Sapiologie

DOCUMENT OFFICIEL

Accord de traitement des données personnelles (DPA)

Visé par le Devis contractuel · Article 28 du Règlement (UE) 2016/679 (RGPD)

Éditeur / Sous-traitant	SAPIOLOGIE, SAS au capital de 64 302,08 €, immatriculée au RCS de Lille Métropole sous le numéro 901 482 356, dont le siège social est situé 229 rue Solférino, 59000 Lille, France (ci-après « Sapiologie »)
Client / Responsable de traitement	La personne morale désignée au Devis contractuel dont le Devis contractuel vise les présentes (ci-après « le Client »)
Version	1.6
Date d'adoption	17/11/2026
Champ d'application	Le présent accord est visé par le Devis contractuel signé par les représentants habilités des deux Parties et en fait partie intégrante. Il est conclu par la signature du Devis contractuel, sans signature séparée requise. Il s'applique à tout traitement de données à caractère personnel réalisé par Sapiologie pour le compte du Client, et prévaut sur tout autre document contractuel pour ces seuls traitements.
Contact protection des données	Référent protection des données : Selim Youssry. Demandes relatives aux données personnelles : contact@sapiologie.com
Version	La version applicable est celle visée par le Devis contractuel signé. Elle demeure opposable pour la durée initiale et pour chaque période reconduite. Toute modification requiert un avenant écrit signé par les représentants habilités des deux Parties, conformément aux Conditions Générales de Vente.

Préambule

Sapiologie édite et héberge une plateforme SaaS d'analyse de cycle de vie et d'éco-conception (ci-après « la Plateforme »). Pour fournir la Plateforme, Sapiologie traite des données à caractère personnel pour le compte du Client. Au sens du RGPD, le Client agit en qualité de **responsable de traitement** et Sapiologie en qualité de **sous-traitant**, sous réserve de l'article 4 bis.

Le présent accord définit les conditions dans lesquelles Sapiologie s'engage à effectuer, pour le compte du Client, les opérations de traitement définies en Annexe 1, conformément à l'article 28 du RGPD. Il fait partie intégrante du Contrat conclu entre Sapiologie et le Client, que le Devis contractuel vise à l'article 3.1 des Conditions Générales de Vente. En cas de contradiction entre le présent accord et toute autre disposition contractuelle relative à la protection des données à caractère personnel, le présent accord prévaut.

Article 1 : Définitions

Les termes « données à caractère personnel », « traitement », « responsable du traitement », « sous-traitant », « personne concernée » et « violation de données à caractère personnel » ont le sens que leur donne l'article 4 du RGPD. Les « Données Client » désignent les données à caractère personnel traitées par Sapiologie pour le compte du Client dans le cadre des services.

Article 2 : Objet et durée

Le présent accord encadre le traitement des Données Client par Sapiologie pour la durée du contrat principal. Il demeure applicable jusqu'à la suppression effective des Données Client dans les conditions de l'article 10. La nature, la finalité, les catégories de données et de personnes concernées sont décrites en **Annexe 1**.

Pour ses propres finalités (gestion de la relation contractuelle et commerciale, facturation, support par messagerie, conformité à ses obligations légales), Sapiologie agit en qualité de responsable de traitement.

Article 3 : Obligations de Sapiologie

Sapiologie s'engage à :

