

**ACCORD DE SOUS-TRAITANCE RELATIF AU TRAITEMENT DE DONNÉES PERSONNELLES
DANS LE CADRE DE LA GESTION DE LICENCES IA**

DATA PROCESSING AGREEMENT

ENTRE :

MISTER IA Entreprise, société par actions simplifiée (SAS), immatriculée au RCS de Paris sous le numéro 938 949 054, dont le siège social est situé 128 Rue La Boétie, 75008 Paris, prise en la personne de son représentant légal domicilié en cette qualité audit siège.

ci-après « **MISTER IA** »

ET

Le Client,

désignés ensemble les « **Parties** ».

PREAMBULE

MISTER IA propose une prestation de gestion de licences d'outils d'intelligence artificielle (IA) pouvant inclure notamment, selon le périmètre convenu avec le Client : l'achat de licences, leur paramétrage sécurisé, une veille technologique, la gestion centralisée des mouvements, l'analytics (analyse de l'utilisation des Solutions IA), ou encore des prestations de support utilisateur (ci-après les « Services »).

Les Solutions IA concernées peuvent inclure tout outil d'IA sélectionné par le Client et pris en charge par MISTER IA.

Le présent Accord encadre les Traitements de Données Personnelles réalisés par MISTER IA pour le compte du Client dans le cadre de ces Services, conformément à l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD »).

ARTICLE 1 – DÉFINITIONS

Aux fins du présent Accord, les termes ci-dessous contenant une majuscule ont la signification suivante :

« **Accord** » : désigne le présent accord de sous-traitance (Data Processing Agreement), incluant ses annexes.

« **Client** » : désigne la personne physique ou morale professionnelle ayant souscrit aux Services et partie au présent Accord.

« **Contenus IA** » : désigne des contenus saisis, importés, transmis, traités ou générés au moyen d'une Solution IA notamment, à titre d'exemple, les prompts, conversations, fichiers téléversés, documents analysés, résultats générés, ainsi que les contenus des projets. Les Contenus IA ne constituent des Données Personnelles que dans la mesure où ils contiennent des informations se rapportant à une personne physique identifiée ou identifiable.

« **Contrat Commercial** » : désigne les conditions générales, conditions particulières, devis, bon de commande, proposition commerciale, ou tout autre document contractuel conclus entre les Parties et définissant les Services fournis par MISTER IA au Client.

« **Donnée(s) Personnelle(s)** » : désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « Personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

« **Donnée(s) Sensible(s)** » : désigne des Données Personnelles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique (au sens de l'article 9 du RGPD), ou des données relatives aux condamnations pénales et aux infractions (au sens de l'article 10 du RGPD).

« **Donnée(s) de Compte, de Licence et d'Habilitation** » : désigne des Données Personnelles relatives au compte utilisateur, à la licence qui lui est attribuée et à ses droits d'accès à une Solution IA, notamment, à titre d'exemple, l'identifiant du compte, la Solution IA et la formule attribuées, le rôle, le niveau d'autorisation, l'espace de rattachement, le statut du compte ou de la licence, ainsi que les dates d'activation, de modification, de suspension ou de suppression.

« **Donnée(s) d'Usage** » : désigne des Données Personnelles relatives à l'utilisation des licences et des Solutions IA par les utilisateurs du Client, lorsqu'elles sont rattachées ou raisonnablement rattachables à un utilisateur notamment, à titre d'exemple, le statut d'activation de la licence, le nombre de messages, de conversations, de projets, d'assistants, de requêtes ou de tokens, les modèles utilisés, les volumes et taux d'utilisation, les coûts associés ainsi que les indicateurs relatifs au niveau d'adoption ou d'utilisation. Les Données d'Usage n'incluent pas le contenu des prompts, conversations, fichiers ou résultats générés, qui relève des Contenus IA.

« **Donnée(s) de Connexion et de Traçabilité** » : désigne, lorsqu'elles sont accessibles à MISTER IA, des Données Personnelles relatives à l'authentification, aux connexions et aux opérations réalisées sur les comptes ou espaces concernés, notamment, à titre d'exemple, la méthode d'authentification utilisée, les adresses IP, les dates et heures de connexion, les informations relatives au terminal ou au navigateur, les tentatives de connexion, les journaux d'activité et les opérations d'administration.

« **Donnée(s) de Support** » : désigne des Données Personnelles traitées dans le cadre du support utilisateur, notamment, à titre d'exemple, les demandes, tickets, échanges, incidents, informations techniques, catégories de demandes et informations nécessaires à leur résolution.

L'emploi des termes désignant, le cas échéant, certaines catégories de Données Personnelles (tels que « Donnée(s) Sensible(s) », « Donnée(s) de Compte, de Licence et d'Habilitation », « Donnée(s) d'Usage », « Donnée(s) de Connexion et de Traçabilité », « Donnée(s) de Support ») n'emporte pas nécessairement le Traitement de l'intégralité des Données Personnelles citées seulement à titre d'exemple au sein de leur définition.

« **Fournisseur de Solution IA** » : toute personne fournissant, éditant, exploitant, mettant à disposition ou commercialisant une Solution IA utilisée dans le cadre des Services.

« **Responsable(s) du Traitement** » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement; lorsque les finalités et les moyens de ce Traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le Responsable du Traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

« **Service(s)** » : les prestations de gestion de licences IA fournies par MISTER IA au Client, telles que décrites dans le Contrat Commercial et dans le présent Accord.

« **Solution(s) IA** » : les outils, logiciels, services, plateformes ou applications d'intelligence artificielle, notamment d'IA générative, dont les licences sont gérées par MISTER IA pour le compte du Client.

« **Sous-traitant(s)** » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données Personnelles pour le compte du Responsable du Traitement.

« **Sous-traitant(s) ultérieur(s)** » : Autre Sous-traitant recruté par un Sous-traitant pour mener des activités de Traitement spécifiques pour le compte du Responsable du Traitement.

« **Traitement(s)** » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de Données Personnelles, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

« **Violation(s) de Données Personnelles** » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

ARTICLE 2 – OBJET, CHAMP D'APPLICATION ET HIÉRARCHIE

Le présent Accord a pour objet de définir les conditions dans lesquelles MISTER IA traite des Données Personnelles pour le compte du Client dans le cadre des Services.

Il s'applique aux Traitements de Données Personnelles tels que décrits à l'Annexe 1.

Le présent Accord ne s'applique pas notamment :

1. Aux Traitements réalisés par le Client sous sa propre responsabilité sans intervention de MISTER IA en qualité de Sous-traitant.
2. Aux Traitements réalisés par le Client ou un Fournisseur de Solution IA lorsque le Client contracte directement avec le Fournisseur de Solution IA, pour tout ou partie des fonctionnalités offertes par la Solution IA, sans intervention de MISTER IA dans le cadre des Services.

En cas de contradiction entre le présent Accord et le Contrat Commercial, le présent Accord prévaut pour toutes les stipulations relatives au Traitement de Données Personnelles réalisé par MISTER IA en qualité de Sous-traitant pour le compte du Client. Les stipulations du Contrat Commercial demeurent applicables pour les aspects commerciaux, financiers, opérationnels ou techniques des Services qui ne relèvent pas de la protection des Données Personnelles.

Les Parties reconnaissent que les Services fournis par MISTER IA peuvent varier selon l'offre souscrite par le Client, la Solution IA concernée, le nombre et le type de licences commandées, les fonctionnalités disponibles, le statut ou le secteur d'activité du Client, ainsi que les prestations effectivement confiées à MISTER IA.

En conséquence, les Traitements (et conditions afférentes) mentionnés dans le présent Accord ne s'appliquent au Client que dans la mesure où ils sont nécessaires aux Services effectivement fournis par MISTER IA pour le compte du Client.

Le présent Accord vise à encadrer l'ensemble des Traitements susceptibles d'être réalisés dans le cadre de la gestion de licences IA, sans que chaque Traitement listé ait vocation à s'appliquer systématiquement à tous les Clients ou à toutes les offres.

