

ACCORD DE SOUS-TRAITANCE RGPD

Version en vigueur au 12 février 2026 – v4.0

Article 1. Définitions

« **Accord** » : désigne le présent document et constitue l'accord de sous-traitance RGPD référencé dans le Contrat ;

« **Client** » : désigne la société ayant souscrit à des Prestations auprès du Prestataire ;

« **Contrat** » : désigne le contrat conclu entre les Parties encadrant les Prestations que le Prestataire réalise pour le Client ;

« **Données à caractère personnel** » : désigne toute information se rapportant à une personne physique identifiée ou identifiable au sens de la Réglementation applicable ;

« **Prestataire** » : désigne la société ayant émis une offre commerciale portant sur des Prestations et auprès de laquelle le Client a commandé les Prestations ;

« **Prestations** » : désigne l'ensemble des tâches confiées par le Client au Prestataire telles que définies au Contrat et qui incluent des opérations de traitement de Données à caractère personnel pour lesquelles le Client a la qualité de Responsable de traitement et le Prestataire la qualité de Sous-traitant ;

« **Réglementation applicable** » : désigne la réglementation en vigueur applicable au traitement de Données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;

« **Responsable de traitement** » : désigne 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 ;

« **Sous-traitant** » : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel pour le compte du Responsable de traitement ;

Article 2. Objet

Le présent Accord a pour objet de définir les conditions dans lesquelles le Prestataire, en sa qualité de Sous-traitant, s'engage à effectuer pour le compte de son Client, en sa qualité de Responsable de traitement, les opérations de traitement de Données à caractère personnel liées aux Prestations.

Article 3. Description du traitement faisant l'objet de la sous-traitance

Le Sous-traitant est autorisé à agir selon les instructions du Responsable de traitement et à traiter les Données à caractère personnel du Responsable de traitement dans la mesure nécessaire à la fourniture des Prestations.

Les modalités de traitement sont décrites en **Annexe A** du présent Accord.

Article 4. Durée de l'Accord

Le présent Accord entre en vigueur pour la durée des Prestations et expire à l'arrivée au terme pour laquelle que raison que ce soit du Contrat.

Article 5. Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à (i) respecter la Réglementation applicable, (ii) fournir au Sous-traitant les Données à caractère personnel concernées, (iii) documenter par écrit toute instruction concernant le traitement des Données à caractère personnel par le Sous-traitant, (iv) veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par la Réglementation applicable de la part du Sous-traitant, et (v) superviser le traitement, en ce compris le fait de réaliser des audits et/ou des inspections du Sous-traitant.

Article 6. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à (i) ne traiter les Données à caractère personnel que pour les seules finalités qui font l'objet de la sous-traitance, (ii) traiter les Données à caractère personnel conformément aux instructions documentées du Responsable de traitement – si le Sous-traitant considère qu'une instruction constitue une violation de la Réglementation applicable, il en informe immédiatement le Responsable de traitement ou si le Sous-traitant est tenu de procéder à un transfert de Données à caractère personnel vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis, il doit informer le Responsable du traitement de cette obligation juridique avant ledit transfert, sauf si le droit concerné interdit une telle information, (iii) garantir la confidentialité des Données à caractère personnel traitées dans le cadre du présent Accord, (iv) veiller à ce que les personnes autorisées à traiter les Données à caractère personnel en vertu du présent Accord s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité, et reçoivent la formation nécessaire en matière de protection des Données à caractère personnel, (v) prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut, et (vi) respecter la Réglementation applicable.

Article 7. Aide du Sous-traitant au Responsable de traitement

7.1. Assistance du Sous-traitant

Le Sous-traitant fournira les informations nécessaires et assistera le Responsable de traitement en cas d'opérations de contrôle et/ou de la mise en œuvre de mesures imposées par une autorité de contrôle, dès lors que ces opérations se réfèrent aux Prestations confiées.

Dans le cas où une autorité compétente le demanderait au Sous-traitant (par exemple : dans le cadre d'une procédure de recherche d'infraction ou une procédure relative au traitement de Données à caractère personnel couvert par l'Accord), le Sous-traitant s'engage à en informer le

Responsable de traitement, dès qu'il y est autorisé. En tout état de cause, le Sous-traitant s'engage à ne fournir que les informations strictement pertinentes à la demande formulée par l'autorité compétente.

