

Politique d'utilisation acceptable de PageMind (AUP)

Dernière mise à jour : 2026-07-24

1. Objet, portée et relation avec d'autres termes

1.1. Cette politique d'utilisation acceptable de PageMind (« **AUP** ») définit les règles et restrictions qui s'appliquent à tout accès et utilisation du service PageMind et de ses modules et interfaces associés (ensemble, les « **Services** »). PageMind est exploitée par INAI, une société française par actions simplifiée (SASU) dont le siège social est à Lille, France (« **inAi** », « **nous** », « **nous** »).

1.2. Ce AUP fait partie de, et est incorporé par référence dans, l'accord applicable entre inAi et l'entité client concernée (l'« **Accord** »), tel que :

- Conditions de service en ligne acceptées sur le site Web PageMind ; et/ou
- un contrat-cadre de service signé, un bon de commande ou un accord pilote.

1.3. **Relation avec l'accord et d'autres documents.** Ce AUP fait partie de l'accord et est intégré à celui-ci. En cas de conflit direct entre ce AUP et l'accord, l'accord prévaut. Pour les questions relatives au traitement des données à caractère personnel, l'accord de traitement des données applicable et la documentation sur la confidentialité prévaudront sur ce AUP. En cas de conflit entre ce AUP et la documentation, ce AUP prévaut.

1.4. Ce AUP s'applique à :

- le **Client** qui conclut le Contrat avec inAi ;
- tous les employés, sous-traitants et autres personnes du Client à qui le Client accorde l'accès aux Services (« **Utilisateurs autorisés** ») ; et
- tout tiers qui utilise les Services au nom du Client ou sous le compte du Client.

1.5. Le client est responsable de s'assurer que tous les utilisateurs autorisés et tout autre tiers agissant sous son contrôle ou en son nom se conforment au présent AUP. Toute violation de ce AUP par un utilisateur autorisé ou un tiers est considérée comme une violation par le client.

1.6. **Utilisation prévue ; contextes à haut risque.** Les Services sont destinés uniquement aux flux professionnels de catalogues et de documents, principalement pour les détaillants, les marques et les places de marché qui ont besoin de transformer les fichiers fournisseurs en données produits multilingues prêtes à catalogue avec traçabilité. Les Services ne sont pas conçus ou destinés à être utilisés par les consommateurs.

Le Client ne doit pas utiliser les Services en relation avec :

a) les décisions en matière d'emploi ou de ressources humaines concernant les individus (y compris le recrutement, la sélection, la promotion ou le licenciement) ; b) la solvabilité, la solvabilité ou la fiabilité financière des personnes physiques ; c) un diagnostic médical, un traitement, un triage ou toute autre décision en matière de soins de santé concernant les individus ; ou d) d'autres contextes de prise de décision personnelle à haut risque où la loi applicable ou les bonnes pratiques du secteur nécessitent des systèmes dédiés et spécialisés.

Des restrictions supplémentaires sur les utilisations à haut risque du AI sont énoncées à la section 7.6.

1.7. **Mises à jour de ce AUP.** Nous pouvons mettre à jour ce AUP de temps à autre, comme décrit dans la section 13 (Modifications apportées à ce AUP). La version alors en vigueur sera disponible sur le hub juridique de inAi et/ou via l'interface des services. Sous réserve de l'article 13, la poursuite de l'utilisation des services après la date d'entrée en vigueur d'une mise à jour constitue l'acceptation du AUP mis à jour.

2. Définitions

Aux fins de ce AUP :

2.1. « **Accord** » a la signification donnée à la section 1.2.

2.2. « **Utilisateur autorisé** » désigne toute personne physique autorisée par le Client à accéder et à utiliser les Services au nom du Client (y compris les employés, les sous-traitants et les prestataires de services) et qui est autorisée par inAi en vertu du Contrat.

2.3. « **Client** » désigne l'entité juridique qui a conclu l'accord avec inAi pour accéder aux services (y compris tout affilié nommé dans un bon de commande ou un énoncé de travail, le cas échéant).

2.4. « **Données client** » désigne toutes les données, documents, fichiers, images et autres contenus que le client ou ses utilisateurs autorisés soumettent ou téléchargent dans les services (par exemple, les PDF des fournisseurs, les fiches techniques, les feuilles de calcul, les images d'emballage) ainsi que toutes les informations de configuration, modèles ou glossaires fournis par le client. 2.5. « **Données dérivées** » désigne les métriques, statistiques, journaux, rapports d'exécution, modèles anonymisés et autres données générées par inAi dans le cadre du fonctionnement des Services (par exemple, taux de remplissage, nombre de corrections, indicateurs d'anomalies, hachages et empreintes digitales de l'environnement), à l'exclusion dans chaque cas des données client et des résultats eux-mêmes. Dans la mesure où les données dérivées constituent des données à caractère personnel, inAi traitera ces données conformément à l'accord, à l'accord de traitement des données applicable et à la documentation de confidentialité de inAi.

2.6. « **Documentation** » désigne la documentation, les descriptions techniques et les FAQ que inAi met à disposition concernant les Services, y compris via la page produit PageMind, la FAQ et le Centre juridique.

2.7. « **Domage** » désigne tout dommage, perte ou risque de dommage ou de perte, y compris les blessures corporelles, le décès, les dommages matériels, la perte financière, l'atteinte à la réputation, l'exposition réglementaire ou criminelle, la compromission de la sécurité ou la perturbation matérielle des systèmes ou des services.

2.8. « **Sortie** » désigne tout contenu produit par les Services sur la base des données et de la configuration du client, y compris, mais sans s'y limiter, les fichiers CSV/Excel structurés, les listes d'assurance qualité, les listes de nouvelles tentatives, les rapports d'exécution, les packs de preuves de conformité, les titres, les descriptions et les valeurs d'attribut.

2.9. « **Services** » désigne PageMind et tous les modules associés, y compris, mais sans s'y limiter :

- Flux d'ingestion et de transformation du catalogue (des fichiers fournisseurs au CSV aligné sur un modèle) ;
- flux de traduction, d'application du glossaire et de normalisation des attributs ;
- mécanismes d'assurance qualité et de nouvelle tentative ;
- modules axés sur la conformité tels que Verify.UE, dans la mesure où ils sont activés pour le Client dans le cadre du Contrat.

2.10. « **Verify.UE** » désigne le module de PageMind qui, lorsqu'il est disponible et configuré, récupère les informations officielles sur le produit et l'étiquette énergétique des registres pertinents (tels que l'EPREL) et génère des champs axés sur la conformité et des ensembles de preuves selon des règles telles que « aucune preuve, aucune publication ».