- **Instructions documentées.** Ne traiter les Données Client que sur instruction documentée du Client, y compris en ce qui concerne les transferts vers un pays tiers. Le Devis contractuel, les Conditions Générales de Vente, le présent accord et le paramétrage de la Plateforme par le Client constituent les instructions initiales du Client ; toute instruction complémentaire est formulée par écrit. Si Sapiologie estime qu'une instruction constitue une violation du RGPD ou d'une autre disposition applicable en matière de protection des données, elle en informe immédiatement le Client. Si le droit de l'Union européenne ou le droit français impose un traitement à Sapiologie, elle en informe le Client avant le traitement, sauf interdiction légale.
- **Finalité exclusive.** Ne traiter les Données Client que pour la fourniture des services au Client, jamais pour son propre compte. Sapiologie peut produire des statistiques d'usage sous forme agrégée et anonymisée au sens du RGPD, ne permettant aucune réidentification directe ou indirecte.
- **Confidentialité du personnel.** Veiller à ce que les personnes autorisées à traiter les Données Client s'engagent à respecter la confidentialité (accord de confidentialité signé à l'embauche et acceptation de la politique de sécurité interne) et reçoivent une sensibilisation à la sécurité de l'information au moins une fois par an.
- **Sécurité.** Mettre en œuvre les mesures techniques et organisationnelles décrites en **Annexe 2**, conformément à l'article 32 du RGPD, et les maintenir à un niveau au moins équivalent pendant toute la durée du contrat.
- **Registre.** Tenir le registre des catégories d'activités de traitement effectuées pour le compte du Client, conformément à l'article 30.2 du RGPD.
- **Coopération.** Coopérer avec l'autorité de contrôle compétente (en France, la CNIL) à la demande de celle-ci, et mettre à la disposition du Client les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD.
- **Personnel habilité.** Restreindre l'accès aux Données Client aux seuls membres de son personnel qui en ont besoin pour l'exécution des services, selon le principe du moindre privilège.

Article 4 : Obligations du Client

Le Client, en sa qualité de responsable de traitement, s'engage à : documenter par écrit toute instruction complémentaire concernant le traitement des Données Client ; veiller à disposer d'une base légale pour les traitements qu'il opère via la Plateforme et à informer les personnes concernées ; ne pas soumettre à la Plateforme de données relevant des catégories particulières de l'article 9 du RGPD ni de données relatives aux condamnations pénales et infractions visées à l'article 10 du RGPD ; superviser les traitements, en ce compris l'usage des comptes utilisateurs qu'il administre.

Article 4 bis : Configuration cabinet et chaîne de sous-traitance

Lorsque le Client utilise la Plateforme pour réaliser des analyses au bénéfice de ses propres clients au sens de l'article 13 des Conditions Générales de Vente et qu'il agit à ce titre en qualité de sous-traitant d'un de ses clients responsable de traitement, le présent accord s'applique entre les Parties comme un **accord de sous-traitance ultérieure au sens de l'article 28.4 du RGPD** : Sapiologie intervient en qualité de sous-traitant ultérieur du Client et ses obligations sont dues au seul Client.

Dans cette configuration, le Client déclare et garantit : (i) disposer de l'autorisation écrite, générale ou spécifique, de chaque responsable de traitement concerné pour recourir à Sapiologie en qualité de sous-traitant ultérieur, ainsi que du droit de conclure le présent accord ; (ii) que les instructions qu'il adresse à Sapiologie sont conformes à celles reçues du responsable de traitement et n'excèdent pas les finalités autorisées par celui-ci ; (iii) qu'il assume envers le responsable de traitement l'information des personnes concernées, l'instruction de l'exercice de leurs droits et les notifications prévues aux articles 33 et 34 du RGPD ; (iv) **que les obligations souscrites par Sapiologie au titre du présent accord satisfont celles qu'il a lui-même souscrites envers chaque responsable de traitement concerné**.

Le Client informe Sapiologie par écrit, préalablement au dépôt des Données correspondantes, de toute exigence d'un responsable de traitement excédant les obligations du présent accord, notamment un délai de notification abrégé, une fréquence d'audit supérieure ou une contrainte de localisation. Une telle mesure requiert un avenant

écrit signé des deux Parties ; à défaut d'information préalable, ces exigences ne sont pas opposables à Sapiologie.

Sapiologie ne reçoit d'instructions que du Client, seul point de contact : toute demande émanant d'un responsable de traitement ou d'un client final du Client est transmise sans délai indu au Client, qui y répond, sauf obligation légale ou instruction écrite de celui-ci ; les demandes émanant d'une personne concernée suivent l'article 7. Le Client garantit Sapiologie contre toute réclamation d'un responsable de traitement ou d'une personne concernée résultant d'un manquement aux garanties du présent article, dans les termes de l'article 13.2 des Conditions Générales de Vente.

Audits du responsable de traitement final. Les demandes d'audit ou d'inspection émanant d'un responsable de traitement du Client, ou fondées sur le droit d'audit dont celui-ci dispose sur l'ensemble de la chaîne de sous-traitance, s'exercent par l'intermédiaire du Client, dans les conditions et sur le même quota d'audit prévus à l'article 11, quel que soit le nombre de responsables de traitement concernés.