7.2. Analyse d'impact et consultation préalable

Si le Responsable de traitement lui en fait la demande, le Sous-traitant contribue, dans la mesure des Prestations qui lui ont été confiées et qui sont concernées, aux analyses d'impact relative à la protection des données décidées par le Responsable de traitement. Le Sous-traitant assistera également le Responsable de traitement si ce dernier doit consulter l'autorité de contrôle préalablement à la mise en œuvre du traitement considéré.

7.3. Droit d'information des personnes concernées

Le Responsable de traitement, au moment de la collecte des Données à caractère personnel, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de Données à caractère personnel qu'il réalise. Les Parties peuvent convenir dans certains cas que le Sous-traitant fournira cette information. Dans ce cas, les Parties conviendront de la formulation et du format de l'information avant la collecte de Données à caractère personnel.

7.4. Exercice de droits par une personne concernée

Dans le cas où une personne concernée exerce l'un de ses droits en vertu de la Réglementation applicable, le Responsable de traitement doit répondre, en son nom et pour son compte, et dans les délais prévus par la Réglementation applicable. Lorsque la demande porte sur des Données à caractère personnel faisant l'objet de la sous-traitance prévue par le présent Accord, le Sous-traitant doit aider, dans la mesure du possible, le Responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées, notamment en informant le Responsable de traitement dans les meilleurs délais lorsque la personne concernée a exercé son droit auprès du Sous-traitant.

7.5. Violation de Données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement, dans les meilleurs délais et au plus tard quarante-huit (48) heures sur les jours ouvrés, toute violation de Données à caractère personnel dont il a connaissance. Ce délai permet au Sous-traitant de mettre en place les actions correctives, même de manière provisoire, analyser la source des anomalies rencontrées et produire un pré-rapport qu'il transmet au Responsable de traitement.

Conformément à la Réglementation applicable, la notification contient au moins :

- La description de la nature de la violation de Données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de Données à caractère personnel concernés ;
- La description des conséquences probables de la violation de Données à caractère personnel ;
- La description des mesures prises ou que le Sous-traitant propose de prendre pour remédier à la violation de Données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ;

- Le nom et les coordonnées du point de contact auprès duquel des informations supplémentaires peuvent être obtenues.

La notification est réalisée par téléphone ou par e-mail, au point de contact désigné conformément à l'article 11 POINTS DE CONTACT du présent Accord. Cette notification est accompagnée de toute la documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Il est rappelé qu'en application de la Réglementation applicable, le Responsable de traitement peut devoir (i) notifier à l'autorité de contrôle compétente la violation de Données à caractère personnel, et ce dans les meilleurs délais (et, si possible, soixante-douze (72) heures au plus tard après en avoir pris connaissance) et (ii) communiquer aux personnes concernées sur l'existence de ladite violation.

Article 8. Sous-traitance

Le Sous-traitant peut faire appel à un autre sous-traitant (ci-après, le « **Sous-traitant Ulérieur** ») pour mener des activités de traitement spécifiques. Le Sous-traitant informera préalablement et par écrit le Responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'un Sous-traitant Ulérieur. Cette information devra indiquer clairement les activités de traitement sous-traitées ainsi que l'identité et les coordonnées du Sous-traitant Ulérieur. Le Responsable de traitement disposera d'un délai de quinze (15) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne pourra être effectuée que si le Responsable de traitement n'a pas émis d'objection pendant le délai convenu. En cas d'objection raisonnable et justifiée, le Sous-traitant peut proposer au Responsable de traitement un Sous-traitant Ulérieur alternatif.

A la date d'entrée en vigueur du présent Accord, le Sous-traitant peut, pour les besoins de tout ou partie des Prestations, faire appel à ses Affiliés ainsi qu'à tout sous-traitant accepté par le Responsable de traitement.

Il appartient au Sous-traitant de s'assurer que le Sous-traitant Ulérieur présente les mêmes garanties quant à la mise en œuvre de mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences de la Réglementation applicable. Si le Sous-traitant Ulérieur ne remplit pas ses obligations en matière de protection des Données à caractère personnel, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement de l'exécution par le Sous-traitant Ulérieur de ses obligations.

Article 9. Mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre toutes les mesures de sécurité qui sont à sa disposition et qui permettent d'assurer le niveau de sécurité proportionné au regard de la Réglementation applicable.

Le Sous-traitant s'engage notamment à mettre en œuvre les mesures de sécurité suivantes :

- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- Les moyens permettant de rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du

traitement. A ce titre, le Sous-traitant est autorisé à mettre en œuvre des mesures alternatives, à la condition que ces mesures continuent à assurer un niveau de sécurité équivalent à celui assuré par la mesure initiale.