2.11. « **Espace de travail** » désigne un environnement logique ou un espace de projet au sein des Services qui est associé à un Client (ou à une unité commerciale du Client) et qui peut contenir des Données Client, des Sorties, des configurations, des journaux et des Données Dérivées pour ce Client.

2.12. « **Loi applicable** » désigne toutes les lois, réglementations, orientations réglementaires et codes de bonnes pratiques qui s'appliquent au Client, à son activité, à son utilisation des Services et aux données et résultats client qu'il traite (y compris, mais sans s'y limiter : les lois sur la protection des données telles que la RGPD, la loi sur la protection des consommateurs et la sécurité des produits, les règles sur les pratiques commerciales déloyales, les obligations en matière d'étiquetage et d'étiquetage énergétique, les régimes de contrôle et de sanctions à l'exportation et les réglementations spécifiques au secteur).

3. Description du service et rôle de PageMind

3.1. PageMind est conçu comme un outil d'**automatisation des opérations de catalogue** qui convertit les fichiers fournisseurs désordonnés (tels que les PDF, les documents Word, les feuilles de calcul et les images) en une feuille de calcul de produit multilingue (CSV/Excel) propre, alignée sur un modèle, avec une traçabilité par ligne, des listes d'assurance qualité et des rapports d'exécution. Il peut également fournir une assistance spécialisée en matière de conformité via des modules tels que Verify.UE.

3.2. PageMind se situe logiquement **avant** les systèmes de gestion des informations sur les produits (PIM), de commerce électronique ou de catalogue du client : il n'agit pas lui-même comme un PIM, une plateforme de magasin ou une base de données d'enregistrement, mais génère plutôt des données prêtes à l'importation que le client peut choisir de charger dans ses propres systèmes. PageMind ne remplace pas les systèmes PIM, MDM, ERP, de commerce électronique, de gestion de contenu ou de réglementation du Client.

3.3. Les services s'appuient sur l'apprentissage automatique, de grands modèles de langage et une infrastructure tierce exploitée à la fois par inAi et par des fournisseurs de cloud et AI sélectionnés. La qualité du résultat est influencée par la qualité et l'exhaustivité des données client, la clarté des modèles et des glossaires, ainsi que la configuration des services. Bien que les Services soient conçus pour minimiser les hallucinations et assurer la traçabilité, aucun système automatisé n'est infaillible et les Résultats peuvent contenir des erreurs, des omissions, des incohérences ou des classifications erronées, et peuvent ne pas être complets, à jour ou adaptés à un usage particulier.

3.4. **Aucun conseil professionnel.** PageMind et ses résultats ne constituent pas des conseils juridiques, réglementaires, de conformité ou autres conseils professionnels. En particulier, Verify.UE est une aide technique pour prendre en charge les flux de travail internes de conformité des produits et la collecte de preuves du Client ; cela ne remplace pas la propre évaluation juridique, réglementaire ou de conformité du Client, ni une garantie que le catalogue ou les pages de produits du Client répondent à une exigence légale ou réglementaire spécifique.

3.5. Le Client reste seul responsable de :

- décider si et comment utiliser une sortie ;
- vérifier que le résultat est exact, approprié et conforme avant de s'y fier ou de le publier ;

- appliquer ses propres processus d'examen humain et de contrôle qualité à un niveau adapté au contexte de risque et de réglementation.

3.6. Le PageMind n'est pas conçu, testé ou destiné à :

- systèmes critiques pour la sécurité (par exemple, dispositifs médicaux, aviation, nucléaire, survie, intervention d'urgence) ;
- prendre ou automatiser des décisions qui créent un risque élevé de préjudice pour les individus ou le public sans examen humain adéquat ;
- Interaction directe avec le consommateur, sauf lorsque le client a superposé sa propre interface utilisateur, ses propres flux de travail et ses propres protections sur les résultats.

3.7. **Modifications apportées aux services.** inAi peut mettre à jour, modifier, améliorer ou interrompre les fonctionnalités des services, des modèles, des invites et des flux de travail de temps à autre, notamment pour refléter les progrès techniques ou les changements dans la loi applicable. inAi n'a pas l'intention de réduire matériellement les fonctionnalités de base des services fournis au client pendant une durée engagée. Si inAi apporte une modification qui réduit sensiblement ces fonctionnalités de base pour le Client pendant une durée engagée, inAi fournira un préavis raisonnable et, le cas échéant, discutera de bonne foi de solutions alternatives ou des conséquences en vertu du Contrat.

4. Éligibilité, comptes et utilisateurs autorisés

4.1. **Usage professionnel uniquement.** Les Services sont destinés uniquement à être utilisés par des entreprises et des organisations. Le Client déclare et garantit qu'il n'est pas un consommateur et qu'il acquiert les Services à des fins professionnelles uniquement.

4.2. **Âge et capacité.** Le Client doit s'assurer que tous les Utilisateurs autorisés ont au moins 18 ans (ou l'âge de la majorité légale dans leur juridiction, si plus élevé) et ont la capacité juridique d'utiliser les Services au nom du Client.

4.3. **Création de compte.** Le client peut être amené à créer un ou plusieurs comptes ou espaces de travail (par exemple via l'interface PageMind ou via un processus d'intégration). Le client doit fournir des informations précises et complètes pour la création de compte et maintenir ces informations à jour.

4.4. **Contrôle d'accès.** Le client est responsable de :

- désignant quelles personnes sont des utilisateurs autorisés ;
- attribuer des rôles et des autorisations appropriés à chaque utilisateur autorisé ; et
- révoquer rapidement l'accès à toute personne qui ne devrait plus utiliser les Services (par exemple, en cas de cessation d'emploi ou de contrat).

4.5. **Identifiants.** Le Client doit s'assurer que tous les identifiants d'accès (noms d'utilisateur, mots de passe, clés API, jetons) utilisés pour accéder aux Services sont :

- gardés confidentiels et non partagés au-delà de l'utilisateur autorisé spécifique auquel ils sont attribués (sauf là où expressément autorisé par inAi, par exemple pour les comptes de service) ; et
- stockés et transmis de manière sécurisée, conformément aux politiques de sécurité du Client.

4.6. **Incidents de sécurité.** Le client doit informer rapidement inAi s'il prend connaissance de :

- accès non autorisé réel ou suspecté aux Services ou à un Espace de travail ;
- perte, vol ou compromission de tout identifiant ou jeton d'accès ; ou
- utilisation abusive des Services sous son compte.

