grace period described in Clause 12.1, whichever is later. Deletion shall be performed in such a way that Customer Personal Data cannot reasonably be reconstructed or read.

12.4 **Backups and archives.** Customer acknowledges that Customer Personal Data may remain in Processor’s backups and archival systems for a limited period after deletion from active systems, in line with Processor’s backup and disaster recovery policies. Processor shall ensure that:

(a) such backups are kept securely and are subject to appropriate Technical and Organisational Measures;
(b) access to backups containing Customer Personal Data is strictly limited to personnel who need such access for backup and recovery purposes; and
(c) Customer Personal Data in backups is not restored to active systems or otherwise Processed except as necessary for backup integrity verification, disaster recovery or as required by law.

Customer Personal Data in backups shall be overwritten and permanently deleted in the ordinary course of Processor’s backup cycles, typically within a period not exceeding that stated in Annex 2 or Processor’s then-current security documentation.

12.5 **Retention required by law.** Processor may retain Customer Personal Data (or a portion thereof) where Processor is required to do so by Union or Member State law to which it is subject, including for the establishment, exercise or defence of legal claims or for compliance with statutory retention obligations. In such cases, Processor shall ensure that any retained Customer Personal Data is processed only for the purposes for which it is required under such law and is subject to appropriate Technical and Organisational Measures.

12.6 **Aggregated statistics and metrics.** Nothing in this DPA shall require Processor to delete or return data that does not constitute Personal Data. Processor may also generate, retain and use aggregated statistics and metrics derived from the Processing of Customer Personal Data for its own legitimate business purposes, including to improve and develop its services and for security, performance and analytics purposes, provided that any such outputs do not enable identification of any Data Subject by Customer or any third party and do not disclose Customer’s business secrets.

13. AUDITS AND INSPECTIONS

13.1 **Information and documentation.** Processor shall make available to Customer, upon reasonable written request, all information necessary to demonstrate Processor's compliance with its obligations under this DPA and Article 28 of the GDPR, including:

(a) summaries of policies and procedures relating to information security and data protection;
(b) descriptions of Technical and Organisational Measures;
(c) information regarding Sub-processors and international transfer mechanisms; and
(d) third-party attestations, certifications, audit reports or summaries thereof (if any) that Processor chooses to make available; and
(e) high-level information on the standard contractual clauses or other transfer mechanisms used for international transfers involving Sub-processors, and, where available, summaries or references to relevant third-party certifications or audit reports of such Sub-processors.

13.2 **Audit right.** Subject to Clauses 13.3 to 13.7, Customer or an independent third-party auditor mandated by Customer (who is not a competitor of Processor and who is bound by appropriate confidentiality obligations) shall have the right to conduct an audit or inspection of Processor's Processing of Customer Personal Data, solely to verify Processor's compliance with this DPA and Applicable Data Protection Law as a processor.

13.3 **Conditions of audit.** Any audit or inspection shall be:

(a) carried out no more than once in any rolling twelve (12) month period, except where required by a Supervisory Authority or where there are reasonable grounds to suspect a material breach of this DPA;
(b) conducted with at least thirty (30) days' prior written notice to Processor, unless shorter notice is required by a Supervisory Authority;
(c) undertaken during Processor's normal business hours and in a manner that minimises disruption to Processor's business operations; and
(d) limited in scope to systems, processes and documentation directly related to the Processing of Customer Personal Data.

13.4 **Use of existing audits and certifications.** Before initiating any on-site audit, Customer agrees to first review the information and third-party audit reports or certifications made available by Processor in accordance with Clause 13.1. Customer agrees that these materials, together with any written responses provided by Processor, may satisfy Customer's audit requirements where they provide reasonably sufficient evidence of Processor's compliance. On-site inspections of Processor's premises or data centres shall be used only as a last resort and shall be permitted only where, following such review and any remote audit measures reasonably proposed by Processor, Customer can demonstrate that a remote audit is objectively insufficient to verify Processor's compliance with this DPA.

13.5 **Confidentiality.** Customer shall ensure that any persons conducting an audit on its behalf are bound by confidentiality obligations no less stringent than those contained in the Principal Agreement. Customer shall not, and shall procure that auditors do not, access or obtain information relating to other customers of Processor or to Processor's trade secrets, proprietary information or security details beyond what is strictly necessary to verify compliance with this DPA.