ARTICLE 3 – QUALIFICATIONS AU SEIN DE LA CHAÎNE DE TRAITEMENT

Pour les Traitements couverts par le présent Accord :

- Le Client agit en qualité de Responsable du Traitement.
- MISTER IA agit en qualité de Sous-traitant du Client.
- Les Fournisseurs de Solution IA ou autres prestataires auxquels MISTER IA recourt pour fournir les Services peuvent agir en qualité de Sous-traitants ultérieurs, lorsque les conditions prévues au présent Accord sont réunies.

Le Client demeure responsable de la détermination notamment :

- Des finalités poursuivies au moyen des Solutions IA.
- Des moyens essentiels du Traitement.
- Des catégories d'utilisateurs autorisés.
- Des catégories de Personnes concernées.
- Des catégories de Données Personnelles pouvant être traitées dans les Solutions IA.
- Des règles internes d'usage applicables aux utilisateurs.
- Des restrictions internes applicables aux Données Sensibles, confidentielles ou couvertes par un secret légal, professionnel ou contractuel.
- Des instructions données à MISTER IA dans le cadre de la fourniture des Services.

MISTER IA intervient pour gérer (administrer, paramétrer, suivre, optimiser) les licences IA pour le compte du Client et, plus généralement, fournir les Services souscrits par le Client, sur la base des instructions de ce dernier.

En tout état de cause, le Client reste responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que le Traitement est effectué conformément au RGPD et être en mesure de le démontrer.

ARTICLE 4 – DESCRIPTION DES TRAITEMENTS

Les Traitements de Données Personnelles réalisés par MISTER IA pour le compte du Client sont décrits en Annexe 1.

Cette Annexe 1 précise notamment :

- L'objet du Traitement.
- La ou les finalité(s) pour laquelle (lesquelles) les Données Personnelles sont traitées pour le compte du Client.
- La durée du Traitement.
- La nature du Traitement.
- Les catégories de Données Personnelles traitées.
- Les catégories de Personnes concernées.

ARTICLE 5 – INSTRUCTIONS DOCUMENTÉES DU CLIENT

MISTER IA ne traite les Données Personnelles que sur instruction documentée du Client, y compris en ce qui concerne les transferts de Données Personnelles vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel MISTER IA est soumis. Dans ce cas, MISTER IA informe le Client de cette obligation juridique avant le Traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Les instructions du Client résultent notamment :

- Du Contrat Commercial.
- Du présent Accord.
- De toute demande relative aux Services impliquant le Traitement de Données Personnelles.

Des instructions documentées peuvent également être données ultérieurement par le Client pendant toute la durée du Traitement de Données Personnelles.

MISTER IA peut suggérer des éléments qui, s'ils sont acceptés par le Client, deviennent partie intégrante des instructions données.

Ces instructions laissent néanmoins à MISTER IA une certaine latitude et marge d'appréciation quant à la manière de servir au mieux les intérêts du Client, en permettant notamment à MISTER IA de choisir les moyens techniques et organisationnels (non essentiels) les plus appropriés.

MISTER IA informe immédiatement le Client si, selon lui, une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

Une fois informé que l'une de ses instructions pourrait être contraire à la législation / réglementation en matière de protection des données, le Client devra évaluer la situation et déterminer si l'instruction constitue effectivement une violation de la législation / réglementation en matière de protection des données.

Lorsque MISTER IA estime qu'une instruction constitue une violation de la législation / réglementation en matière de protection des données, MISTER IA est en droit de :

- Suspendre la mise en œuvre de l'instruction concernée jusqu'à ce que le Client confirme, modifie ou retire son instruction.
- Résilier le Contrat Commercial (y compris le présent Accord) dans la mesure où il concerne le Traitement de Données Personnelles en vertu des présentes clauses lorsque, après avoir informé le Client que ses instructions enfreignent les exigences juridiques applicables conformément au présent article, le Client insiste pour que ses instructions soient suivies.

ARTICLE 6 – SÉCURITÉ DU TRAITEMENT

MISTER IA met en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Ces mesures de sécurité sont notamment précisées à l'Annexe II.

Lors de l'évaluation du niveau de sécurité approprié, les Parties tiennent dûment compte :

- De l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du Traitement.
- Des risques (dont le degré de probabilité et de gravité varie) que présente le Traitement pour les droits et libertés des Personnes concernées, notamment ceux résultant d'une Violation de Données Personnelles.

MISTER IA veille à ce que :

- Les personnes qu'il autorise à traiter les Données Personnelles s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
- Les membres de son personnel n'aient accès aux Données Personnelles faisant l'objet du Traitement que dans la mesure strictement nécessaire à la fourniture des Services ou à l'exécution, à la gestion ou au suivi du Contrat Commercial ou du présent Accord.

Les Parties reconnaissent que certaines mesures de sécurité relèvent directement des Fournisseurs de Solution IA et non de MISTER IA. Dans ce cas, MISTER IA communique au Client les informations raisonnablement disponibles concernant les mesures de sécurité du Fournisseur de Solution IA concerné, dans les limites prévues par les engagements contractuels de ce Fournisseur de Solution IA.

Le Client reconnaît que le degré de détail des informations relatives aux mesures de sécurité incluses dans le présent Accord lui permet d'apprécier le caractère approprié de ces mesures qu'il approuve.

ARTICLE 7 – RECOURS À DES SOUS-TRAITANTS ULTÉRIEURS

MISTER IA dispose de l'autorisation générale du Client pour ce qui est du recrutement des Sous-traitants ultérieurs afin de mener des activités de Traitement spécifiques pour le compte du Client.

Cette autorisation générale est accordée sur la base d'une liste convenue en Annexe 3 du présent Accord.

MISTER IA informe par écrit le Client de tout projet de modification de cette liste par l'ajout ou le remplacement de Sous-traitants ultérieurs, donnant ainsi au Client suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des Sous-traitants ultérieurs concernés.

Pour présenter ses objections, le Client dispose d'un délai de 15 jours à compter de la date de réception de l'information relative au changement de Sous-traitants ultérieurs. En l'absence d'opposition dans le délai imparti, le nouveau Sous-traitant ultérieur est réputé accepté par le Client. En cas d'opposition, dans le délai imparti, au recrutement d'un nouveau Sous-traitant ultérieur, le Client et MISTER IA collaboreront de bonne foi afin de trouver une solution mutuellement acceptable pour répondre à l'objection soulevée par le Client.

MISTER IA fournit au Client les informations nécessaires pour lui permettre d'émettre des objections à l'encontre de ce ou ces changement(s).

Lorsque MISTER IA recrute un Sous-traitant ultérieur pour mener des activités de Traitement spécifiques pour le compte du Client, il le fait au moyen d'un contrat (ou d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre) qui impose au Sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées à MISTER IA en vertu du présent Accord. Lorsque le Sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, MISTER IA demeure pleinement responsable devant le Client de l'exécution par le Sous-traitant ultérieur de ses obligations.

L'imposition des « mêmes » obligations est interprétée de manière fonctionnelle et non formelle : il n'est pas nécessaire que le contrat comporte exactement les mêmes termes que ceux utilisés dans le contrat conclu entre MISTER IA et le Client. Cela signifie également que si MISTER IA confie à un Sous-traitant ultérieur une partie spécifique du Traitement, à laquelle certaines des obligations ne peuvent s'appliquer, ces obligations ne devraient pas être mentionnées « par défaut » dans le contrat conclu avec le Sous-traitant ultérieur.

Les notions de Responsable du Traitement et de Sous-traitant sont des concepts fonctionnels : ils visent à répartir les responsabilités en fonction des rôles réels des parties. Cela implique que le statut juridique d'un acteur en tant que « Responsable du Traitement » ou « Sous-traitant » doit, en principe, être déterminé par ses activités réelles dans un cas particulier, plutôt que par la désignation formelle d'un acteur en tant que « Responsable du Traitement » ou « Sous-traitant » (par exemple, dans le cadre d'un contrat).