4.7. Accès de tiers. Si le Client accorde l'accès aux Services à un entrepreneur, consultant ou fournisseur de services tiers, le Client :

- reste entièrement responsable du respect par ce tiers du présent AUP et de l'accord ; et
- doit s'assurer que des contrôles contractuels et de sécurité appropriés sont en place avec ce tiers.

4.8. Accès pilote ou bêta. Lorsque le Client accède aux Services à titre d'essai, bêta ou pilote (par exemple, dans le cadre d'un accord bêta privé ou pilote PageMind), les mêmes règles d'éligibilité et de compte s'appliquent. inAi peut imposer des limitations techniques supplémentaires ou des droits de résiliation pour les pilotes et les versions bêta, comme indiqué dans l'accord concerné.

4.9. Responsabilité de l'activité du compte. Sauf dans la mesure expressément indiquée autrement dans le Contrat, le Client est responsable de tout accès et utilisation des Services sous ses comptes et Espaces de travail, y compris par les Utilisateurs autorisés et les tiers agissant en son nom, que cet accès ou cette utilisation soit autorisé ou non par le Client, et qu'il résulte de l'incapacité du Client à protéger les informations d'identification d'accès ou autre.

5. Responsabilités du client et obligations générales

5.1. Conformité à la loi. Le Client doit s'assurer que son utilisation des Services, et l'utilisation des Services par tout Utilisateur Autorisé ou tiers sous son contrôle :

- est conforme à toutes les lois applicables ; et
- ne doit pas utiliser les Services d'une manière dont il sait ou devrait raisonnablement savoir qu'elle entraînerait une violation par inAi ou l'un de ses fournisseurs ou partenaires de la loi applicable.

Cela inclut, sans limitation, le respect de :

- lois sur la protection des données et la confidentialité (telles que RGPD) ;
- loi sur la protection des consommateurs et les pratiques commerciales déloyales ;
- obligations en matière de sécurité des produits, d'étiquetage et d'étiquetage énergétique (y compris les obligations liées à l'EPREL pour les produits étiquetés énergétiquement) ;
- contrôle des exportations et sanctions, y compris des restrictions sur les relations avec les personnes inscrites sur la liste ou les pays sous embargo ; et
- les réglementations sectorielles applicables aux produits ou services du Client ;
- Le client reconnaît que inAi ne surveille pas, et n'a aucune obligation de surveiller, la conformité du client à la loi applicable et que le client reste seul responsable d'évaluer si son utilisation des services et des résultats est légale dans chaque juridiction concernée.

5.2. Contexte d'utilisation approprié. Le client doit utiliser PageMind uniquement dans les contextes où :

- l'extraction, la traduction et la transformation automatisées de la documentation des fournisseurs en données prêtes à être cataloguées sont appropriées et licites ; et

- Le client a mis en œuvre un processus d'examen humain adéquat avant que les résultats ne soient utilisés ou rendus publics, en particulier pour les domaines critiques en matière de conformité ou liés à la sécurité.

5.3. Responsabilité des données client. Le client est seul responsable de :

- la légalité, l'exactitude, l'exhaustivité et l'intégrité de toutes les données client qu'il soumet aux services ;
- s'assurer qu'il dispose de tous les droits, licences et autorisations nécessaires (y compris de la part des fournisseurs, concédants de licence et personnes concernées) pour télécharger les données client dans les services et pour permettre à inAi et à ses sous-traitants de traiter les données client conformément à l'accord et au présent AUP ;
- s'assurer que les Données Client ne portent atteinte à aucun droit de tiers, y compris les droits de propriété intellectuelle, de confidentialité, de publicité ou de confidentialité.

5.4. Responsabilité des résultats. Le client est seul responsable de :

- examiner les résultats générés par les services ;
- décider si et comment utiliser, publier ou s'appuyer sur un résultat ;
- s'assurer que tout contenu de catalogue publié, pages de produits ou autre utilisation en aval des résultats est conforme à la loi applicable et aux propres politiques internes du client ;
- mettre en œuvre des contrôles, des validations et une surveillance supplémentaires adaptés au niveau de risque du cas d'utilisation.

5.5. Aucune confiance en tant que source unique de vérité. Le client ne doit pas traiter les résultats comme une source de vérité définitive ou exclusive, en particulier pour :

- classifications légales ou réglementaires ;
- valeurs critiques de conformité (par exemple, cotes de sécurité, limites, classifications de danger) ;
- domaines où la loi applicable requiert des sources officielles spécifiques, des laboratoires accrédités ou des organismes notifiés.

Lorsqu'il existe des obligations légales ou réglementaires, le Client doit s'assurer de recouper les Résultats avec des sources officielles ou faisant autorité et d'appliquer un jugement professionnel approprié.

Cette section 5.5 est conforme et complète les sections 3 et 10 des conditions de service de PageMind. En cas de doute, le Client doit suivre l'interprétation la plus stricte.

5.6. Minimisation des données et données à caractère personnel. Les Services sont conçus principalement pour le contenu lié aux produits et au catalogue et non pour le traitement de données à caractère personnel sensibles ou à grande échelle. Le client doit : a) éviter de télécharger intentionnellement des documents contenant principalement des données à caractère personnel sur des personnes identifiables (tels que des dossiers RH, des dossiers médicaux, des plaintes de consommateurs, des CV ou des documents d'identité), sauf lorsque cela est expressément autorisé dans l'Accord et l'accord de traitement de données applicable ; et b) ne jamais utiliser les Services pour traiter des catégories particulières de données à caractère personnel ou des données à caractère personnel relatives à des condamnations pénales ou à des infractions, à moins que cela ne soit expressément convenu par écrit dans le Contrat ou dans un accord de traitement de données et que des garanties supplémentaires appropriées soient en place.

Le Client reste responsable de s'assurer qu'il dispose d'une base juridique valide et d'une transparence appropriée pour toute donnée personnelle incluse accidentellement dans les Données Client, conformément à l'article 8.

5.7. Modèles, glossaires et configuration. Le client est responsable de :

- définir ses propres modèles de catalogue, les champs obligatoires et les valeurs acceptables ;
- configurer les listes autorisées (par exemple pour les couleurs et les tailles), les glossaires, les termes interdits et autres contrôles pour refléter ses règles internes et ses obligations réglementaires ;
- maintenir cette configuration à jour au fur et à mesure que ses règles internes ou la loi applicable changent.