13.6 **Costs.** Customer shall bear all costs and expenses associated with any audit or inspection it initiates. If an audit reveals a material breach by Processor of this DPA or Applicable Data Protection Law, Processor shall bear its own costs of remediation. Processor may charge Customer at its standard professional services rates for time spent by Processor's personnel in supporting an audit that goes beyond the provision of existing documentation, unless the audit is mandated by a Supervisory Authority specifically due to Processor's suspected non-compliance.

13.7 **Regulatory audits.** Nothing in this DPA shall restrict or limit the rights of a Supervisory Authority to access Processor's premises or systems directly in accordance with Applicable Data Protection Law. Processor shall promptly inform Customer of any regulatory audit relating to the Processing of Customer Personal Data, to the extent lawful, and shall share non-confidential outcomes relevant to Customer where appropriate.

---

14. LIABILITY AND ALLOCATION OF RISK

14.0 **Relationship with GDPR Article 82**
Nothing in this DPA is intended to, or shall be construed as, limiting the rights of Data Subjects under Article 82 GDPR or the powers of competent supervisory authorities. Any limitations and allocations of liability agreed between the Parties in this Clause 14 apply only as between the Parties and do not affect the ability of Data Subjects or supervisory authorities to bring claims directly against either Party under Applicable Data Protection Law.

14.1 **Application of Principal Agreement.** The limitations and exclusions of liability set out in the Principal Agreement (including any caps on liability, exclusions of indirect or consequential damages, and any specific indemnities) shall apply to all claims arising in connection with this DPA, including any claims arising from or related to the Processing of Customer Personal Data, to the fullest extent permitted by Applicable Data Protection Law.
Without prejudice to the rights of data subjects under Applicable Data Protection Law, the Parties expressly agree that any contractual liability of Processor towards Customer arising out of or in connection with this DPA (including in relation to any Personal Data Breach, regulatory investigation or administrative fine imposed on Customer) shall be subject to and limited by the exclusions and caps set out in the Principal Agreement.

14.2 **No enlargement of liability.** Nothing in this DPA is intended to, or shall be construed as, increasing Processor's liability or Customer's rights beyond the limitations agreed in the Principal Agreement, except to the limited extent that such limitations would be void or unenforceable under mandatory Applicable Data Protection Law.

14.3 **Customer's responsibility for legal compliance.** Customer acknowledges that:

(a) Customer, as Controller (or as a processor acting on behalf of a third-party controller), is responsible for its own compliance with Applicable Data Protection Law in relation to Customer Personal Data, including for decisions about using the PageMind Service and relying on its outputs;
(b) Processor has no control over the content, accuracy or completeness of Customer Personal Data or over the configuration and use of the PageMind Service by Customer; and
(c) Customer remains solely responsible for verifying any outputs generated by the PageMind Service (including but not limited to catalog attributes, translations, energy-label information and compliance fields) before using such outputs in production systems or disclosing them to third parties.

14.4 **Exclusions of Processor's liability.** Without prejudice to Clauses 14.1 and 14.2 and subject always to any mandatory statutory limitations, Processor shall not be liable for any loss, damage or regulatory sanction arising from:

(a) Customer's failure to comply with its obligations as Controller under Applicable Data Protection Law;
(b) Customer's failure to configure or use the PageMind Service in accordance with the Principal Agreement, this DPA or Processor's documentation;
(c) Customer's decision to publish or otherwise rely upon outputs generated by the PageMind Service without appropriate human review and validation;
(d) any Customer instruction that Processor reasonably considers to be unlawful or that Processor has notified as potentially unlawful in accordance with Clause 5.2, where Customer insists on such instruction; or
(e) Customer's upload of Personal Data that is excessive, irrelevant, or falls into categories (such as Special Categories of Personal Data or criminal-conviction data) that are not intended to be Processed by the PageMind Service.

14.5 **Customer indemnity.** Subject always to any mandatory statutory limitations under Applicable Data Protection Law, Customer shall indemnify and hold harmless Processor from and against any claims, damages, fines, penalties or costs (including reasonable legal fees) arising out of or in connection with:

(a) Customer's breach of this DPA or the Principal Agreement in relation to Customer Personal Data; or
(b) Customer's failure to comply with its obligations as Controller (or as a processor acting on behalf of a controller) under Applicable Data Protection Law, including obligations relating to transparency, legal basis, Data Subject rights, DPIAs and international transfers,

except to the extent that such claims, damages, fines, penalties or costs result from Processor's own breach of this DPA or Applicable Data Protection Law. This indemnity covers, in particular, any reasonable costs of investigation and defence, and any administrative fines or sanctions imposed on Processor by a Supervisory Authority, to the extent that such measures result primarily from Customer's breach of this DPA, the Principal Agreement or Applicable Data Protection Law, and subject always to any mandatory statutory limitations.