Les mesures de sécurité mises en œuvre par le Sous-traitant sont décrites en **Annexe B** du présent Accord.

Le Sous-traitant s'engage à fournir au Responsable de traitement, à sa demande, toutes les informations nécessaires et notamment à démontrer que les mesures techniques et organisationnelles ont été mises en œuvre.

Article 10. Sort des Données à caractère personnel

Au terme des Prestations ou des opérations impliquant le traitement de Données à caractère personnel, le Sous-traitant s'engage, conformément au délai indiqué par le Contrat et au choix du Responsable de traitement à :

- Renvoyer toutes les Données à caractère personnel au Responsable de traitement ; ou
- Détruire toutes les Données à caractère personnel.

Article 11. Points de contact

Les Parties se communiquent l'une à l'autre les coordonnées de leur délégué à la protection des données, si elles en ont désigné un conformément à la Réglementation applicable. Les Parties s'informeront mutuellement de tout changement des coordonnées du délégué à la protection des données. Le Groupe OCl auquel appartient le Prestataire a désigné des points de contact par région. Le Client peut contacter le point de contact du Prestataire à l'adresse répertoriée dans le Contrat.

En l'absence d'une telle communication, le Sous-traitant contactera les points de contact désignés par le Client dans le cadre des Prestations.

Article 12. Registre des catégories d'activités de traitement

Chaque Partie déclare tenir par écrit un registre de traitement conforme à la Réglementation applicable. Le Sous-traitant y répertorie les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement.

Article 13. Transferts de Données à caractère personnel hors de l'Union européenne

Le Responsable de traitement autorise le Sous-traitant à procéder à des transferts de Données à caractère personnel hors de l'Union européenne ou à destination de sociétés ne relevant pas exclusivement du droit européen. Dans ce cas, le Sous-traitant y procède conformément à la Réglementation applicable. A ce titre, le Sous-traitant agit en tant que mandataire du Responsable et revêt la qualité d'« exportateur de Données à caractère personnel » tandis que le Sous-traitant Ultimeur est « importateur de Données à caractère personnel ». C'est le cas notamment lors du recours à certains Sous-traitants Ultimeurs (par exemple : Fournisseur opérant de tels transferts). Lorsque ce transfert a lieu vers un pays reconnu comme n'offrant pas un niveau suffisant de protection des Données à caractère personnel par la Commission européenne, le Sous-traitant mettra en place des garanties appropriées préalablement à ce transfert. Dans le cas où le Sous-traitant met en place

permettant de garantir un niveau de protection équivalent à la Réglementation applicable.

Article 14. Audit

Le Responsable de traitement (ou l'auditeur mandaté par lui ne concurrençant pas les activités du Sous-traitant et soumis à une stricte obligation de confidentialité) peut procéder à toute vérification qui lui paraîtrait utile pour s'assurer du respect des obligations du Sous-traitant fixées par le présent Accord.

A cette fin, le Sous-traitant met à sa disposition la documentation nécessaire aux vérifications menées pour démontrer le respect de ses obligations, permet la réalisation d'audits, y compris des inspections, par le Responsable de traitement et y contribue. Les informations du Sous-traitant seront considérées comme des informations confidentielles.

Le Responsable de traitement pourra procéder à cet audit sur le site convenu avec le Sous-traitant, sous réserve des conditions éventuellement prévues dans la relation entre le Sous-traitant et les Sous-traitants Ultimeurs (par exemple : interdiction de réaliser un audit physique) et dans la limite d'un (1) audit par an. Pour ce faire, le Responsable de traitement devra au préalable demander au Sous-traitant que ce dernier lui communique la documentation sur les traitements mis en œuvre pour le compte du Responsable de traitement. Si ceux-ci laissent apparaître l'éventualité d'un manquement aux obligations du Sous-traitant, le Responsable de traitement pourra mettre en œuvre sa faculté d'audit et en informera le Sous-traitant par écrit du démarrage de la vérification avec un délai de préavis minimum de dix (10) Jours Ouvrés avant la date effective d'audit. L'information devra indiquer (i) l'objet et le périmètre de l'audit, qui ne sauraient être plus larges que le périmètre des Prestations, et (ii) la durée de l'audit qui ne pourra pas excéder un (1) jour, et (iii) l'identité de la ou des personnes qui effectueront l'audit.