5.8. Coopération et commentaires. Le client doit coopérer raisonnablement avec inAi dans les cas suivants :

- enquête sur une utilisation abusive potentielle ou des incidents de sécurité liés au compte du Client ;
- projets pilotes ou bêta dans lesquels PageMind est évalué, y compris en fournissant des commentaires et, si convenu, des mesures de performance non confidentielles.

5.9. Politiques internes. Le Client doit s'assurer que ses propres politiques internes (par exemple, concernant l'utilisation de AI, la protection des données, la sécurité des informations, la conformité et l'approvisionnement) permettent l'utilisation de PageMind de la manière souhaitée par le Client. Il est de la responsabilité du Client d'obtenir toutes les approbations internes nécessaires (par exemple, auprès des fonctions juridiques, de conformité, de confidentialité, de sécurité de l'information ou des comités d'entreprise).

5.10. Indemnité (espace réservé conceptuel). Sous réserve de l'accord, le client sera responsable de toute réclamation, dommage, amende ou autre responsabilité subie par inAi qui découlent de :

- Violation par le client du présent AUP ou de l'accord ;
- Utilisation illégale des Services par le Client ;
- L'incapacité du Client à obtenir les droits ou consentements nécessaires pour les Données Client ou leur utilisation en aval des Résultats.

(Le libellé précis de l'indemnisation, sa portée et ses limites seront définis dans l'accord et devront être examinés avec un conseiller juridique.)

6. Utilisation autorisée des services

6.1. Utilisation professionnelle prévue. Sous réserve du Contrat et du présent AUP, le Client et ses Utilisateurs autorisés peuvent utiliser les Services uniquement à des fins commerciales internes du Client, en particulier pour :

a) ingérer et traiter la documentation des fournisseurs (y compris les PDF, les images, les DOCX, les feuilles de calcul et les fichiers similaires) afin de générer des données produit prêtes à être cataloguées et alignées sur des modèles et des rapports associés ; b) traduire et localiser le contenu du catalogue dans les langues prises en charge selon les glossaires et les règles terminologiques définies par le Client ; c) aider à la normalisation et à la validation des attributs du produit (tels que la couleur, la taille et d'autres spécifications techniques) conformément aux listes et modèles autorisés du Client ; d) générer des listes d'assurance qualité, des listes de nouvelles tentatives, exécuter des rapports et des ensembles de preuves pour prendre en charge les flux de travail internes de qualité et de conformité du catalogue du Client ; e) lorsque cette option est activée, utilisez Verify.UE ou des modules similaires pour faciliter la récupération et la vérification croisée des informations sur les produits et les étiquettes énergétiques à partir des registres pertinents (tels que EPREL), sous réserve des règles spécifiques à Verify.UE de ce AUP.

6.2. Utilisateurs autorisés. Seuls les utilisateurs autorisés peuvent accéder et utiliser les services. Le Client doit s'assurer que chaque Utilisateur Autorisé utilise les Services uniquement :

a) pour le compte du Client et dans le cadre de ses fonctions professionnelles ; et b) conformément au présent AUP, à l'accord et à toute documentation fournie par inAi.

6.3. Limitations de la portée prévue. Les Services sont conçus pour les flux de travail liés aux produits et aux catalogues, et non pour une utilisation par les consommateurs ou pour une prise de décision générale à haut risque concernant les individus. Le Client ne doit pas utiliser les Services à des fins sortant du cadre prévu, y compris toute utilisation interdite en vertu de la Section 7.

6.4. Intégrations tierces. Lorsque les Services fournissent des connecteurs ou des formats d'exportation pour le PIM, le commerce électronique, la place de marché ou d'autres systèmes tiers, le Client peut utiliser ces intégrations uniquement pour déplacer les Sorties dans ses propres environnements et uniquement conformément aux conditions applicables de ces systèmes tiers. inAi n'accorde aucun droit et n'assume aucune responsabilité quant au respect des conditions de tiers.

6.5. Analyses de référence et tests. Le Client peut effectuer des tests et des évaluations raisonnables des Services à ses propres fins internes (y compris les pilotes, les preuves de concept et l'assurance qualité). Le Client ne doit pas publier ou divulguer à un tiers tout test de référence, test de performance ou évaluation des Services (y compris des comparaisons avec d'autres produits ou services) sans le consentement écrit préalable de inAi. Le Client ne doit pas accéder aux Services ni les utiliser d'une manière qui relèverait des interdictions énoncées à l'article 7 (par exemple, utiliser des tests comme moyen d'utiliser abusivement l'infrastructure ou de violer des droits).

6.6. Réserve de droits. Tous les droits relatifs aux Services non expressément accordés au Client en vertu du Contrat sont réservés par inAi et ses concédants de licence. Aucun droit n'est accordé par implication ou par préclusion.

7. Contenus et activités interdits

Le Client et ses utilisateurs autorisés ne doivent pas, directement ou indirectement, utiliser les Services, ou permettre que les Services soient utilisés, d'une manière qui entre dans l'une des catégories énoncées dans la présente Section 7. Une telle utilisation constitue une violation substantielle du présent AUP et de l'Accord.

7.1. Activités illégales, nuisibles ou offensantes

Le Client ne doit pas utiliser les Services pour :

a) violer toute loi applicable ; b) planifier, commettre, promouvoir ou faciliter toute activité frauduleuse, trompeuse, criminelle ou autrement illégale ; c) créer, stocker, distribuer ou promouvoir du contenu incitant à la violence, au terrorisme ou à l'extrémisme violent, ou destiné à menacer, harceler ou intimider des individus ou des groupes ; d) exploiter ou nuire aux mineurs de quelque manière que ce soit, y compris en les exposant à des contenus inappropriés ou en collectant leurs données à caractère personnel en violation des lois sur la protection de l'enfance ; ou e) se livrer à ou promouvoir la traite des êtres humains, l'esclavage ou d'autres violations graves des droits de l'homme.

7.2. Violation de la propriété intellectuelle ou d'informations confidentielles

Le client ne doit pas :

a) télécharger ou traiter des données client qui enfreignent un droit d'auteur, une marque commerciale, un droit de base de données, un secret commercial ou tout autre droit de propriété intellectuelle ou droit de propriété de toute personne ; b) utiliser les Services pour copier, reconstruire ou détourner des ensembles de données,

taxonomies, catalogues ou documents confidentiels de tiers d'une manière qui violerait les restrictions contractuelles ou les obligations de secret commercial ; c) télécharger des documents de fournisseurs ou de partenaires lorsque le Client ne dispose pas et n'a pas obtenu tous les droits et autorisations nécessaires pour que ces documents soient traités via les Services à des fins de catalogue ; ou d) supprimer ou modifier tout avis de propriété (y compris les avis de droit d'auteur et de marque) inclus dans les services ou dans la documentation.