Les Parties reconnaissent ainsi que les conditions contractuelles, accords de traitement de données ou autres documentations standards de certains Fournisseurs de Solution IA ou autres prestataires peuvent ne pas refléter expressément l'ensemble de la chaîne de sous-traitance applicable aux Services, au regard notamment de la terminologie et des formulations employées. Cela n'a pas pour effet de modifier la répartition des rôles prévue par le présent Accord.

ARTICLE 8 – ASSISTANCE AU CLIENT

8.1. Sur les demandes d'exercice des droits prévus au chapitre III du RGPD

Dans toute la mesure du possible, MISTER IA prête assistance au Client, par des mesures techniques et organisationnelles appropriées, pour ce qui est de remplir l'obligation qui lui incombe de répondre

aux demandes des Personnes concernées d'exercer leurs droits prévus au chapitre III du RGPD, en tenant compte de la nature du traitement.

Le Client donne lui-même suite aux demandes d'exercice de droits formulées par les Personnes concernées.

Dans ce cadre, l'aide de MISTER IA consiste à :

- Transmettre rapidement au Client, par tous moyens appropriés, les demandes d'exercice de droits que MISTER IA aurait reçues directement de la part des Personnes concernées. En ce cas, MISTER IA peut éventuellement conseiller aux Personnes concernées de soumettre directement leurs demandes au Client.
- Le cas échéant, extraire ou traiter de toute autre manière les Données Personnelles pertinentes dans la mesure strictement nécessaire au respect par le Client de son obligation de donner suite aux demandes d'exercice des droits des Personnes concernées et sous réserve des possibilités raisonnables de MISTER IA.
- Le cas échéant, effectuer d'autres tâches spécifiques et/ou techniques dans la mesure strictement nécessaire au respect par le Client de son obligation de donner suite aux demandes d'exercice des droits des Personnes concernées et sous réserve des possibilités raisonnables de MISTER IA.

L'appréciation de la recevabilité des demandes d'exercice des droits des Personnes concernées et du respect des exigences imposées par le RGPD incombent au Client.

8.2. Sur d'autres obligations incombant au Client

En outre, compte tenu de la nature du Traitement et des informations dont dispose MISTER IA, ce dernier aide le Client à garantir le respect des obligations suivantes :

- Si nécessaire et sur demande, l'obligation de procéder à une évaluation de l'incidence des opérations de Traitement envisagées sur la protection des Données Personnelles (analyse d'impact relative à la protection des données) lorsqu'un type de Traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques. Il est rappelé qu'il incombe au Client, et non à MISTER IA, de prendre l'initiative de réaliser une analyse d'impact relative à la protection des données.
- Si nécessaire et sur demande, l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au Traitement lorsqu'une analyse d'impact relative à la protection des données indique que le Traitement présenterait un risque élevé si le Client ne prenait pas de mesures pour atténuer le risque.
- L'obligation de veiller à ce que les Données Personnelles soient exactes et à jour, en informant sans délai le Client si (et seulement si) MISTER IA apprend, dans le cadre de l'exécution des Services, que les Données Personnelles qu'il traite sont inexactes ou sont devenues obsolètes.

MISTER IA n'est toutefois pas tenu à une obligation générale de surveillance ou de recherche active de l'exactitude ou de la mise à jour des Données Personnelles fournies par le Client.

- Les obligations prévues à l'article 32 du RGPD, s'agissant notamment de la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité du Traitement adapté au risque.

8.3. Sur la notification de Violations de Données Personnelles

En cas de Violation de Données Personnelles dans le cadre des Services souscrits par le Client et des Traitements effectués par MISTER IA en qualité de Sous-traitant, MISTER IA coopère avec le Client et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu

des articles 33 et 34 du RGPD, en tenant compte de la nature du Traitement et des informations dont dispose MISTER IA, selon les modalités définies ci-après.

En tout état de cause, la responsabilité juridique d'une notification / communication de Violation de Données Personnelles incombe au Client.

8.3.1. Violation de Données Personnelles en rapport avec des Données Personnelles traitées par le Client

En cas de Violation de Données Personnelles en rapport avec des Données Personnelles traitées par le Client et faisant l'objet des Traitements décrits à l'Annexe 1, MISTER IA prête assistance au Client :

- Aux fins de la notification de la Violation de Données Personnelles à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le Client en a eu connaissance, le cas échéant (sauf si la Violation de Données Personnelles est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques).
- Aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3 du RGPD, doivent figurer dans la notification du Client, et inclure, au moins :
 - La nature de la Violation de Données Personnelles, y compris, si possible, les catégories et le nombre approximatif de Personnes concernées par la Violation de Données Personnelles et les catégories et le nombre approximatif d'enregistrements de Données Personnelles concernés.
 - Les conséquences probables de la Violation de Données Personnelles.
 - Les mesures prises ou les mesures que le Client propose de prendre pour remédier à la Violation de Données Personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

- Aux fins de la satisfaction, conformément à l'article 34 du RGPD, de l'obligation de communiquer dans les meilleurs délais la Violation de Données Personnelles à la Personne concernée, lorsque la Violation de Données Personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

8.3.2. Violation de Données Personnelles en rapport avec des Données Personnelles traitées par MISTER IA

En cas de Violation de Données Personnelles en rapport avec des Données Personnelles traitées par MISTER IA, celui-ci en informe le Client dans les meilleurs délais après en avoir pris connaissance.

Cette notification contient au moins :

- Une description de la nature de la Violation de Données Personnelles constatée (y compris, si possible, les catégories et le nombre approximatif de Personnes concernées par la Violation de Données Personnelles et d'enregistrements de Données Personnelles concernés).
- Les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la Violation de Données Personnelles.
- Ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la Violation de Données Personnelles, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

8.4. Modalités, portée et étendue de l'assistance

Le devoir d'assistance de MISTER IA ne consiste pas en un transfert de responsabilité, car ces obligations demeurent imposées au Client.

L'assistance fournie par MISTER IA au titre du présent article est limitée aux actions strictement nécessaires et proportionnées pour permettre au Client de satisfaire aux obligations qui lui incombent au titre des dispositions précitées, compte tenu :

- De la nature des Traitements réalisés par MISTER IA.
- Des Données Personnelles et des informations dont MISTER IA dispose.
- Des fonctionnalités des Solutions IA concernées.
- Des accès et moyens techniques raisonnablement disponibles pour MISTER IA.
- De la complexité, de l'urgence et des risques associés à la demande.

Le Client utilise en priorité les informations, accès, fonctionnalités et moyens dont il dispose directement.

Le Client sollicite l'assistance de MISTER IA lorsqu'il ne peut raisonnablement satisfaire seul, en tout ou partie, à l'obligation concernée, notamment lorsque l'intervention nécessite une information détenue par MISTER IA, un accès dont il dispose ou la réalisation d'une opération technique relevant des Services.

En sus des modalités particulières d'assistance applicables à certaines obligations spécifiques, il est également précisé que toute demande d'assistance est :

- Adressée par écrit à MISTER IA.
- Comporte les informations raisonnablement nécessaires à son Traitement, notamment l'obligation concernée, la nature de l'assistance demandée, les Données Personnelles et les Personnes concernées, les opérations attendues ainsi que, le cas échéant, le délai applicable.

MISTER IA peut demander au Client toute précision complémentaire nécessaire avant d'exécuter la demande.

MISTER IA n'est pas tenu :

- D'effectuer des opérations que le Client peut raisonnablement réaliser lui-même au moyen des accès et fonctionnalités dont il dispose.
- De répéter une opération ou de fournir une information déjà mise à la disposition du Client.
- De réaliser des opérations étrangères aux Services effectués ou aux Traitements confiés en qualité de Sous-traitant, ou nécessitant le développement de fonctionnalités non comprises dans les Services, sauf accord écrit entre les Parties.
- D'accéder à des Données Personnelles plus nombreuses que celles strictement nécessaires à l'assistance demandée.