Le Responsable de traitement prend à sa charge tous les frais occasionnés par l'audit et rembourse au Sous-traitant ou au Sous-traitant Ultimeur toutes les dépenses et frais justifiés occasionnés par cet audit, y compris le temps consacré à l'audit en fonction du taux horaire moyen du personnel du Sous-traitant ou du Sous-traitant Ultimeur ayant collaboré à l'audit, dans la limite du taux horaires pratiqué entre les Parties. Les Parties peuvent au préalable convenir des conditions financières dans une Offre commerciale.

L'audit se déroulera pendant les Jours Ouvrés et aux Heures Ouvrées et ne devra en aucune façon porter atteinte au secret des affaires du Sous-traitant ou du Sous-traitant Ultimeur concerné, ni leur causer une quelconque désorganisation au-delà de la mise à disposition par le Sous-traitant ou du Sous-traitant Ultimeur des ressources humaines, logiques ou matérielles permettant la réalisation de l'audit. Le Sous-traitant devra mettre à disposition du Responsable de traitement toutes les informations nécessaires pour permettre la réalisation de l'audit. Ces informations seront couvertes par l'obligation de confidentialité.

Le Responsable de traitement mettra gratuitement à disposition du Sous-traitant le rapport d'audit produit. Dans l'hypothèse où des écarts seraient constatés durant l'audit, les Parties s'engagent à échanger et collaborer de bonne foi pour la mise en œuvre des mesures nécessaires.

ANNEXE A

DESCRIPTION DU TRAITEMENT FAISANT L'OBJET DE LA SOUS-TRAITANCE

Nature des opérations réalisées sur les Données à caractère personnel	Les opérations réalisées sur les Données à caractère personnel sont fonction des Prestations souscrites par le Client et décrites au Contrat. Dans ce cadre, les opérations réalisées peuvent être les suivantes : collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement. Les Prestations peuvent inclure des produits et des services de tiers traitant les Données à caractère personnel qui sont mis à disposition du Responsable de traitement par l'intermédiaire du Sous-traitant (distribution, achat-revente) : il peut s'agir de solutions logicielles et prestations associées et/ou de matériel. Le Responsable de traitement reconnaît et accepte que ces tiers sont ses sous-traitants directs (par exemple : éditeur ou hébergeur-tiers d'une solution, constructeur d'un matériel)
Finalité(s) du traitement	Le traitement est réalisé par le Sous-traitant pour fournir les Prestations. La finalité du traitement est définie par le Responsable de traitement.
Catégories de Données à caractère personnel traitées	Les catégories de Données à caractère personnel sont déterminées et contrôlées par le Responsable de traitement, à sa seule discrétion. Le Responsable de traitement fournit les Données à caractère personnel nécessaires au Sous-traitant dans le cadre des Prestations. Les Données à caractère personnel peuvent être les suivantes : ☒ Identité ☒ Vie personnelle ☒ Vie professionnelle ☒ Information d'ordre économique et financier ☒ Données techniques (ex : adresse IP, logs, identifiants, nature d'une problématique dès que lors que celle-ci se rapporte à de la Donnée à caractère personnel) ☒ Données de localisation
Catégories de Données à caractère personnel particulières	Conformément à l'article 9 RGPD, il est rappelé au Responsable de traitement par le Sous-traitant que certaines Données à caractère personnel ne doivent, en principe, ni être collectées ni traitées. Le Responsable de traitement devra informer le Sous-traitant si les Données à caractère personnel suivantes sont traitées dans le cadre des Prestations : ☐ Données sensibles (dont : données de santé, religion, orientation sexuelle etc.) ; ☐ Données d'infraction et/ou de condamnation ; ☐ Données biométriques.
Catégories de personnes concernées	Les catégories de personnes concernées sont déterminées et contrôlées par le Responsable de traitement.
Durée du traitement	La durée du traitement réalisé par le Sous-traitant correspond à la durée précisée à l'article 10 SORT DES DONNEES A CARACTERE PERSONNEL. Il revient à la Partie qui a la qualité de Responsable de traitement de définir les durées de conservation applicables à chaque traitement. Chaque Partie s'assure que les durées de conservation pour les autres finalités n'excèdent pas la durée nécessaire au traitement concerné (exemple : conservation dans le cadre du respect d'une obligation légale pendant la durée de ladite obligation légale).