Le client est responsable de s'assurer que ses accords avec les fournisseurs et autres fournisseurs de données permettent l'utilisation de leur contenu dans PageMind comme décrit dans l'accord et dans le présent AUP.

7.3. Données personnelles et confidentialité

Le Client ne doit pas utiliser les Services d'une manière qui viole les lois sur la protection des données, la confidentialité ou la confidentialité, ou qui entre en conflit avec les rôles et responsabilités attribués dans l'Accord, l'accord de traitement des données applicable ou la documentation de confidentialité de inAi. En particulier, le Client doit se conformer aux règles d'utilisation des données à caractère personnel énoncées aux sections 5.6 et 8 et ne doit pas utiliser intentionnellement les Services pour traiter des catégories particulières de données à caractère personnel ou des données à caractère personnel relatives à des condamnations pénales ou à des infractions, à moins que cela ne soit expressément autorisé par ces documents et que des garanties appropriées soient en place.

7.4. Violations de sécurité et abus du réseau

Le client ne doit pas : a) accéder ou tenter d'accéder à toute donnée, compte, système ou ressource lié aux Services auxquels il n'est pas expressément autorisé à accéder ; b) sonder, analyser, tester ou tenter de sonder, analyser ou tester la vulnérabilité de tout système ou réseau inAi sans l'autorisation écrite préalable de inAi (pas de test d'intrusion non autorisé) ; c) interférer ou tenter d'interférer avec le bon fonctionnement des Services, y compris en se livrant à une attaque par déni de service, une surcharge, une inondation, un spam ou un mail-bombing ; d) introduire des logiciels malveillants, des virus, des vers, des chevaux de Troie, des ransomwares ou tout autre code malveillant dans les Services ou dans les Données Client téléchargées sur les Services ; ou e) utiliser les Services pour tenter d'obtenir un accès non autorisé ou de perturber tout système, réseau ou service tiers.

7.5. Utilisation abusive des Services ou de l'infrastructure

Le client ne doit pas :

a) contourner ou tenter de contourner les limites d'utilisation, les quotas, les contrôles de sécurité ou les restrictions techniques mis en œuvre dans les Services (y compris en créant plusieurs comptes ou clés API uniquement pour contourner ces limites) ; b) utiliser les Services comme plate-forme informatique générique, proxy LLM ou outil d'analyse comparative pour des charges de travail non liées, en dehors des flux de travail de catalogue et de documents envisagés par l'Accord et la Documentation ; c) utiliser des niveaux gratuits, des comptes de test, des crédits ou un accès bêta pour exécuter des charges de travail qui ne sont pas raisonnablement liées à l'évaluation ou à l'utilisation des Services à des fins autorisées d'exploitation de catalogue ou d'exploitation de documents ; d) tenter de faire de l'ingénierie inverse, de décompiler, de désassembler ou de dériver le code source, les modèles sous-jacents ou les interfaces non publiques des Services, sauf dans la mesure où une telle restriction est interdite par la loi applicable ; ou e) utiliser les Services, ou toute information non publique sur les Services obtenue en y accédant, pour concevoir, former ou exploiter un service substantiellement similaire ou en concurrence directe avec PageMind d'une manière qui utilise de manière abusive la propriété intellectuelle ou les informations confidentielles de inAi. Pour plus de clarté, rien

dans le présent AUP n'est destiné à empêcher le Client de développer de manière indépendante des produits ou des services qui concurrencent le PageMind, à condition qu'un tel développement n'implique pas une utilisation abusive des Services ou de la propriété intellectuelle ou des informations confidentielles de inAi.

7.6. Utilisations du AI à haut risque ou interdites

Sans le consentement écrit exprès préalable de inAi et un cadre de gestion des risques et de conformité documenté séparément, le Client ne doit pas utiliser les Services en relation avec :

a) prendre, ou soutenir matériellement, des décisions concernant la solvabilité, la notation de crédit ou la fiabilité financière des personnes physiques ; b) le recrutement, la sélection, le classement, la promotion ou le licenciement d'employés, de travailleurs ou de candidats, lorsque les résultats sont utilisés comme facteur décisif ; c) identification biométrique, catégorisation biométrique ou reconnaissance émotionnelle des individus ; d) la notation des risques liés à l'application de la loi, la police prédictive, les décisions en matière de migration ou de contrôle des frontières ; ou e) tout autre cas d'utilisation classé comme « à haut risque » ou interdit par la loi applicable et pour lequel PageMind n'est pas explicitement conçu ou documenté.

Le Client ne doit pas utiliser les Services pour contourner les obligations de sauvegarde, de surveillance ou de conformité qui s'appliquent à d'autres systèmes AI ou outils de prise de décision automatisés exploités par ou pour le Client.

inAi peut, sans responsabilité, refuser, suspendre ou mettre fin à toute utilisation des Services qu'elle considère raisonnablement comme entrant dans les catégories décrites dans la présente Section 7.6 ou comme créant un niveau inacceptable de risque réglementaire, de sécurité ou de réputation pour inAi, ses sous-traitants ou d'autres clients.

7.7. Verify.UE et utilisation abusive liée au registre

Lorsque le client utilise Verify.UE ou tout module similaire : a) Le Client ne doit pas représenter les Services, Verify.UE ou tout résultat comme un service officiel, une approbation, une certification ou une décision de l'Union européenne, d'EPREL ou de tout régulateur ; b) Le Client ne doit pas modifier ou présenter les résultats d'une manière qui suggère faussement qu'une valeur provient d'un registre officiel alors que ce n'est pas le cas, ou qui omet des qualificatifs ou des indicateurs d'une manière qui donnerait l'impression que le résultat fait plus autorité ou est plus définitif qu'il ne l'est ; c) Le Client ne doit pas utiliser Verify.UE d'une manière qui viole les conditions d'utilisation ou les conditions d'accès des registres ou API concernés ; et d) Le Client reste seul responsable de la vérification que ses obligations en matière d'étiquette énergétique et d'information sur les produits sont respectées pour chaque produit dans chaque juridiction où il commercialise ce produit, et ne peut pas se fier aux Services pour remplacer une telle vérification.