Fin de la relation entre le Client et l'un de ses clients. Lorsque le Client cesse d'intervenir pour l'un de ses clients tout en conservant son abonnement, le sort des Données correspondantes est réglé conformément à l'**article 13.3 des Conditions Générales de Vente** : l'export est adressé à l'entité désignée à ce titre au Devis contractuel et la suppression n'est exécutée que sur instruction de la personne qui y est habilitée.

Article 5 : Sous-traitance ultérieure

Le Client autorise de manière générale Sapiologie à recourir à des sous-traitants ultérieurs pour l'exécution des services. Sapiologie recourt à un seul sous-traitant ultérieur : **OVHcloud (OVH SAS)**, société de droit français, qui héberge la Plateforme, les fichiers et les sauvegardes en France.

Sapiologie informe le Client par écrit de tout projet d'ajout ou de remplacement d'un sous-traitant ultérieur au moins **30 jours** avant sa prise d'effet. Le Client dispose de ce délai pour formuler des objections motivées et légitimes. En cas d'objection à laquelle il ne peut être remédié raisonnablement, chaque partie peut résilier le service concerné, sans indemnité de part ni d'autre pour ce seul motif ; Sapiologie rembourse alors au Client, au prorata temporis, les sommes prépayées correspondant à la période postérieure à la date d'effet de la résiliation.

Sapiologie impose contractuellement à chaque sous-traitant ultérieur des obligations en matière de protection des données au moins équivalentes à celles du présent accord, et demeure pleinement responsable envers le Client de l'exécution de leurs obligations.

Lorsque le Client déclare ses propres clés d'interface de programmation pour alimenter l'agent conversationnel intégré (article 17 des Conditions Générales de Vente) ou connecte son agent externe par le connecteur MCP (même article), la relation avec le fournisseur de modèles relève du seul Client, dans les conditions de ces articles.

Les prestataires auxquels Sapiologie recourt pour ses propres traitements en qualité de responsable de traitement, notamment sa messagerie, son outil de gestion de la relation client, son outil de facturation et sa plateforme agréée de transmission des factures électroniques, sont décrits dans la politique de confidentialité de Sapiologie.

Ecoinvent Association agit en responsable de traitement autonome, dans les conditions de l'article 6 bis.

Article 6 : Localisation des données et transferts

La Plateforme et les Données Client, sauvegardes comprises, sont hébergées **exclusivement en France**, chez OVHcloud, sur des **serveurs dédiés et un service de stockage d'objets situés exclusivement sur le territoire français** ; elles sont chiffrées au repos, sauvegardes comprises, et les Données de chaque client sont cloisonnées logiquement. Les Données Client sont traitées **exclusivement dans l'Union européenne et l'Espace économique européen**. Tout transfert qui deviendrait nécessaire, y compris du fait d'un sous-traitant ultérieur déjà autorisé, serait notifié par écrit au Client au moins 30 jours à l'avance, soumis au droit d'objection de l'article 5, et subordonné à la mise en place préalable des garanties appropriées prévues au chapitre V du RGPD.

Article 6 bis : Destinataire tiers agissant pour son propre compte

La base de données ecoinvent est éditée par **ecoinvent Association**, de droit suisse, et soumise à une licence nominative propre. Lorsqu'un Utilisateur souscrit, par l'intermédiaire de Sapiologie, une licence d'accès à cette base, Sapiologie communique à ecoinvent Association les données nécessaires à l'émission et au suivi de cette

licence : **nom et prénom de l'Utilisateur, adresse de messagerie professionnelle, pays, identification de l'entreprise, dates de début et de fin de la licence, type de licence et volume de jeux de données consultés**. Ces informations sont transmises **à la fin de chaque trimestre**.

Ecoinvent Association détermine seule les finalités et les moyens du traitement qu'elle opère sur ces données, au titre de la gestion de ses licences et du respect de ses propres obligations. Elle agit à cet égard en qualité de **responsable de traitement autonome**, et non de sous-traitant ultérieur de Sapiologie : l'article 5 du présent accord ne lui est pas applicable. Sapiologie agit en qualité de **destinataire transmettant** et n'opère aucun autre traitement de ces données pour le compte d'ecoinvent Association.