ANNEXE B

MESURES DE SECURITE MISES EN ŒUVRE PAR LE SOUS-TRAITANT

Gouvernance	
Nomination d'un référent RGPD	Le Sous-traitant a désigné un point de contact joignable à l'adresse rappelée en Annexe A .
Formation des collaborateurs	Les collaborateurs du Sous-traitant et notamment ceux qui sont amenés à manipuler régulièrement des Données à caractère personnel ont suivi une formation dédiée à la protection des Données à caractère personnel.
Sécurisation du système d'information	Une Politique de Sécurité des Systèmes d'Information (PSSI) est définie et mise en œuvre au sein des systèmes d'information du Sous-traitant.
Veille de sécurité	Le Sous-traitant surveille en continu les menaces, vulnérabilités ou vecteurs d'attaque : - Systèmes de détection et de réponse (EDR, SOC, CERT, etc.) ; - Pare-feu et systèmes de filtrage des accès dédiés (proxy, vpn...) ; - Protection contre les attaques logicielles (WAF). Le Sous-traitant se tient informer par le biais de bulletins de veille en <i>Cyber Threat Intelligence</i> (CTI).
Sécurité des données	
Authentification des collaborateurs	Le système d'information du Sous-traitant comporte une procédure d'authentification où chaque collaborateur dispose d'un identifiant qui lui est propre. Ce dernier doit impérativement s'authentifier avant de pouvoir utiliser les outils numériques mis à sa disposition dans le cadre de l'activité du Sous-traitant. Le Sous-traitant a également limité le nombre de tentatives de connexion lors de chaque authentification sur ses outils. Le Sous-traitant applique la double authentification sur les composants compatibles de ses systèmes d'information.
Complexité des mots de passe	Les mots de passe sont composés au minimum de douze caractères parmi les chiffres, symboles, lettres et majuscules, les mots de passe les plus classiques sont interdits (par exemple login, nom, simples suites de chiffres).
Processus de récupération sécurisé	Les informations du compte sont vérifiées avant de permettre sa récupération, conformément aux bonnes pratiques de l'ANSSI.
Gestion des accès	Le Sous-traitant a mis en place une procédure de gestion des habilitations afin de limiter les accès aux données aux seuls collaborateurs qui ont un intérêt à en connaître. Le Sous-traitant a également mis en œuvre une procédure d'habilitation relative aux opérations de maintenance réalisées sur son système d'information par les tiers. La revue de ces habilitations est effectuée périodiquement. Seules quelques personnes accréditées et sensibilisées peuvent éventuellement accéder aux données dans le cas d'une défaillance liée au stockage des données.
Traçabilité des accès	Le Sous-traitant a mis en place un système de traçabilité des accès à son système d'information (journalisation des données d'accès) et des actions des utilisateurs du Sous-traitant (journalisation des actions) afin, par exemple, de détecter l'origine d'un incident sur son système d'information.
Sécurité des postes de travail	Les postes de travail des collaborateurs du Sous-traitant font l'objet de mesures techniques de sécurité qui assurent l'intégrité, la confidentialité et la disponibilité des données qui y sont stockées. Ces mesures sont notamment les suivantes : outils de détection et contrôle des menaces, chiffrement possible des postes nomades, sauvegarde des données qui y sont contenues conformément à sa politique en la matière. Les postes de travail nomades des collaborateurs du Sous-traitant sont sécurisés et l'accès à distance est effectué par un accès VPN sécurisé avec double authentification.
Chiffrement des données et des flux	Sur son système d'information, les données échangées avec et entre les systèmes sont chiffrées grâce aux protocoles TLS. Ce protocole est configuré afin de délivrer le meilleur compromis entre compatibilité et sécurité.
Sécurisation des infrastructures	
Mises à jour de sécurité	Les correctifs de sécurité sont qualifiés et appliqués automatiquement sur les composants du système d'information du Sous-traitant.
Protection des systèmes d'exploitation	Les systèmes d'exploitation sont mis à jour et renforcés.

Disponibilité des infrastructures	Toutes les données sont répliquées dans un datacenter sécurisé et situé en France. Le Sous-traitant a défini des procédures de reprise d'activité, le plus souvent automatique, en cas de défaillance détectée sur son système d'information. Dans ce cadre, les défaillances détectées provoquent une alerte grâce à un système de surveillance des composants techniques et services métier.
Sauvegarde	Le Sous-traitant a mis en place une politique de sauvegarde et de récupération des données présentes sur son système d'information.
Tests d'intrusion	Le Sous-traitant contrôle ses plateformes et son système d'information à échéances régulières afin d'assurer un niveau de sécurité adéquat.
Protection du réseau informatique interne	Le réseau filaire et/ou Wi-fi du Sous-traitant est segmenté afin d'assurer un contrôle des zones de sécurité selon les usages. Le réseau Wifi est sécurisé.
Protection des accès physiques	
Protection des locaux	L'accès aux locaux techniques du Sous-traitant est restreint par des portes sécurisées et des badges.