---

15. MISCELLANEOUS

15.1 **Order of precedence.** In the event of any inconsistency between this DPA and the Principal Agreement, the hierarchy and order of precedence provisions set out in the Principal Agreement (including, where applicable, the PageMind Terms of Service) shall apply, it being understood that this DPA governs the allocation of roles and obligations for the Processing of Customer Personal Data. In the event of any inconsistency between this DPA and any Standard Contractual Clauses or other transfer mechanism executed between the Parties, the terms of such clauses or mechanism shall prevail to the extent of the inconsistency in relation to international transfers of Personal Data.

15.2 **Amendments.** Processor may propose reasonable updates to this DPA from time to time to reflect changes in Applicable Data Protection Law, the PageMind Service, or Processor's Sub-processors or Technical and Organisational Measures. Processor shall notify Customer of any material changes and, where required by law, obtain Customer's consent. If Customer does not agree to a proposed update that is necessary for compliance with Applicable Data Protection Law, Processor may, after good-faith efforts to reach agreement, suspend or terminate the affected Processing and/or the affected portion of the PageMind Service upon written notice.

15.3 **Severability.** If any provision of this DPA is held to be invalid or unenforceable by a court of competent jurisdiction, such provision shall be deemed modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions shall remain in full force and effect.

15.4 **Governing law and jurisdiction.** This DPA shall be governed by and construed in accordance with the governing law specified in the Principal Agreement. Any disputes arising out of or in connection with this DPA shall be subject to the exclusive or non-exclusive jurisdiction (as applicable) specified in the Principal Agreement.

15.5 **Counterparts and electronic signatures.** This DPA may be executed in any number of counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument. Signatures provided by electronic means (including click-through acceptance, electronic signature platforms or scanned signatures) shall have the same legal effect as original signatures to the fullest extent permitted by Applicable Data Protection Law.

15.6 **Entire agreement on Processing.** This DPA, together with the Principal Agreement and any incorporated Standard Contractual Clauses or other applicable transfer mechanisms, constitutes the entire agreement between the Parties with respect to the Processing of Customer Personal Data in connection with the PageMind Service and supersedes all prior or contemporaneous agreements, understandings or representations relating to such Processing, except where expressly stated otherwise.

ANNEX 1 – DESCRIPTION OF PROCESSING ACTIVITIES (PAGEMIND SERVICE)

1. **Subject-matter of Processing**
   Processor provides the PageMind Service, which automates catalog operations for retail and e-commerce clients by ingesting, parsing, transforming and structuring product-related information from Supplier Materials and other Customer inputs into catalog-ready outputs, QA artefacts and evidence packs. Processing covers all Customer Personal Data that may be included in such materials or generated as part of the operation of the PageMind Service.

2. **Nature of Processing**
   Processing operations performed by Processor may include, as applicable:

- Collection and receipt of Supplier Materials and other Customer inputs (files, data feeds, API payloads, manual entries);
- Storage and organisation of such materials in workspaces, projects, batches or equivalent logical structures;
- Reading and parsing of documents, including OCR and structured/unstructured extraction;
- Machine translation and localisation of text elements;
- Normalisation, enrichment and mapping of attributes to Customer-defined schemas and templates;
- Comparison and reconciliation of information from multiple sources (for example, Supplier Materials vs. official registries, including EPREL or other energy-label registries, where enabled);
- Generation of structured outputs (e.g. CSVs, JSON, API payloads, configuration bundles) aligned with Customer’s catalog templates;
- Generation of QA and retry lists, issue flags, completeness scores and similar artefacts;
- Generation of run reports, audit logs, evidence packs and configuration fingerprints to support traceability and reproducibility;
- Storage, indexing and querying of logs and technical metadata relating to runs, jobs, workflows, users and workspaces;
- Deletion, restriction, pseudonymisation and archiving, as configured by Customer or required by law.