Cette communication est **nécessaire à l'exécution** de la commande de licence passée par le Client : sans elle, la licence nominative ne peut être émise au nom de l'Utilisateur désigné. Elle n'a lieu que pour les Utilisateurs pour lesquels une licence est souscrite par l'intermédiaire de Sapiologie. La Suisse fait l'objet d'une décision d'adéquation de la Commission européenne ; aucune garantie complémentaire de transfert n'est requise à ce titre.

Le Client informe les Utilisateurs concernés de cette communication et de son destinataire, au titre des articles 13 et 14 du RGPD. Sapiologie lui fournit sur demande les éléments nécessaires à cette information.

Article 7 : Assistance au Client

Compte tenu de la nature du traitement, Sapiologie assiste le Client par des mesures techniques et organisationnelles appropriées :

- pour donner suite, dans la mesure du possible, aux demandes d'exercice des **droits des personnes concernées** (accès, rectification, effacement, limitation, portabilité, opposition). Si une telle demande est adressée directement à Sapiologie, celle-ci la transmet au Client sans délai indu ; la réponse relève du Client, sauf instruction contraire de celui-ci ou obligation légale ;
- pour garantir le respect des obligations prévues aux **articles 32 à 36 du RGPD** (sécurité du traitement, notification des violations, analyses d'impact relatives à la protection des données et consultations préalables de l'autorité de contrôle), compte tenu des informations à la disposition de Sapiologie.

Article 8 : Violations de données à caractère personnel

Sapiologie notifie au Client toute violation de données à caractère personnel affectant les Données Client **sans délai indu et au plus tard 24 heures** après avoir qualifié l'événement comme une violation de données à caractère personnel, à l'adresse de contact désignée par le Client ou, à défaut de désignation, aux administrateurs du compte Client. La notification comprend, dans la mesure des informations disponibles : la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, le point de contact chez Sapiologie, les conséquences probables de la violation et les mesures prises ou proposées pour y remédier ou en atténuer les effets. Les informations peuvent être fournies de manière échelonnée si elles ne sont pas toutes disponibles simultanément.

Sapiologie documente la violation et les mesures prises. Le Client, en sa qualité de responsable de traitement, procède le cas échéant aux notifications prévues aux articles 33 et 34 du RGPD ; toute notification effectuée par Sapiologie au nom du Client suppose l'accord préalable de celui-ci, sauf obligation légale incombant en propre à Sapiologie.

Article 9 : Demandes d'autorités publiques

Si une autorité publique ou un tiers demande à Sapiologie l'accès à des Données Client, Sapiologie en informe le Client sans délai avant toute divulgation, sauf interdiction légale. Sapiologie vérifie la légalité de la demande, conteste par les voies de droit disponibles toute demande qu'elle estime illégale ou excessive, et ne divulgue que les données strictement nécessaires pour y répondre. Elle documente chaque demande et les suites qui y sont données.

Article 10 : Sort des données en fin de contrat

Au terme du contrat, quelle qu'en soit la cause, le Client bénéficie de la **fenêtre de réversibilité** prévue à l'article 27 des Conditions Générales de Vente, pendant laquelle les Données Client sont conservées aux seules fins de leur restitution et d'un accès en lecture et en export.

Au choix du Client, Sapiologie lui **restitue** l'intégralité des Données Client dans des formats standards exploitables puis les **supprime**, ou les **supprime** sans restitution préalable ; la suppression porte sur toutes les copies existantes, sauvegardes comprises. Le Client exprime ce choix par écrit dans les 30 jours suivant la fin du contrat ; à défaut, Sapiologie les supprime à l'expiration de la fenêtre de réversibilité, après en avoir notifié la date par écrit au moins 15 jours à l'avance. Les délais de suppression, la purge des sauvegardes et l'attestation de suppression sont régis par les **articles 27 et 28 des Conditions Générales de Vente**, qui s'appliquent à l'ensemble des Données Client.