L'assistance de MISTER IA ne vaut ni validation de la conformité des Traitements du Client ni transfert à MISTER IA des obligations ou responsabilités incombant au Client en sa qualité de Responsable du Traitement.

Le Client demeure notamment responsable de l'opportunité des mesures prises, des décisions adoptées, du contenu des réponses adressées aux Personnes concernées, de la notification /

communication de Violations de Données Personnelles ou encore du respect des délais prévus par la législation / réglementation applicable.

ARTICLE 9 – DOCUMENTATION ET CONFORMITÉ

Les Parties doivent pouvoir démontrer la conformité avec les présentes clauses.

MISTER IA traite dans un délai raisonnable les demandes du Client concernant le Traitement des Données Personnelles conformément aux présentes clauses.

MISTER IA met à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD.

À la demande écrite du Client, MISTER IA permet également la réalisation d'audits des activités de Traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. L'objet de ces audits est de garantir que le Client dispose de toutes les informations relatives à l'activité de Traitement effectuée pour son compte et aux garanties fournies par MISTER IA.

Le Client peut décider de procéder lui-même à l'audit ou de mandater, à ses propres frais, un auditeur indépendant. MISTER IA peut suggérer un auditeur particulier, mais la décision finale revient au Client. Lorsque MISTER IA demande un audit, il supporte les frais exposés par l'auditeur indépendant.

Dans ce cadre, le Client peut également tenir compte, le cas échéant, des certifications pertinentes en possession de MISTER IA.

Les audits sont effectués moyennant un préavis raisonnable.

Les Parties coopèrent de bonne foi et déterminent si, comment et quand il convient de réaliser des audits, ainsi que le type d'audit ou d'inspection (à distance, sur site, ou d'une autre manière pour recueillir les informations nécessaires) qui serait nécessaire et approprié dans le cas d'espèce, compte tenu également des préoccupations en matière de sécurité.

Les Parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

ARTICLE 10 – SORT DES DONNÉES PERSONNELLES AU TERME DE LA PRESTATION DE SERVICES RELATIFS AU TRAITEMENT

À la fin des Services (en particulier en cas de résiliation du Contrat Commercial ou, plus généralement, en cas de cessation du Contrat Commercial, y compris le présent Accord, pour quelque cause que ce soit), selon le choix du Client, MISTER IA supprime toutes les Données Personnelles traitées pour le compte du Client et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les Données Personnelles au Client et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps.

MISTER IA continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des Données Personnelles.

ARTICLE 11 – TRANSFERTS INTERNATIONAUX DE DONNÉES PERSONNELLES

Tout transfert de Données Personnelles vers un pays tiers (hors UE ou EEE) ou une organisation internationale par MISTER IA n'est effectué que sur la base d'instructions documentées du Client ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle MISTER IA est soumis et s'effectue conformément au chapitre V du RGPD.

Le Client convient que, lorsque MISTER IA recrute un Sous-traitant ultérieur conformément à l'article 7 pour mener des activités de Traitement spécifiques (pour le compte du Client) et que ces activités de Traitement impliquent un transfert de Données Personnelles au sens du chapitre V du RGPD, MISTER

IA et le Sous-traitant ultérieur peuvent encadrer le transfert conformément au chapitre V du RGPD notamment, mais sans s'y limiter, via l'existence d'une décision d'adéquation au sens de l'article 45 du RGPD ou, en l'absence d'une telle décision, en présence de garanties appropriées en utilisant, par exemple, les clauses contractuelles types adoptées par la Commission européenne sur la base de l'article 46, paragraphe 2, du RGPD, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

ARTICLE 12 – RÈGLES PARTICULIÈRES RELATIVES AUX CONTENUS IA

Le Client demeure seul responsable des Contenus IA qu'il choisit de saisir, importer, téléverser, transmettre ou faire traiter au moyen des Solutions IA.

Le Client s'engage à définir et communiquer à ses utilisateurs les règles internes applicables à l'usage des Solutions IA et à l'utilisation des Services, notamment concernant :

- Les catégories de Données Personnelles pouvant être saisies.
- Les Données Sensibles.
- Les données interdites ou soumises à validation préalable.
- Les données confidentielles, couvertes par le secret professionnel, le secret des affaires ou toute autre exigence de confidentialité.

Le Client demeure responsable de l'adoption de ses règles, de leur diffusion et de leur respect par ses utilisateurs.

MISTER IA n'accède pas aux Contenus IA et ne traite pas les Contenus IA sauf si :

- Le Client a autorisé le Traitement par MISTER IA de ces Contenus IA.
- Le Client le demande expressément.
- Le Client les transmet volontairement à MISTER IA (dans le cadre, par exemple, d'une demande de support).
- Une prestation spécifique convenue avec le Client nécessite cet accès ou un autre Traitement.

ARTICLE 13 – RÔLES D'ADMINISTRATEUR CONFIÉS À MISTER IA

Dans le cadre de certaines Solutions IA, MISTER IA peut se voir attribuer, pour les besoins des Services, un rôle d'administration de l'espace du Client.

Selon la Solution IA concernée, ce rôle peut notamment être désigné par les termes « administrateur », « propriétaire » (« Owner »), « propriétaire principal » (« Primary Owner ») ou toute autre qualification employée par le Fournisseur de Solution IA.

Ces intitulés sont propres à la Solution IA concernée et ne modifient pas, à eux seuls, la répartition des rôles entre le Client et MISTER IA au titre du présent Accord.

MISTER IA n'utilise les droits attachés à ces rôles que pour les besoins des Services et conformément aux instructions documentées du Client.

Les droits attachés au rôle confié à MISTER IA dépendent de la Solution IA concernée, des Services souscrits, de la configuration retenue et des fonctionnalités mises à disposition par le Fournisseur de Solution IA.

Le rôle d'administrateur confié peut notamment permettre, selon le rôle effectivement attribué :

- De fournir tout ou partie des Services.
- D'ajouter ou désactiver des utilisateurs.
- De gérer des niveaux d'accès et des plafonds de dépense.
- D'autoriser ou de bloquer des connecteurs.
- De déployer des paramètres au niveau de l'espace du Client.
- De traiter certaines métadonnées ou autres Données Personnelles.

ARTICLE 14 – DURÉE

Le présent Accord entre en vigueur à la date de sa conclusion qui peut être matérialisée par l'acceptation / la signature du Contrat Commercial (comprenant le présent Accord) ou l'acceptation / la signature du présent Accord seul.

Il demeure applicable pendant toute la durée des Services impliquant le Traitement de Données Personnelles pour le compte du Client (en particulier jusqu'à la résiliation du Contrat Commercial ou, plus généralement, jusqu'à la cessation du Contrat Commercial, y compris le présent Accord, pour quelque cause que ce soit) et aussi longtemps que MISTER IA traite des Données Personnelles pour le compte du Client afin notamment d'assurer la suppression ou la restitution des Données Personnelles dans les conditions prévues à l'article 10 du présent Accord.

ARTICLE 15 – MISE À JOUR DE L'ACCORD

Les Parties reconnaissent que les Services, les Solutions IA, leurs fonctionnalités, leurs conditions contractuelles et leurs modalités peuvent évoluer.

Le présent Accord pourra ainsi être mis à jour afin de tenir compte notamment :

1. D'une évolution des Traitements de Données Personnelles.
2. D'une évolution des Services.
3. De l'ajout ou du retrait d'une Solution IA.
4. D'un changement de Sous-traitants ultérieurs.
5. D'un changement de Fournisseur de Solution IA.
6. D'une évolution des conditions contractuelles ou DPA d'un Fournisseur de Solution IA.
7. D'une évolution légale, réglementaire ou jurisprudentielle.

Sans préjudice du mécanisme particulier (autorisation générale) prévu à l'article 7 et applicable au recrutement de Sous-traitants ultérieurs, la mise en œuvre de l'Accord mis à jour est soumise à l'information et l'acceptation préalables du Client.