3. **Purposes of Processing**

Processor Processes Customer Personal Data strictly for the following purposes, as further detailed in Clause 3 of the DPA:

- Provision, operation and maintenance of the PageMind Service;
- Provision of support, incident response and problem resolution;
- Security monitoring, threat detection, abuse prevention and service integrity;
- Service quality, performance monitoring and optimisation;
- Creation and use of aggregated statistics and metrics derived from Processing of Customer Personal Data for security, performance monitoring, product improvement and business analytics, subject to the strict prohibition on training shared AI models using Customer Personal Data as defined in Clause 3.1(d) of the DPA;
- Compliance with legal obligations and responses to lawful requests.

4. **Types of Customer Personal Data**

Depending on Customer's configuration and the materials it uploads, the PageMind Service may Process the following types of Personal Data:

- **Identification and contact data**:
  - Name, surname;
  - Job title, function or role;
  - Employer or organisation name;
  - Business email address, business phone number, fax number;
  - Business postal address.
- **Professional and organisational data**:
  - Department or team;
  - Country, region or market responsibility;
  - Relationship to Customer or its suppliers (e.g. account manager, category manager, technical contact).
- **Electronic identifiers and technical data**:
  - Usernames, internal user IDs or workspace identifiers;
  - Timestamps and metadata embedded in documents (author, creation date, modification history);
  - IP addresses and device identifiers captured in logs;
  - Session identifiers and activity logs.
- **Content-related data**:
  - Names, contact blocks and other personal details that may be present in Supplier Materials (e.g. signatures, letterheads, email footers, author credits);

  - Free-text notes entered by Customer's users that may contain Personal Data.

Customer shall ensure that unnecessary Personal Data is not included in Supplier Materials or free-text inputs where such inclusion is not required for the purposes of the PageMind Service.

5. **Categories of Data Subjects**

Customer Personal Data relates, in particular, to the following categories of Data Subjects:

- Employees, contractors, consultants and representatives of Customer who use the PageMind Service or whose details appear in Customer's documents;
- Employees, contractors, consultants and representatives of Customer's suppliers, brands, manufacturers, distributors and other business partners whose details are included in Supplier Materials;
- Other individuals whose names or contact information may appear incidentally in documents or data provided to the PageMind Service by or on behalf of Customer.

6. **Duration of Processing**

- Processor shall Process Customer Personal Data for the term of the Principal Agreement, subject to the provisions on return and deletion set out in Clause 12 of the DPA.
- Upon termination or expiry of the Principal Agreement, Customer Personal Data will be deleted from active systems within a commercially reasonable period and retained only in backups and archives for the limited retention periods defined in Annex 2, unless a longer retention period is required by law or expressly agreed in writing between the Parties.

7. **Special Categories of Data and Criminal Data**

- The Parties do not anticipate Processing of Special Categories of Personal Data or data relating to criminal convictions and offences.
- To the extent Customer nevertheless uploads such data in breach of the DPA, Processor may restrict or delete such data and shall not be liable for any resulting loss or damage, without prejudice to any mandatory obligations under Applicable Data Protection Law.
- Any deliberate Processing of Special Categories of Personal Data or criminal data shall require an additional written agreement between the Parties and may be subject to additional safeguards and fees.

ANNEX 2 – TECHNICAL AND ORGANISATIONAL MEASURES

The following Technical and Organisational Measures ("TOMs") are implemented by Processor in relation to the PageMind Service and Customer Personal Data. Processor may update or modify these TOMs from time to time, provided that the overall level of protection is not materially reduced.

1. **Organisation of Information Security**

1.1 Information security is managed at company level, with clearly assigned responsibilities and escalation paths for security incidents.

1.2 Staff with access to Customer Personal Data are bound by confidentiality obligations and receive training on information security and data protection appropriate to their role.

1.3 Processor maintains internal policies and procedures covering information security, access control, acceptable use, incident response, backup and recovery, change management and vendor management.

2. **Physical and Environmental Security**

2.1 PageMind’s production systems are hosted in secure data centres operated by reputable infrastructure providers, with industry-standard physical protections, including:

- Controlled access to facilities (badges, guards, CCTV);
- Environmental controls (power redundancy, fire suppression, climate control);
- Visitor registration and escort policies.

2.2 Processor does not typically store Customer Personal Data on its own premises except for limited support or administrative purposes; where such storage occurs, it is subject to appropriate physical security controls (locked offices, restricted access).

3. **Network and System Security**

3.1 Production systems are deployed in isolated virtual private cloud (VPC) environments with network segmentation and firewalling to restrict inbound and outbound traffic to what is strictly necessary for operation of the PageMind Service.