7.8. Utilisation abusive des sorties et automatisation

Le client ne doit pas :

a) s'appuyer uniquement sur les résultats, sans examen humain approprié, pour les décisions juridiques, critiques en matière de sécurité ou réglementaires lorsque la loi applicable ou les bonnes pratiques industrielles nécessitent un jugement humain ou une validation supplémentaire ; b) représenter à tout tiers que les Résultats sont garantis corrects, à jour, complets ou légalement suffisants, ou que PageMind assume la responsabilité de la conformité du catalogue du Client ; c) supprimer, masquer ou ignorer les indicateurs, avertissements, champs de traçabilité ou autres indicateurs insérés par les Services d'une manière qui pourrait raisonnablement induire autrui en erreur sur la fiabilité ou la provenance des Résultats ; d) mettre en œuvre des flux de travail de « publication sans révision » entièrement automatisés pour les résultats dans des contextes critiques en matière de conformité, pertinents pour la sécurité ou soumis à des obligations réglementaires spécifiques (y compris

l'étiquetage énergétique), indépendamment de toute évaluation des risques interne ; ou e) utiliser les résultats dans toute tentative délibérée d'induire en erreur les régulateurs, les consommateurs, les partenaires ou les marchés quant aux caractéristiques, aux performances ou à la conformité des produits.

7.9. Sanctions, contrôle des exportations et parties restreintes

Le Client ne doit pas utiliser les Services :

a) en violation de toute loi applicable en matière de sanctions, de contrôle des exportations ou d'embargo, y compris celles de l'Union européenne, des Nations Unies, des États-Unis ou du Royaume-Uni ; b) pour ou au nom de toute personne ou entité inscrite sur toute liste de sanctions applicable ou qui est autrement la cible de sanctions ; ou c) dans toute juridiction où la fourniture ou l'utilisation des Services est interdite par la loi applicable ou nécessiterait que inAi obtienne une licence qu'elle ne détient pas.

Si le Client devient une personne ou une entité sanctionnée, ou est détenu ou contrôlé par une personne ou une entité sanctionnée, le Client doit immédiatement cesser d'utiliser les Services et en informer inAi.

8. Règles de protection des données et d'utilisation de la confidentialité

8.1. Rôles en vertu de la loi sur la protection des données. L'attribution des rôles et des responsabilités pour les données à caractère personnel (par exemple, si le Client est le responsable du traitement et inAi est le sous-traitant, ou inAi est un responsable du traitement indépendant) est régie par l'Accord, l'accord de traitement des données applicable et la documentation de confidentialité de inAi. En cas de conflit entre ce AUP et ces documents concernant les données à caractère personnel, ces documents prévaudront. Cette section 8 définit des obligations d'utilisation supplémentaires pour le client et doit être lue de manière cohérente avec celles-ci.

8.2. Minimisation des données. Le Client doit utiliser les Services conformément au principe de minimisation des données. En particulier :

a) Le Client téléchargera uniquement les Données Client qui sont raisonnablement nécessaires aux flux de travail de catalogue et de documents pour lesquels il utilise PageMind ; b) Le Client évitera de télécharger des fichiers qui concernent principalement des personnes identifiables (tels que des dossiers RH, des plaintes de consommateurs, des rapports médicaux, des CV, des documents d'identité), sauf si cela est clairement nécessaire et autorisé par le Contrat et les documents de confidentialité ; et c) Le Client configurera les modèles, les projets et les espaces de travail de manière à éviter la duplication inutile des données à caractère personnel.

8.3. Base légale et transparence. Pour toute donnée personnelle incluse dans les Données Client, le Client est responsable de : a) établir et documenter une base juridique valide pour le traitement en vertu du droit applicable ; b) informer de manière appropriée les personnes concernées sur le traitement de leurs données à caractère personnel via les Services, y compris toute divulgation pertinente concernant les transferts à inAi et ses sous-traitants ultérieurs ; et c) respecter les droits de la personne concernée (accès, rectification, effacement, restriction, opposition, portabilité) conformément au droit applicable et à l'accord.

8.4. Restrictions sur les catégories spéciales et les données criminelles. Sauf accord exprès écrit et accompagné de garanties supplémentaires appropriées, le Client ne doit pas utiliser les Services pour traiter :

a) catégories particulières de données à caractère personnel ; ou b) les données à caractère personnel relatives aux condamnations pénales ou aux infractions.

Si inAi estime raisonnablement que le Client utilise les Services pour traiter ces données sans garanties appropriées, inAi peut exiger du Client qu'il mette fin à ce traitement, suspende les fonctionnalités concernées ou prenne d'autres mesures en vertu de l'article 11.

8.5. Transferts transfrontaliers. Les transferts internationaux, le cas échéant, sont régis par l'Accord signé et l'accord de traitement des données applicable. Le présent AUP public n'indique aucun lieu de traitement ni arrangement avec un prestataire. Le Client ne doit pas contourner intentionnellement le cadre de transfert convenu ni entrer en conflit avec celui-ci.

8.6. Combinaison avec d'autres ensembles de données. Le Client ne doit pas utiliser les Services pour combiner les Données ou les Résultats du Client avec d'autres ensembles de données d'une manière qui :

a) réidentifier les individus à partir de données anonymisées ou pseudonymisées ; ou b) modifier sensiblement le profil de risque des individus par rapport à la manière dont PageMind est normalement utilisé (par exemple, transformer les données d'utilisation des produits en profils détaillés de consommateurs ou d'employés).

8.7. Incidents et coopération. Si le Client prend connaissance d'un incident de sécurité, d'une violation de données ou de tout autre événement impliquant les Données du Client dans les Services et pouvant nécessiter une notification aux régulateurs ou aux personnes concernées, le Client doit :

a) informer rapidement inAi via les canaux indiqués dans l'accord ou la documentation ; et b) coopérer raisonnablement avec inAi pour enquêter et atténuer l'incident, conformément à l'accord et aux conditions de protection des données applicables.

9. Utilisation équitable, limites de débit et consommation de ressources

9.1. Limites d'utilisation. Les Services peuvent inclure des limites techniques et contractuelles d'utilisation, telles que :

a) nombre maximum de documents ou de produits traités par période ; b) les limites de débit sur les appels API ou les soumissions de travaux ; c) limites par plan ou espace de travail sur les exécutions, environnements ou fonctionnalités simultanés.

Ces limites peuvent être définies dans le Contrat, la Documentation, l'interface utilisateur ou tout bon de commande applicable.

9.2. Respect des limites. Le Client doit se conformer à toutes ces limites d'utilisation et ne doit pas tenter de les contourner, notamment en :

a) créer plusieurs comptes, espaces de travail ou clés API uniquement pour contourner les limites ; b) créer des scripts ou automatiser les appels de manière à ignorer les en-têtes d'attente ou de limite de débit documentés ; ou c) modifier ou interférer avec toute bibliothèque client ou intégration fournie par inAi pour supprimer les mécanismes d'application des limites.