ARTICLE 16 – POINT DE CONTACT RELATIF AUX DONNÉES PERSONNELLES

Pour toute question relative aux Traitements de Données Personnelles réalisés dans le cadre du présent Accord et de la fourniture des Services, le Client peut contacter MISTER IA à l'adresse électronique suivante : privacy@mister-ia.com

Cette adresse constitue le point de contact de MISTER IA pour les demandes relatives à la protection des Données Personnelles, notamment concernant le présent Accord, les Traitements réalisés par MISTER IA en qualité de Sous-traitant, les demandes d'information du Client, les demandes d'assistance, les Violations de Données Personnelles et les demandes relatives aux Sous-traitants ultérieurs.

ANNEXES :

- Annexe 1 – Description du Traitement réalisé pour le compte du Client.
- Annexe 2 – Mesures de sécurité techniques et organisationnelles fournies par MISTER IA.
- Annexe 3 – Liste des Sous-traitants ultérieurs.

ANNEXE 1 – DESCRIPTION DU TRAITEMENT RÉALISÉ POUR LE COMPTE DU CLIENT

Les Traitements décrits dans la présente Annexe 1 s'appliquent uniquement dans la mesure où ils correspondent aux Services effectivement souscrits et activés par le Client.

Le périmètre des Traitements dépend notamment de la Solution IA concernée, du nombre et du type de licences commandées, des fonctionnalités disponibles, du statut professionnel ou du secteur d'activité du Client, ainsi que des prestations effectivement confiées à MISTER IA.

En conséquence, l'ensemble des Traitements, finalités, catégories de Données Personnelles et catégories de Personnes concernées mentionnés dans la présente Annexe n'est pas nécessairement applicable à chaque Client.

La présente Annexe vise à encadrer l'ensemble des Traitements susceptibles d'être réalisés dans le cadre des Services, sans que chacun des éléments décrits ait vocation à s'appliquer systématiquement à tous les Clients ou à toutes les offres.

OBJET DU TRAITEMENT	La fourniture des Services effectivement souscrits par le Client.
DURÉE DU TRAITEMENT	Les Traitements sont réalisés pendant la durée des Services effectivement souscrits par le Client, conformément au Contrat Commercial et au présent Accord. À la cessation des Services concernés, MISTER IA ne poursuit les Traitements que pendant la période nécessaire à la restitution ou à la suppression des Données Personnelles et à la clôture des comptes et accès, conformément aux modalités prévues à l'article 10 du présent Accord et, le cas échéant, aux conditions afférentes à la Solution IA concernée. Lorsque le droit de l'Union européenne ou le droit d'un État membre impose le Traitement de certaines Données Personnelles (notamment leur conservation), celles-ci sont traitées pendant la seule durée légalement requise.
NATURE DU TRAITEMENT	Selon les Services effectivement souscrits : - Réception et collecte. - Enregistrement, organisation, structuration et conservation. - Création, activation, attribution, réaffectation, suspension et suppression des comptes, licences et accès. - Paramétrage et modification des comptes, rôles, habilitations et espaces associés. - Consultation et utilisation. - Agrégation et analyse. - Production d'indicateurs, de rapports et de recommandations. - Transmission, communication ou mise à disposition. - Journalisation et traçabilité des opérations. - Limitation ou restriction des accès. - Restitution, suppression, destruction.

FINALITÉ(S) DU TRAITEMENT	Gestion des licences IA dans le cadre des Services effectivement souscrits par le Client comprenant selon les cas : - L'acquisition, la mise à disposition et l'attribution des licences IA. - Le paramétrage des licences IA. - La formulation de suggestions et de recommandations personnalisées relatives aux nouvelles fonctionnalités, aux nouveaux paramétrages ou aux optimisations d'usage potentielles, notamment dans le cadre de la veille technologique réalisée par MISTER IA. - La gestion centralisée des mouvements de licences et d'utilisateurs, notamment leur ajout, leur attribution, leur réaffectation, leur suspension ou leur retrait, ainsi que l'identification des licences inutilisées. - L'analyse de l'utilisation des Solutions IA pour fournir des indicateurs, rapports et recommandations relatifs notamment à l'activation, à l'utilisation et à l'optimisation des licences IA. - La fourniture d'une assistance aux utilisateurs concernant l'utilisation et la gestion des licences IA.
CATÉGORIES DE DONNÉES PERSONNELLES TRAITÉES	Selon les Services effectivement souscrits et les fonctionnalités de la Solution IA concernée, les catégories de Données Personnelles susceptibles d'être traitées sont les suivantes : - Identité, coordonnées professionnelles et vie professionnelle (ex : nom, prénom, adresse électronique professionnelle, numéro de téléphone professionnel, organisme, direction ou service de rattachement, fonction ou qualité professionnelle). - Données de Compte, de Licence et d'Habilitation. - Données de Connexion et de Traçabilité. - Données d'Usage. - Données de Support. - Données Personnelles contenues dans les Contenus IA.

	Les Services ne sont pas destinés, par défaut, au Traitement de Données Sensibles. Lorsque le Client envisage de traiter des Données Sensibles au moyen d'une Solution IA, il doit en informer préalablement MISTER IA afin que les Parties puissent vérifier : - La compatibilité de cet usage avec les conditions contractuelles de la Solution IA concernée. - L'existence ou non d'un DPA adapté avec le Fournisseur de Solution IA. - Les garanties prévues par le Fournisseur de Solution IA. - Les limitations spécifiques et les garanties supplémentaires applicables. - Les mesures techniques et organisationnelles nécessaires. À défaut d'accord écrit spécifique entre les Parties et de validation de la compatibilité de la Solution IA concernée, le Client s'engage à ne pas utiliser les Services pour traiter des Données Sensibles.
CATÉGORIES DE PERSONNES CONCERNÉES	Selon les Services effectivement souscrits et l'utilisation faite des Solutions IA par le Client, les Personnes Concernées peuvent comprendre : - Les utilisateurs actuels, futurs ou anciens auxquels le Client attribue ou envisage d'attribuer un compte, un accès ou une licence, notamment ses salariés, dirigeants, agents, membres, stagiaires, travailleurs temporaires, consultants, prestataires ou autres collaborateurs autorisés. - Les administrateurs des espaces clients ainsi que les contacts techniques, fonctionnels, de sécurité, de gestion des licences ou de support. - Les personnes qui adressent une demande de support ou dont les Données Personnelles sont mentionnées dans une telle demande. - Les personnes dont les Données Personnelles sont saisies, importées, transmises ou autrement traitées dans les Contenus IA par le Client, notamment, selon l'activité du Client, ses clients, prospects, patients, usagers, bénéficiaires, candidats, salariés, fournisseurs, partenaires, conseils, etc. A toutes fins utiles, il est rappelé que MISTER IA ne peut anticiper de façon exhaustive toutes les catégories de Personnes concernées dont les Données Personnelles sont introduites dans les Contenus IA notamment. Cette détermination relève du Client, en sa qualité de Responsable du Traitement.

ANNEXE 2 – MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES FOURNIES PAR MISTER IA

Les mesures décrites dans la présente Annexe sont mises en œuvre ou configurées par MISTER IA selon les Services effectivement fournis, la Solution IA concernée, les fonctionnalités disponibles, les accès confiés à MISTER IA, le périmètre retenu avec le Client et les instructions documentées de ce dernier.

Les Parties reconnaissent que certaines mesures relèvent directement de MISTER IA, tandis que d'autres relèvent des paramètres disponibles au sein des Solutions IA ou des garanties déclarées par les Fournisseurs de Solutions IA.

MISTER IA ne garantit pas la disponibilité de paramètres, fonctionnalités, certifications ou garanties qui relèveraient exclusivement des Fournisseurs de Solutions IA.

La présente Annexe, sans prétendre à l'exhaustivité, présente les principales mesures de sécurité fournies par MISTER IA et connues à la date de conclusion de l'Accord.