3.2 Access to management interfaces and administrative endpoints is restricted via security groups, VPN, IP allow-listing and/or other access-control mechanisms.

3.3 Processor uses industry-standard protections (such as TLS) to encrypt Customer Personal Data in transit over public networks.

3.4 Processor employs network monitoring and logging to detect anomalous activity and potential intrusion attempts, subject to proportionality and privacy requirements.

4. **Access Control and Authentication**

4.1 Access to Customer Personal Data within PageMind is governed by role-based access control (RBAC). Each user is assigned one or more roles defining their permissions within Customer’s workspace(s).

4.2 Authentication to the PageMind Service is enforced via secure mechanisms (e.g. passwords meeting minimum complexity rules, and/or single sign-on where integrated).

4.3 Administrative access to production systems (including databases, orchestration layers and monitoring tools) is restricted to a limited set of authorised personnel and is protected by strong authentication (e.g. SSH keys, multi-factor authentication where applicable).

4.4 Access rights are granted on a need-to-know basis and are periodically reviewed and revoked when no longer required (for example, when personnel change roles or leave employment).

5. **Data Storage, Encryption and Separation**

5.1 Customer Personal Data stored in databases or file stores managed by Processor is encrypted at rest using industry-standard encryption algorithms.

5.2 Logical separation is implemented between different customers' data through the use of separate workspaces, projects or equivalent isolation mechanisms at the application and/or database layer.

5.3 Temporary working copies of data (for example, intermediate files used during Processing) are stored in controlled locations and are deleted or overwritten when no longer needed.

6. **Logging, Monitoring and Traceability**

6.1 PageMind maintains application-level logs capturing relevant events, including:

- Authentication and authorisation events;
- Creation, modification and deletion of workspaces, projects and runs;
- Key Processing actions and errors;
- Administrative and support actions taken by authorised Processor staff.

6.2 For PageMind Processing runs, the service captures:

- Input and output identifiers and hashes;
- Configuration fingerprints (including model versions, templates, mapping rules and environment identifiers);
- Evidence objects (such as document snippets or registry responses) linked to specific fields where available;
- Timestamps and execution metadata.

6.3 Logs are protected against unauthorised access and tampering and are retained for limited periods necessary for security, support, traceability and audit, typically not exceeding twelve (12) months unless a longer period is justified (e.g. ongoing incident, legal hold or audit requirement).

7. Backup, Business Continuity and Disaster Recovery

7.1 Processor maintains regular backups of key production databases and storage volumes that may contain Customer Personal Data.

7.2 Backups are encrypted and stored in secure locations separate from primary systems, with access restricted to authorised personnel.

7.3 Processor maintains procedures for restoration from backups and periodically tests backup restoration as part of its business continuity planning.

7.4 Customer Personal Data in backups is retained only for the duration of the applicable backup cycle, which shall not normally exceed thirty (30) days after deletion from active systems, unless a longer retention period is required by law or explicitly agreed with Customer.

8. Vulnerability Management and Change Management

8.1 Processor operates a process for identifying, assessing and addressing security vulnerabilities, including the evaluation of vendor security advisories, public vulnerability disclosures and internal findings.

8.2 Patches and updates to operating systems, databases, frameworks and application components are applied on a risk-based schedule, prioritising vulnerabilities with high severity or exploitable impact.

8.3 Changes to production systems are subject to change-management controls, including testing, peer review and approval, to reduce the risk of introducing security defects.

9. Incident Detection and Response

9.1 Processor maintains an incident response process for detecting, reporting and managing security incidents that may affect the confidentiality, integrity or availability of Customer Personal Data.

9.2 Incidents are triaged, investigated and remediated according to their severity and potential impact, with escalation paths up to senior management for significant events.

9.3 Personal Data Breaches are handled in accordance with Clause 11 of the DPA, including notification to Customer and, where appropriate, support for Customer’s own notification obligations.

10. Privacy by Design and Default

10.1 When developing or modifying the PageMind Service, Processor considers privacy and data protection principles at the design stage, including minimisation of Personal Data processed, pseudonymisation where possible, and limitation of retention.

10.2 Default service configurations are designed to avoid unnecessary Processing of Personal Data where feasible and to give Customer control over data retention and export.