9.3. Utilisation équitable des ressources partagées. Le client doit utiliser l'infrastructure partagée (telle que le calcul, le stockage, les files d'attente) d'une manière équitable et ne dégradant pas de manière déraisonnable l'expérience des autres clients. inAi peut appliquer une limitation, une mise en file d'attente, une planification ou d'autres mesures techniques pour protéger la qualité globale du service.

9.4. Modèles anormaux ou abusifs. Si le inAi détecte raisonnablement des modèles d'utilisation anormaux ou abusifs (par exemple, des pics soudains cohérents avec du scraping, des tests de charge ou des charges de travail hors catalogue) :

a) inAi peut temporairement limiter ou suspendre les tâches, utilisateurs ou espaces de travail concernés ; et b) inAi informera, dans la mesure du possible, le client et travaillera avec lui pour comprendre et résoudre le problème.

9.5. Mise à niveau et planification de la capacité. Lorsque l'utilisation légitime et autorisée du Client dépasse les niveaux envisagés par son plan ou sa commande actuelle :a) inAi peut demander au Client de passer à un plan plus adapté ou de conclure une nouvelle commande reflétant une telle utilisation ; et b) jusqu'à ce qu'une telle mise à niveau soit convenue, inAi peut appliquer des limites provisoires raisonnables pour garantir la stabilité et la prévisibilité des services.

9.6. Interdiction des tests de résistance sans consentement. Le Client ne doit pas utiliser les Services pour des tests de résistance, des tests de charge ou des tests de résilience délibérés de l'infrastructure de inAi, sauf :

a) comme étant raisonnablement accessoire à une utilisation professionnelle normale ; ou b) si cela a été explicitement convenu par écrit au préalable avec inAi (par exemple, dans le cadre d'un test coordonné).

10. Services tiers, sous-traitants et sources de données

1

10.1. Sous-traitants et fournisseurs. Lorsqu'un tiers traite des données à caractère personnel du Client pour les Services, la documentation de traitement applicable et les notifications propres au Client régissent ce traitement. La présente AUP publique ne publie pas les détails de l'infrastructure ou des fournisseurs.

1

0.2. Aucun lien avec des tiers. L'accord et le présent AUP ne créent aucune relation contractuelle entre le client et les sous-traitants ou fournisseurs de inAi. Les droits et recours du Client concernant les Services s'appliquent uniquement à inAi, sous réserve du Contrat.

1

0.3. Conformité aux conditions tierces. Lorsque les Services fournissent des intégrations, des connecteurs ou des exportations vers des services tiers (tels que des PIM, des plateformes de commerce électronique ou des registres), le Client doit :

a) utiliser ces services tiers conformément à leurs conditions générales applicables ; et b) ne pas configurer ou utiliser les Services d'une manière qui amène, ou est raisonnablement susceptible d'amener, le Client ou inAi à violer ces conditions de tiers.

1

0.4. Registres externes et sources officielles. Pour les modules tels que Verify.UE qui se connectent aux registres officiels ou semi-officiels :

a) Le client reconnaît que ces registres sont gérés par des tiers et que inAi ne contrôle pas leur contenu, leur disponibilité ou leur exactitude ; b) Le Client doit respecter toutes les exigences d'accès, d'utilisation ou d'attribution imposées par ces registres ; et c) Le Client ne doit pas utiliser les Services pour récupérer, récolter ou réafficher systématiquement des données de registre d'une manière qui n'est pas envisagée par le Contrat ou qui violerait les conditions du registre.

1

0.5. Propres sous-traitants tiers du Client. Si le Client engage ses propres sous-traitants, consultants ou prestataires de services tiers pour utiliser les Sorties, intégrer PageMind à d'autres systèmes ou exploiter des flux de travail de catalogue :

a) Le client reste entièrement responsable du respect par ces tiers du présent AUP et de l'accord ; et b) Le client doit s'assurer que ses contrats avec ces tiers sont conformes aux restrictions et responsabilités décrites dans le présent AUP.

11. Surveillance, enquête et application

1

1.1. Contrôle de l'utilisation. inAi peut surveiller l'utilisation des Services, notamment via des journaux, des mesures et des outils automatisés, aux fins de :

a) assurer la sécurité, la stabilité et la performance des Services ; b) détecter, prévenir et répondre aux violations réelles ou suspectées du présent AUP ou de l'accord ; et c) générer des statistiques agrégées et des données dérivées pour l'amélioration du service, la planification des capacités et le reporting, comme décrit dans l'accord et la documentation sur la confidentialité.

La surveillance sera effectuée d'une manière proportionnée et conforme à la loi applicable et aux engagements de inAi en matière de confidentialité.

1

1.2. Examen des données client. inAi n'examine pas systématiquement la substance des données client. Cependant, inAi peut accéder et examiner des parties limitées des données client lorsque cela est raisonnablement nécessaire :

a) pour exploiter, maintenir, sécuriser et améliorer les services conformément à l'accord, à l'accord de traitement des données applicable et à la documentation de confidentialité de inAi ; b) pour enquêter sur une violation présumée du présent AUP ou de l'accord ; c) pour répondre à un incident de sécurité ou à un problème technique affectant les Services ; ou d) pour se conformer à une demande légale valide ou à un ordre d'une autorité compétente. Un tel accès sera limité au personnel ayant besoin de connaître et traité conformément aux obligations applicables en matière de confidentialité et de protection des données. Pour plus de clarté, rien dans le présent AUP ne doit être interprété comme imposant à inAi une quelconque obligation générale de surveiller les données du client, les sorties ou l'utilisation des services par le client.

1

1.3. ** Signalement et escalade. ** Si inAi prend connaissance d'une utilisation abusive ou d'une violation présumée du présent AUP, inAi peut :

a) informer le Client et fournir les détails pertinents, dans la mesure permise par la loi ; b) demander des informations supplémentaires au Client ; et c) exiger du Client qu'il prenne des mesures correctives spécifiques (par exemple, supprimer certaines Données Client, désactiver certains utilisateurs ou modifier les configurations).

1

1.4. Mesures d'exécution. Sans limiter les autres droits ou recours en vertu de l'accord ou de la loi, inAi peut, à sa discrétion raisonnable et en fonction de la gravité et de la nature du problème :

a) émettre des avertissements ou des instructions au Client concernant une utilisation non conforme ; b) suspendre ou restreindre temporairement l'accès aux Services pour des utilisateurs spécifiques, des espaces de travail, des fonctionnalités ou l'ensemble du compte ; c) supprimer, désactiver l'accès ou demander la suppression des données ou des sorties client qui semblent enfreindre le présent AUP ou la loi applicable ; d) refuser de traiter ou d'accomplir des travaux ou des tâches spécifiques que inAi estime raisonnablement non conformes ; et/ou e) résilier le Contrat ou les commandes concernées en cas de violations graves, répétées ou délibérées.