MISTER IA peut faire évoluer les mesures décrites dans la présente Annexe afin de tenir compte de l'évolution des Services, des Solutions IA, des risques identifiés, des pratiques de sécurité, de l'état des connaissances ou des exigences légales et réglementaires applicables.

Si nécessaire, le Client peut demander à MISTER IA des informations complémentaires pour apprécier le caractère approprié des mesures de sécurité mises en œuvre conformément à l'article 32 du RGPD. En l'absence d'une telle demande, le Client reconnaît que le degré de détail des informations relatives aux mesures de sécurité incluses dans le présent Accord lui permet d'apprécier le caractère approprié de ces mesures qu'il approuve.

1. Mesures internes mises en œuvre par MISTER IA

1.1. Authentification

MISTER IA met en œuvre des mesures d'authentification destinées à sécuriser les accès, notamment l'authentification multifacteur lorsque celle-ci est disponible, activée et applicable aux comptes concernés.

Une authentification multifacteur a pour caractéristique de s'appuyer sur plusieurs preuves, appelées facteurs d'authentification, appartenant à au moins deux des trois catégories suivantes :

- Facteur de connaissance (ce que la personne sait).
- Facteur de possession (ce que la personne a).
- Facteur d'inhérence (ce que la personne est ou fait).

1.2. Limitation des accès aux consoles clients

MISTER IA limite l'accès aux consoles clients à l'équipe chargée de l'activité de gestion de licences IA.

1.3. Gestion des autorisations selon le principe du moindre privilège

MISTER IA applique le principe du moindre privilège, c'est-à-dire que seules sont accordées les autorisations strictement nécessaires à l'exécution des actions dont l'utilité est avérée.

1.4. Gestion des incidents

MISTER IA dispose d'une pratique opérationnelle de gestion des incidents.

Lorsqu'un incident est susceptible de constituer une Violation de Données Personnelles, MISTER IA l'analyse afin de déterminer les suites à donner et, le cas échéant, d'en informer le Client dans les conditions prévues au présent Accord.

2. Mesures configurées par MISTER IA dans les Solutions IA

Selon la Solution IA concernée, les fonctionnalités disponibles, le niveau d'offre souscrit et les instructions du Client, MISTER IA peut configurer ou accompagner la configuration des mesures suivantes.

2.1. Authentification unique

MISTER IA peut configurer ou accompagner la configuration du SSO lorsque cette fonctionnalité est disponible dans la Solution IA concernée.

2.2. Désactivation de l'utilisation des données pour l'entraînement des modèles

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration des paramètres visant à désactiver l'utilisation des données du Client pour l'entraînement des modèles.

Cette mesure dépend des paramètres effectivement disponibles dans la Solution IA concernée et des conditions contractuelles applicables auprès du Fournisseur de Solution IA.

2.3. Paramétrage des rétentions

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration des paramètres de rétention applicables au sein de la Solution IA concernée.

2.4. Gestion des rôles et permissions

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration des rôles et permissions disponibles, notamment les rôles administrateurs et membres.

2.5. Provisioning SCIM

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration du provisioning SCIM.

2.6. Restriction des connecteurs et MCP autorisés

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la restriction des connecteurs et MCP autorisés.

2.7. Désactivation des évaluations / feedbacks utilisateurs

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration des paramètres visant à désactiver les évaluations / feedbacks utilisateurs.

2.8. Désactivation des métadonnées de localisation

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration des paramètres visant à désactiver les métadonnées de localisation.

2.9. Désactivation des connecteurs par défaut

Lorsque la Solution IA le permet, MISTER IA configure ou accompagne la configuration des paramètres visant à désactiver les connecteurs par défaut, sauf demande contraire du Client.

3. Garanties déclarées par les Fournisseurs de Solution IA

Certaines mesures de sécurité, telles que décrites plus précisément au sein de l'Annexe 3 du présent Accord, relèvent directement des Fournisseurs de Solutions IA. La connaissance de ces mesures et garanties procède notamment de :

- Du Data Processing Agreement (ou tout autre contrat ou autre acte juridique au titre du droit de l'Union ou du droit d'un État membre) conclu avec le Fournisseur de Solution IA concerné.
- Du Contrat Commercial du Fournisseur de Solution IA.
- Des certifications, attestations ou rapports d'audit déclarés par le Fournisseur de Solution IA notamment, et de manière non exhaustive, ISO 27001, ISO 42001 ou SOC 2 Type II, lorsque ces certifications sont effectivement applicables à la Solution IA concernée et au périmètre utilisé.

ANNEXE 3 – LISTE DES SOUS-TRAITANTS ULTÉRIEURS

I. PRINCIPES APPLICABLES À LA LISTE DES SOUS-TRAITANTS ULTÉRIEURS

MISTER IA recourt à certains Sous-traitants ultérieurs afin de mener des activités de Traitements spécifiques pour le compte du Client et fournir les Services correspondants.

La présente Annexe identifie les Sous-traitants ultérieurs autorisés dans le cadre du présent Accord et de l'autorisation générale accordée.

Il est rappelé que la décision finale de recruter un Sous-traitant ultérieur, et la responsabilité qui en découle, y compris en ce qui concerne la vérification du caractère suffisant des garanties fournies par le Sous-traitant ultérieur, incombent au Client en sa qualité de Responsable du Traitement.

En acceptant le présent Accord, le Client reconnaît avoir reçu ou avoir pu accéder aux informations mises à disposition concernant les Sous-traitants ultérieurs listés dans la présente Annexe et estime que ces informations sont suffisantes pour lui permettre d'apprécier les garanties présentées par ces Sous-traitants ultérieurs au regard des Traitements concernés.

Lorsque le Client estime que les informations fournies ou mises à disposition sont incomplètes, insuffisantes, inexactes ou soulèvent des questions particulières, il peut solliciter MISTER IA afin d'obtenir des informations complémentaires, notamment celles raisonnablement nécessaires à l'appréciation des garanties présentées par le Sous-traitant ultérieur concerné.

Lorsque cela est nécessaire, MISTER IA peut, sur demande écrite du Client, communiquer des informations complémentaires, notamment celles relatives au contrat conclu avec le Sous-traitant ultérieur concerné, voire une copie ou des extraits dudit contrat, dans la mesure où cette communication est possible. Cette demande doit préciser le Sous-traitant ultérieur concerné, les informations sollicitées, le Traitement concerné et les raisons pour lesquelles les informations déjà mises à disposition seraient insuffisantes.

MISTER IA répond dans un délai raisonnable, dans la limite des informations dont elle dispose ou auxquelles elle peut raisonnablement accéder, et sous réserve de la protection des informations confidentielles, secrets d'affaires, mesures de sécurité sensibles et Données Personnelles de tiers.

MISTER IA peut occulter, purger ou caviarder les éléments confidentiels, non communicables ou non pertinents avant toute communication.

II. FOURNISSEURS DE SOLUTION IA

1. INTERPRÉTATION ET ARTICULATION AVEC LES CONDITIONS DES FOURNISSEURS DE SOLUTIONS IA

Lorsqu'un Fournisseur de Solution IA traite des Données Personnelles afin de permettre à MISTER IA de fournir les Services pour le compte du Client, ce Fournisseur intervient, pour les Traitements concernés, en qualité de Sous-traitant ultérieur de MISTER IA.

Les notions de Responsable du Traitement et de Sous-traitant sont des concepts fonctionnels : ils visent à répartir les responsabilités en fonction des rôles réels des parties. Cela implique que le statut juridique d'un acteur en tant que « Responsable du Traitement » ou « Sous-traitant » doit, en principe, être déterminé par ses activités réelles dans un cas particulier, plutôt que par la désignation formelle d'un acteur en tant que « Responsable du Traitement » ou « Sous-traitant » (par exemple, dans le cadre d'un contrat).