11. **Personnel and Training**

11.1 Processor provides employees and relevant contractors with training on information security and data protection appropriate to their role, including obligations relating to the handling of Customer Personal Data.

11.2 Access to Customer Personal Data by Processor staff is limited to those who require such access for the performance of their job duties (for example, support engineers resolving specific Customer issues).

12. **Incident Management Standards**

12.1 Processor maintains a documented Incident Response Plan that includes procedures for detection, triage, containment, and recovery.

12.2 Processor tests its incident response capabilities at least annually (e.g., via tabletop exercises or technical drills) to ensure the effectiveness of these measures.

ANNEX 3 – SUB-PROCESSORS

1. **General**

1.1 Processor uses certain Sub-processors to support the provision of the PageMind Service, including infrastructure providers, AI/ML providers, monitoring tools and support tooling.

1.2 Processor maintains an up-to-date list of Sub-processors (the “Sub-processor List”), which is made available to Customer on request, **attached to this DPA as Appendix A (if provided in hard copy)**, or at a dedicated URL notified to Customer.

1.3 For each Sub-processor, the Sub-processor List indicates:

- Name and corporate identity of the Sub-processor;
- Location(s) where Processing is performed;
- Description of the Processing activities carried out;
- Applicable transfer mechanism where Processing involves transfers to Third Countries.

2. **Current Sub-processors**

As at the Effective Date of this DPA, Processor uses the categories of Sub-processors set out below. The specific entities within each category, together with their locations and roles, are listed in the Sub-processor List referred to in section 1.2 of this Annex 3:

- **Cloud infrastructure provider(s)**: hosting of application servers, databases, storage volumes and networking components supporting the PageMind Service.
- **Managed database and storage services**: provision of managed relational or non-relational databases, blob storage and related services.
- **Logging and monitoring providers**: collection and analysis of logs and telemetry for performance, reliability and security purposes.
- **Email and communication providers**: sending of email notifications and customer communications related to the PageMind Service.
- **AI/ML and OCR providers**: provision of large language models, translation engines, OCR engines and other AI/ML capabilities used by the PageMind Service to analyse and transform content.
- **Support and ticketing systems**: management of customer support requests, including limited Processing of contact details and issue descriptions.

3. **Notification of Changes**

3.1 Processor will notify Customer of any intended addition or replacement of a Sub-processor by updating the Sub-processor List and/or sending a notice to the email address associated with Customer's account, in accordance with Clause 7 of the DPA.

3.2 Customer may object to the appointment of a new Sub-processor within the time period specified in such notice, on reasonable, documented data protection grounds only.

4. **Sub-processor Agreements and Safeguards**

4.1 Processor enters into written agreements with Sub-processors that:

- impose obligations on the Sub-processor that are no less protective of Customer Personal Data than those imposed on Processor under this DPA, to the extent applicable;
- require the Sub-processor to implement appropriate technical and organisational measures; and
- address international transfers using legally valid mechanisms where required.

4.2 Processor remains responsible towards Customer for the performance of its Sub-processors in accordance with Clause 7 of the DPA.

ANNEX 4 – INTERNATIONAL TRANSFER MECHANISMS

1. **Adequacy Decisions**

Where Customer Personal Data is transferred to a country or territory that has been recognised by the European Commission as providing an adequate level of protection for Personal Data under Article 45 GDPR, such transfer shall not require additional safeguards under Chapter V GDPR.

2. **Standard Contractual Clauses and Other Appropriate Safeguards**

2.1 For transfers of Customer Personal Data to Third Countries that are not subject to an adequacy decision, Processor (or its relevant Sub-processor) shall implement appropriate safeguards in accordance with Article 46 GDPR. These may include execution of the Standard Contractual Clauses adopted by the European Commission, or equivalent clauses or mechanisms approved by a competent authority.

2.2 Where the Standard Contractual Clauses are used, the following principles apply:

- The Parties (and/or Processor and relevant Sub-processors) shall execute the appropriate module(s) of the Standard Contractual Clauses (for example, Controller-to-Processor or Processor-to-Processor) as required.
- The Standard Contractual Clauses shall be deemed incorporated by reference into this DPA and, where applicable, into the Principal Agreement.
- In the event of a conflict between the Standard Contractual Clauses and any provisions of this DPA or the Principal Agreement relating to international transfers, the Standard Contractual Clauses shall prevail.