1

1.5. Suspension d'urgence. inAi peut immédiatement et sans préavis suspendre ou restreindre l'accès aux Services lorsque :

a) inAi estime raisonnablement qu'une telle action est nécessaire pour protéger la sécurité, l'intégrité ou la disponibilité des Services ou de systèmes tiers ; b) inAi soupçonne raisonnablement que l'utilisation des Services cause, ou est susceptible de causer, un préjudice matériel à toute personne ; ou c) inAi est tenu de le faire par la loi applicable ou par une autorité compétente.

Dans la mesure du possible, inAi informera le client des raisons de cette suspension d'urgence et travaillera de bonne foi avec le client pour rétablir une utilisation conforme.

1

1.6. Demandes policières et réglementaires. inAi peut coopérer avec les organismes chargés de l'application de la loi, les régulateurs et d'autres autorités compétentes dans le cadre d'enquêtes sur des activités illégales présumées impliquant les Services, sous réserve de la loi applicable et, si possible, des efforts raisonnables pour informer le Client, sauf lorsqu'une telle notification est interdite.

12. Signaler un abus, des problèmes de sécurité ou des violations

1

2.1. Canaux de signalement. Le Client et les tiers peuvent signaler des abus présumés, des violations de ce AUP ou des vulnérabilités de sécurité liées aux Services en utilisant les coordonnées spécifiées dans la Documentation ou sur le site Web de inAi (par exemple, adresses e-mail dédiées « abus@ » ou « security@ »).

1

2.2. Informations à inclure. Lorsqu'ils signalent une violation présumée ou un problème de sécurité, les journalistes doivent fournir suffisamment de détails pour permettre à inAi de comprendre et d'évaluer le problème, notamment :

a) une description du comportement ou du contenu en question ; b) les dates, heures et fuseaux horaires pertinents ; c) tout identifiant de compte, espace de travail ou identifiant de poste connu ; et d) le cas échéant, les étapes pour reproduire un problème technique ou une vulnérabilité.

1

2.3. Recherche de sécurité de bonne foi. inAi encourage le signalement responsable et de bonne foi des vulnérabilités de sécurité. Les journalistes doivent :

a) éviter d'accéder à plus de données que ce qui est strictement nécessaire pour démontrer une vulnérabilité ; b) ne pas dégrader intentionnellement les performances ou la disponibilité des Services ; et c) donner à inAi une opportunité raisonnable de résoudre les problèmes avant de les divulguer publiquement.

Tout programme public de prime aux bogues ou de divulgation de vulnérabilités exploité par inAi peut définir des règles ou des canaux supplémentaires pour de tels rapports.

1

2.4. Aucune représailles pour les rapports de bonne foi. inAi ne prendra aucune mesure défavorable à l'encontre du client ou d'un journaliste uniquement pour avoir signalé de bonne foi une vulnérabilité suspectée ou une violation du AUP, à condition que les propres actions du journaliste restent dans les limites de la loi applicable et du présent AUP.

13. Modifications apportées à ce AUP

1

3.1. Droit de mise à jour. inAi peut mettre à jour ce AUP de temps en temps pour refléter :a) les modifications apportées aux Services ou à l'infrastructure de inAi ; b) les changements dans la loi applicable, les directives réglementaires ou les normes de l'industrie ; ou c) la nécessité de s'attaquer aux formes émergentes d'utilisation abusive ou aux nouveaux risques.

1

3.2. Notification. inAi rendra disponible la mise à jour AUP via son hub juridique ou un autre emplacement central et indiquera la date de la dernière mise à jour. Pour les modifications qui élargissent sensiblement les types d'utilisations interdites ou augmentent sensiblement les obligations du Client, inAi fournira un préavis raisonnable au Client (par exemple, par e-mail ou par notifications intégrées au produit). À ces fins, un changement sera considéré comme « élargissant sensiblement » les utilisations interdites ou « augmentant sensiblement » les obligations du Client s'il introduit de nouvelles catégories d'utilisations interdites ou de nouvelles obligations positives pour le Client (par exemple, de nouvelles obligations de configuration, de reporting ou d'audit) au-delà de celles raisonnablement nécessaires pour maintenir la sécurité, se conformer à la loi applicable ou refléter des modifications des Services qui ne réduisent pas les droits existants du Client.

1

3.3. Date d'entrée en vigueur. Sauf indication contraire dans l'avis, les mises à jour de ce AUP prendront effet à la date indiquée comme date de « dernière mise à jour ». L'utilisation continue des Services après cette date constitue l'acceptation par le Client du AUP mis à jour.

1

3.4. Objections. Si le client s'oppose raisonnablement à une mise à jour qui l'affecte de manière importante et négative, le client peut, dans le délai de préavis spécifié, en informer inAi par écrit. Les parties discuteront de bonne foi ; s'ils ne parviennent pas à parvenir à une solution mutuellement acceptable dans un délai raisonnable, le seul et unique recours du Client sera d'exercer tous les droits de résiliation et de sortie applicables énoncés dans le Contrat, et la version de ce AUP en vigueur immédiatement avant la mise à jour concernée continuera de s'appliquer au Client jusqu'à ce que cette résiliation prenne effet.

14. Loi applicable, juridiction et coordonnées

1

4.1. **Loi applicable et juridiction.** Ce AUP est régi par la même loi et la même juridiction spécifiées dans le Contrat (par exemple, la loi française et les tribunaux compétents qui y sont désignés). Tout litige découlant de ou en relation avec ce AUP sera soumis à cette juridiction, sans préjudice des droits obligatoires des régulateurs ou autres autorités.

1

4.2. **Coordonnées.** Les questions ou préoccupations concernant ce AUP peuvent être adressées à inAi en utilisant les coordonnées fournies dans l'accord ou sur le site Web de inAi, notamment :

- les coordonnées du siège social et de la raison sociale telles que précisées dans les mentions légales ; et
- Canaux de contact désignés pour les questions juridiques, de confidentialité, de sécurité et d'assistance.

1

4.3. **Hiérarchie.** En cas d'incohérence entre ce AUP et tout autre document qui y est référencé, les dispositions hiérarchiques de l'Accord s'appliquent.