Par exception, Sapiologie conserve après la suppression : les données qu'elle est légalement tenue de garder, notamment les pièces comptables, pour la durée légale ; le Contrat signé et la preuve de sa signature, pendant cinq ans à compter de sa fin ; les journaux de connexion, pendant la durée prévue à l'article 14.2 des Conditions Générales de Vente. Ces données ne sont traitées qu'aux fins correspondantes.

Article 11 : Audits et démonstration de conformité

Sapiologie met à la disposition du Client les informations nécessaires pour démontrer le respect du présent accord, notamment : le certificat **ISO 27001:2022** en vigueur, délivré par un organisme tiers indépendant, les attestations d'audits et de tests de sécurité disponibles, et des extraits pertinents de sa politique de sécurité sous accord de confidentialité.

Si ces éléments ne suffisent pas raisonnablement à démontrer la conformité, ce caractère suffisant s'appréciant de bonne foi, le Client peut faire réaliser un audit, **y compris une inspection sur site**, dans les conditions de fréquence, de préavis, de désignation de l'auditeur, de déroulement, de périmètre et de frais prévues aux **articles 22.2 et 22.3 des Conditions Générales de Vente**. Les constats de l'audit sont confidentiels et communiqués à Sapiologie. En cas de désaccord persistant sur le caractère suffisant des éléments documentaires après échange écrit, le Client conserve le droit de faire réaliser l'audit dans les conditions du présent article.

Par exception, les limitations de fréquence et de préavis des articles 22.2 et 22.3 des Conditions Générales de Vente ne s'appliquent pas lorsque l'audit fait suite à une violation de données à caractère personnel affectant les Données Client ou à la demande d'une autorité de contrôle compétente ; le préavis est alors réduit à 5 jours ouvrés.

Article 12 : Responsabilité

La responsabilité de chaque partie au titre du présent accord est régie par l'article 82 du RGPD et par le contrat principal.

Article 13 : Droit applicable

Le présent accord est régi par le droit français. Tout litige relatif à sa validité, son interprétation ou son exécution relève de la juridiction désignée par les Conditions Générales de Vente.

Annexe 1 : Description du traitement

Élément	Description
Nature et finalité du traitement	Fourniture de la Plateforme Sapiologie (analyse de cycle de vie et éco-conception) : création et gestion des comptes utilisateurs, authentification des utilisateurs (mot de passe ou fédération d'identité OpenID Connect), fourniture des fonctionnalités collaboratives, journalisation technique et de sécurité.
Catégories de personnes concernées	Utilisateurs de la Plateforme désignés par le Client, qu'ils appartiennent ou non à son personnel : salariés du Client, prestataires intervenant pour son compte, et Utilisateurs invités auxquels le Client ouvre un droit de consultation ou de collecte de données, notamment les collaborateurs de ses fournisseurs et, en configuration cabinet, les collaborateurs de ses propres clients ; contacts du Client dans le cadre contractuel et de facturation ; le cas échéant, contacts professionnels de tiers que le Client renseigne dans la Plateforme.

Catégories de données	Données d'identification et coordonnées professionnelles (nom, prénom, adresse email professionnelle, fonction, téléphone professionnel le cas échéant) ; données de connexion et d'usage (identifiants, journaux de connexion et d'activité).
Durée du traitement	Durée du contrat principal, augmentée des délais de restitution et de suppression prévus à l'article 10. Les journaux de connexion et d'activité sont conservés douze mois à compter de l'enregistrement de chaque trace, conformément à l'article 14.2 des Conditions Générales de Vente.

Annexe 2 : Mesures techniques et organisationnelles (article 32 RGPD)

Gouvernance de la sécurité

- Système de management de la sécurité de l'information **certifié ISO 27001:2022**, audité par un organisme tiers indépendant ; politique de sécurité interne documentée et révisée au moins une fois par an.
- Responsable de la sécurité de l'information désigné (directeur technique).