Les Parties reconnaissent ainsi que les conditions contractuelles, accords de traitement de données ou autres documentations standards de certains Fournisseurs de Solution IA peuvent ne pas refléter expressément l'ensemble de la chaîne de sous-traitance applicable aux Services, au regard notamment de la terminologie et des formulations employées.

Les termes ou qualifications tels que notamment « Customer », « Client », « Organization », « Controller » (« Responsable du traitement ») ou toute notion équivalente employés dans ces documents désignent souvent MISTER IA en sa qualité de cocontractant, de titulaire du compte ou d'administrateur dans sa relation avec le Fournisseur de Solution IA. Toutefois, dans les rapports entre le Client et MISTER IA, ces désignations n'ont pas pour effet de modifier la répartition des rôles prévue par le présent Accord.

En particulier, le fait que MISTER IA soit désigné comme « Customer » « Organization » ou « Controller » (« Responsable du Traitement ») dans les conditions standards d'un Fournisseur de Solution IA ne signifie pas, pour les Traitements réalisés pour le compte du Client, que MISTER IA détermine les finalités et les moyens essentiels de ces Traitements qui doivent être déterminés par le Client.

Les obligations qui relèvent, par leur nature, du Responsable du Traitement au regard du RGPD demeurent à la charge du Client.

Le présent article est sans préjudice des Traitements pour lesquels MISTER IA ou le Fournisseur de Solution IA agit, le cas échéant, en qualité de Responsable du Traitement distinct.

2. LISTE DU OU DES FOURNISSEUR(S) DE SOLUTION IA AGISSANT EN QUALITÉ DE SOUS-TRAITANTS ULTERIEUR(S)

2.1. OpenAI

2.1.1. Fiche de présentation synthétique

OpenAI	
Solution IA concernée	ChatGPT
Entité contractante	OpenAI Ireland Ltd.
Adresse	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43
Personne de contact	privacy@openai.com
Objet du Traitement	OpenAI traite les Données Personnelles afin de fournir la Solution IA ChatGPT et les services associés.
Durée du Traitement	Au sein de son Data Processing Addendum (DPA), OpenAI indique que le Traitement est réalisé pendant la durée du contrat applicable conclu entre OpenAI et MISTER IA, ainsi que le temps nécessaire pour que soient remplies les obligations applicables à l'issue du Traitement, notamment celles relatives à la suppression des données. Dans la relation entre le Client et MISTER IA, OpenAI traite toutefois les Données Personnelles du Client en tant que Sous-traitant ultérieur uniquement pendant la période au cours de laquelle la Solution IA ChatGPT est effectivement fournie au Client dans le cadre des Services. En conséquence, la durée du Traitement réalisé par OpenAI pour le compte du Client ne peut, sauf exceptions, excéder la durée pendant

	laquelle MISTER IA est autorisé à traiter les Données Personnelles concernées pour fournir les Services au Client. La poursuite éventuelle du contrat conclu entre OpenAI et MISTER IA pour les besoins d'autres clients n'emporte pas la poursuite du Traitement des Données Personnelles du Client. À la cessation des Services pour le Client, MISTER IA procède à la désactivation des comptes et accès concernés et met en œuvre, dans la mesure permise par les fonctionnalités et conditions contractuelles applicables, les opérations de restitution ou de suppression des Données Personnelles auprès d'OpenAI. Ces opérations demeurent soumises aux délais et modalités de suppression, aux cycles de sauvegarde, aux conditions contractuelles prévues par le DPA OpenAI ainsi que les exigences légales / réglementaires.
Aperçu des garanties mises en œuvre par OpenAI	Aux termes de son DPA, OpenAI déclare mettre en œuvre et maintenir des mesures de sécurité organisationnelles et techniques raisonnables et appropriées pour protéger les Données Personnelles. Ces mesures comprennent notamment les éléments suivants : - Des mesures relatives au contrôle d'identité, à l'authentification et à l'autorisation d'accès de ses employés / services internes telles que : - o L'authentification unique (SSO) pour l'authentification auprès des services tiers. - o Des contrôles d'accès basés sur les rôles (« Role Based Access Controls » ou RBAC) lors de l'attribution des accès internes. - o L'authentification multifacteur obligatoire pour s'authentifier auprès du fournisseur d'identité d'OpenAI. - o Identifiants de connexion uniques attribués à chaque utilisateur. - o Des audits d'accès périodiques menés afin de s'assurer que les niveaux d'accès sont adaptés aux rôles exercés par chaque utilisateur. - o Des procédures établies pour révoquer rapidement les droits d'accès en cas de départ d'un employé. - o Des procédures pour signaler et révoquer les identifiants compromis, tels que les mots de passe et les clés API. - o Des procédures de réinitialisation des mots de passe, y compris des procédures visant à vérifier l'identité d'un utilisateur avant la création d'un nouveau mot de passe, d'un mot de passe de remplacement ou d'un mot de passe temporaire. - Des mesures relatives au contrôle d'identité, à l'authentification et à l'autorisation des clients telles que : - o L'utilisation d'un service tiers de gestion des identités et des accès pour gérer l'identité des clients. - o La séparation logique des données des clients à l'aide d'identifiants uniques. - La sécurité de l'infrastructure cloud et du réseau, à travers : - o La séparation des environnements de production et hors production.

	○ Des ressources principales « backend » déployées derrière un VPN. ○ Des audits réguliers visant à détecter les failles de sécurité. ○ Des secrets d'application et des comptes de service gérés par un service de gestion des secrets. ○ Des politiques de sécurité réseau et des pare-feux configurés selon le principe du « moindre privilège » par rapport à un ensemble préétabli de flux de trafic autorisés. ○ Le blocage des flux de trafic non autorisés. ○ La surveillance des journaux (logs) des services à des fins de sécurité et de disponibilité. - Le contrôle des systèmes et des postes de travail (y compris les ordinateurs portables et l'infrastructure sur site) : ○ Gestion des terminaux des postes de travail de l'entreprise. ○ Gestion des terminaux des appareils mobiles. ○ Application automatique des configurations de sécurité aux postes de travail. ○ Gestion obligatoire des correctifs. ○ Tenue de journaux (logs) de sécurité appropriés. - Le contrôle d'accès aux données afin d'empêcher les utilisateurs autorisés d'accéder à des données au-delà de leurs droits d'accès et afin d'empêcher la saisie, la lecture, la copie, la suppression, la modification ou la divulgation non autorisées de données : ○ L'accès des employés suit le principe du « moindre privilège ». ○ Seuls les employés dont les fonctions impliquent de contribuer à la fourniture des services sont habilités à accéder à l'environnement des services. - Des mesures visant à empêcher tout accès, toute altération ou toute suppression non autorisés des données pendant leur transfert, et afin de sécuriser et journaliser tous les transferts, telles que : ○ Le chiffrement des données au repos dans les bases de données de production à l'aide d'algorithmes de chiffrement robustes. ○ Le chiffrement des données en transit. ○ Une piste d'audit pour toutes les demandes d'accès aux données des bases de données de production. ○ Un chiffrement complet du disque obligatoire sur tous les postes de travail de l'entreprise. ○ Des contrôles de gestion des appareils obligatoires sur tous les postes de travail de l'entreprise. ○ Des restrictions relatives à l'utilisation de supports portables ou amovibles. - Des mesures visant à garantir le bon fonctionnement des services et le contrôle de la disponibilité notamment en cas d'intention malveillante, telles que : ○ Le fait de veiller à ce que les systèmes puissent être restaurés en cas d'interruption. ○ Le fait de veiller au bon fonctionnement des systèmes et au signalement des défaillances.
--	---