2.3 Processor will evaluate, where appropriate, whether any supplementary measures are required to ensure that transfers afford an essentially equivalent level of protection to that guaranteed within the EEA, having regard to applicable laws in the destination country and guidance from the Court of Justice of the European Union and Supervisory Authorities.

3. **Documentation and Disclosure**

3.1 Upon Customer's reasonable written request, Processor shall provide high-level information about the transfer mechanisms it relies upon for specific Sub-processors or categories of transfers, subject to redaction of confidential or commercially sensitive details.

3.2 Processor is not obliged to disclose full copies of Sub-processor agreements or detailed security architecture documentation, provided that sufficient information is made available to enable Customer to assess compliance with Applicable Data Protection Law.

ANNEX 5 – AUDIT PROCEDURE (SUMMARY)

This Annex supplements Clause 13 of the DPA and sets out a non-exhaustive standard procedure for conducting audits of Processor's compliance with this DPA.

1. **Audit Request**

1.1 Customer submits a written audit request specifying:

- The legal or contractual basis for the audit;

- The objectives and scope (e.g. security controls, Processing records, Sub-processor management);
- The proposed dates and duration.

1.2 Processor and Customer shall agree on a mutually acceptable schedule and scope, taking into account ongoing operations and resource constraints.

2. **Pre-Audit Information Review**

2.1 Before any on-site or in-depth audit, Customer shall review:

- Documentation and information provided by Processor under Clause 13.1;
- Any available third-party certifications, attestations or summaries (e.g. SOC reports, ISO certifications or equivalent);
- Processor's Sub-processor List and security overview.

2.2 If, after reviewing such materials, Customer reasonably concludes that additional verification is required, an on-site or remote audit may be planned.

3. **Conduct of Audit**

3.1 Audits shall be performed:

- By Customer or by an independent auditor appointed by Customer and approved by Processor (such approval not to be unreasonably withheld where the auditor is appropriately qualified and not a competitor of Processor);
- In accordance with professional standards;
- In a manner that minimises disruption to Processor's normal business activities.

3.2 Auditors may:

- Interview relevant Processor personnel responsible for information security, operations and compliance;
- Review relevant policies, procedures and records;
- Inspect systems and facilities that Process Customer Personal Data, subject to security limitations;
- Test selected controls where this can be done safely and without impacting other customers or operations.

3.3 Auditors shall not:

- Access data belonging to other customers;
- Access source code or detailed network diagrams except where strictly necessary and agreed in advance;
- Remove any physical or digital documents from Processor's premises (copies may be provided where appropriate and subject to redaction).

4. Reporting and Remediation

4.1 Following an audit, Customer (or its auditor) shall provide Processor with a summary report highlighting any findings relevant to Processor's compliance with this DPA.

4.2 If the audit identifies any material non-compliance with this DPA, the Parties shall agree on a remediation plan, including reasonable timelines for remediation. Processor shall implement agreed remedial actions within those timelines, taking into account the severity and impact of the issues identified.

4.3 Any audit reports and findings shall be treated as confidential information of Processor and shall be used only for the purposes of verifying compliance with this DPA and Applicable Data Protection Law.

5. Costs and Frequency

5.1 The frequency and cost allocation for audits are governed by Clause 13 of the DPA.

5.2 Unless otherwise required by a Supervisory Authority or mandated by law, follow-up audits to verify remediation shall be limited to confirming that specific issues identified in a previous audit have been adequately addressed.

ANNEX 6 – SPECIAL CATEGORIES OF DATA (OPTIONAL)

1. Default Position

1.1 By default, the Parties agree that Customer shall **not** intentionally provide Special Categories of Personal Data or Personal Data relating to criminal convictions and offences to the PageMind Service.

1.2 Any incidental Processing of such data (for example, where such data is inadvertently included in Supplier Materials) is unintended, and Customer remains responsible for ensuring that such inclusion is minimised or prevented where reasonably possible.

2. Optional Additional Agreement

2.1 If Customer requires Processor to Process Special Categories of Personal Data or personal data relating to criminal convictions and offences as part of the PageMind Service, the Parties shall enter into a separate written agreement or an addendum to this Annex specifying:

- The specific categories of Special Categories or criminal data to be Processed;
- The purposes for which such data will be Processed;
- The legal bases relied upon by Customer;
- Any additional Technical and Organisational Measures implemented to protect such data; and

- Any limitations or additional instructions applicable to such Processing.

2.2 No such Processing shall occur until the additional agreement is signed by both Parties.