Contrôle d'accès

- Comptes individuels nominatifs ; gestion des habilitations par rôles selon le principe du moindre privilège ; revue des accès au moins une fois par an, et tous les six mois pour les systèmes de production.
- Processus documenté d'attribution et de révocation des accès à l'arrivée, au changement de fonction et au départ des collaborateurs.
- Authentification multifacteur obligatoire pour les comptes d'administration, notamment ceux de l'infrastructure d'hébergement.
- Administration des serveurs au moyen de clés personnelles protégées par une phrase secrète, au travers d'un réseau privé virtuel chiffré ; un accès de secours durci et chiffré est maintenu en cas d'indisponibilité de ce réseau ; les autres interfaces d'administration ne sont pas exposées sur Internet.
- Authentification multifacteur disponible pour tous les utilisateurs de la Plateforme.
- Accès aux sauvegardes restreint à l'équipe d'administration des systèmes.

Chiffrement

- Chiffrement des échanges entre les utilisateurs et la Plateforme (TLS 1.2 minimum, TLS 1.3 supporté) et entre serveurs situés sur des hôtes distincts.
- Chiffrement des données au repos : partition de données des serveurs, espaces de stockage et sauvegardes.
- Flux d'administration chiffrés (réseau privé virtuel ou accès de secours durci).
- Postes de travail du personnel : disque chiffré, verrouillage automatique de session, antivirus.

Cloisonnement

- Cloisonnement logique des données entre clients : chaque client n'accède qu'à son propre contenu.
- Séparation des environnements de test et de production ; les données de production ne sont jamais utilisées à des fins de développement ou de test. Par exception, avec l'accord du Client, un fichier qu'il a transmis peut être copié, pour la seule durée nécessaire à la résolution d'une anomalie, sur le poste de travail chiffré d'un membre habilité du personnel ; cette copie est limitée à ce que l'anomalie exige, n'est jamais déposée dans un dépôt de code ni dans un espace partagé, et est supprimée une fois l'anomalie corrigée. Un fichier conservé comme cas de test permanent est préalablement anonymisé.

Journalisation et supervision

- Journalisation des connexions et déconnexions, des actions privilégiées et des événements de sécurité (échecs de connexion, tentatives d'élévation de privilèges), avec rattachement de chaque identifiant technique à une personne physique.
- Journal d'audit applicatif natif : traçabilité horodatée des modifications, consultable par les administrateurs du Client.
- Supervision continue de la Plateforme, alertes automatiques (détection de code malveillant, indisponibilité de service) et procédure d'escalade documentée.

Protection contre les logiciels malveillants et gestion des vulnérabilités

- Protection anti-malware déployée, avec procédures documentées de détection et de réponse ; les fichiers déposés dans la Plateforme sont analysés par un antivirus avant traitement.
- Gestion des vulnérabilités : analyse statique du code à chaque modification, bloquante en cas d'échec ; analyse hebdomadaire des dépendances logicielles et des composants tiers ; mises à jour de sécurité automatiques des systèmes d'exploitation des serveurs ; veille sur les vulnérabilités publiées ; correction selon la gravité et l'exposition ; correctifs appliqués en préproduction puis en production, selon un processus de gestion des changements documenté.
- Test d'intrusion externe réalisé chaque année par un prestataire indépendant.

Sauvegardes et continuité d'activité

- Sauvegarde quotidienne automatique de la base de données de production, chiffrée, stockée dans deux régions géographiquement distinctes en France, rétention de 30 jours, avec contrôle quotidien d'exécution. Les fichiers déposés par le Client sont conservés sur un stockage d'objets chiffré dont la durabilité est assurée par le fournisseur d'hébergement ; ils ne font pas l'objet d'une sauvegarde distincte.
- Plan de reprise d'activité formalisé : objectif de reprise (RTO) de 2 heures et de perte de données maximale (RPO) de 24 heures, testé au moins une fois par an, chaque test étant documenté.

Gestion des incidents et sécurité physique

- Procédure documentée de détection, classification et traitement des incidents de sécurité ; notification des violations conformément à l'article 8 du présent accord.
- Hébergement dans des centres de données opérés par OVHcloud, dont les attestations de conformité sont communiquées sur demande dans les conditions de l'article 22.1 des Conditions Générales de Vente.

Personnel

- Engagement de confidentialité signé par l'ensemble des collaborateurs à l'embauche, qui subsiste après leur départ ; acceptation de la politique de sécurité et de la charte d'usage.
- Sensibilisation à la sécurité de l'information au moins annuelle.