	○ La mise en œuvre systématique de solutions de lutte contre les logiciels malveillants et de détection/prévention des intrusions. - Des mesures visant à assurer le traitement séparé des données collectées à des fins différentes, notamment via : ○ La séparation logique des données des clients. ○ La restriction de l'accès aux données stockées à des fins différentes en fonction des rôles et des responsabilités du personnel. ○ La séparation des fonctions des systèmes d'information d'entreprise. ○ La séparation des environnements de test et de production des systèmes d'information. - Des mesures relatives à la détection et la gestion des risques liés à la cybersécurité, notamment : ○ La modélisation des menaces afin de recenser et de classer par ordre de priorité les sources de risques de sécurité en vue de leur traitement. ○ Des tests d'intrusion effectués au moins annuellement. ○ Sur demande, OpenAI peut fournir un résumé détaillé des tests effectués et indiquera si les problèmes identifiés ont été résolus. ○ Recours annuel à un auditeur externe indépendant et qualifié pour effectuer des examens périodiques des pratiques de sécurité d'OpenAI au regard de normes d'audit reconnues, y compris des audits de certification SOC 2 Type II. Sur demande raisonnable, OpenAI fournira un résumé détaillé. ○ Un programme de gestion des vulnérabilités conçu pour garantir la correction rapide des vulnérabilités. - Des mesures de formation et de gestion du personnel concernant les questions de sécurité, notamment : ○ Des vérifications des antécédents, lorsque cela est légalement permis, des employés ayant accès aux données client ou intervenant dans d'autres aspects des services. ○ Une formation annuelle à la sécurité pour les employés, ainsi que des formations complémentaires à la sécurité si nécessaire. - Des mesures visant à empêcher tout accès physique non autorisé aux locaux, notamment : ○ Des barrières physiques, notamment des portes et portails verrouillés. ○ La présence d'agents de sécurité sur place 24 heures sur 24. ○ Une vidéosurveillance et des systèmes d'alarme fonctionnant 24 heures sur 24, y compris la vidéosurveillance des parties communes et des points d'entrée et de sortie des locaux. ○ Des systèmes de contrôle d'accès nécessitant des données biométriques ou un badge d'identification avec photo et un code PIN pour permettre au personnel d'OpenAI d'accéder à l'ensemble des locaux d'OpenAI. ○ Protocoles d'identification, d'enregistrement et d'accompagnement des visiteurs. ○ Journalisation des entrées et sorties des locaux.
--	---

	- Des mesures relatives à la gestion des risques de sécurité liés aux tiers (y compris en ce qui concerne les sous-traitants ultérieurs), via notamment : - o Des contrats écrits visant à garantir que tout agent s'engage à mettre en place des mesures de protection raisonnables et appropriées pour protéger les données des clients. - o Des évaluations de sécurité des fournisseurs : tous les tiers sont soumis à un processus formel d'évaluation des fournisseurs géré par l'équipe de sécurité d'OpenAI. - Un plan de réponse aux incidents de sécurité destiné à résoudre les événements compromettant la confidentialité, la disponibilité ou l'intégrité des services ou des données client. - Des évaluations de sécurité, à travers notamment des tests réguliers de sécurité et de vulnérabilité afin d'évaluer si les contrôles clés sont correctement mis en œuvre et s'ils sont efficaces au regard des normes de sécurité du secteur et afin de garantir le respect continu des obligations imposées par la loi, la réglementation ou le contrat. OpenAI précise que ces mesures de sécurité peuvent être mises à jour. OpenAI indique par ailleurs disposer des certifications ISO/IEC 27001:2022 (sécurité de l'information) et ISO/IEC 27701:2019 (protection de la vie privée) pour les systèmes de management supportant l'API OpenAI, ChatGPT Enterprise et ChatGPT Edu, des certifications ISO/IEC 27017 et 27018 (services cloud), d'un système de management de l'IA certifié ISO/IEC 42001:2023, ainsi que de rapports d'audit SOC 2 Type 2 couvrant la sécurité, la disponibilité, la confidentialité et la protection de la vie privée. Les attestations correspondantes sont accessibles via le portail de confiance d'OpenAI (https://trust.openai.com). Des informations complémentaires relatives aux mesures de sécurité d'OpenAI sont disponibles à l'adresse suivante [disponible en anglais] : https://cdn.openai.com/osa/security-measures.pdf OpenAI prévoit également une procédure permettant la réalisation d'audits sous conditions (point 2.8. de son DPA). S'agissant des garanties en cas de transferts internationaux de Données Personnelles, le DPA d'OpenAI indique notamment que (point 4 de son DPA) : - Lorsque les données traitées par OpenAI dans le cadre du DPA d'OpenAI relèvent du champ d'application des Lois sur la protection des données de l'Espace économique européen ou de la Suisse (« Données de l'EEE et de la Suisse »), indépendamment de la Partie contractante d'OpenAI en vertu du DPA d'OpenAI, OpenAI Ireland Limited traite toutes les données de l'EEE et de la Suisse en conformité avec le DPA d'OpenAI et, dans la mesure où OpenAI Ireland limited transfère des données de l'EEE et de la Suisse à d'autres affiliés d'OpenAI ou à des tiers en dehors de l'Espace économique européen ou de la Suisse pour fournir les services, elle le fera sur la base d'accords contenant des clauses contractuelles types (« CCT » faisant
--	--

	référence aux clauses contractuelles types pour le transfert de données personnelles vers des pays tiers adoptées par la Commission européenne le 4 juin 2021 telles que modifiées, mises à jour ou remplacées au fil du temps) qui garantissent la mise en place de garanties appropriées pour la protection des données ou d'une décision d'adéquation émise par la Commission européenne en vertu de l'article 45 du RGPD. - Lorsque les données traitées par OpenAI dans le cadre du DPA d'OpenAI relèvent du champ d'application des Lois sur la protection des données du Royaume-Uni (« UK Data » ou « Données du Royaume-Uni »), indépendamment de la Partie contractante d'OpenAI en vertu du DPA d'OpenAI, OpenAI OpCo, LLC traite toutes les Données du Royaume-Uni en conformité avec le DPA d'OpenAI et avec les CCT telles que modifiées par l'Addendum du Royaume-Uni (Addendum du Royaume-Uni aux CCT de l'UE publié par le Commissaire à l'information en vertu de l'article 119A(1) du Data Protection Act de 2018) qui sont réputées conclues (et intégrées audit DPA). Le DPA d'OpenAI applicable est reproduit intégralement à la suite de la présente fiche (voir 2.1.2.) afin de permettre au Client de prendre connaissance de manière plus exhaustive des engagements contractuels et mesures qu'OpenAI déclare mettre en œuvre. Les garanties décrites dans la présente fiche correspondent aux engagements et déclarations contractuels d'OpenAI. Enfin, OpenAI peut lui-même recourir à des Sous-traitants ultérieurs afin de l'assister dans la fourniture de la Solution IA ChatGPT. La liste de ses Sous-traitants ultérieurs est mise à disposition par OpenAI au point 6 de son DPA (https://platform.openai.com/subprocessors).
--	---

2.1.2. Contrat conclu avec OpenAI

Le « Data Processing Addendum » (DPA) d'OpenAI complète la fiche de présentation synthétique ci-dessus (2.1.1.)

Les désignations et qualifications employées dans ce DPA doivent être lues conformément aux règles d'interprétation prévues à l'article 1 de la présente Annexe et ne modifient pas la répartition des rôles convenue entre le Client et MISTER IA dans le présent Accord.

Version du DPA d'OpenAI jointe en date du 1^{er} janvier 2026 : <https://cdn.openai.com/pdf/openai-data-processing-addendum.pdf>

III. LISTE DES AUTRES SOUS-TRAITANTS ULTÉRIEURS

Sous-traitants ultérieurs	Adresse	Contact	Outil concerné	Description du Traitement confié
N8n	Novalisstr. 10 10115 Berlin Germany	help@n8n.io	n8n cloud	Workflows d'activation de licences véhiculant les identités et e-mails des utilisateurs confiés
Supabase	65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513	privacy@supabase.com security@supabase.com legal@supabase.com	Supabase cloud	Suivi des licences
Microsoft 365	One Microsoft Way, Redmond, WA, 98052-6399	https://support.microsoft.com/fr-fr/contactus	Outlook cloud	Boîte support