

CONDITIONS PARTICULIERES TRANSVERSES AU CONTRAT

Accord de sous-traitance RGPD

Version mise en ligne le 10 octobre 2022 – v2.4

I. Objet

Ces conditions particulières viennent compléter toutes les conditions générales que les Parties ont conclues et qui sont encore en vigueur.

Les présentes clauses (ci-après l'« **Accord** ») ont pour objet de définir les conditions dans lesquelles le Prestataire, en sa qualité de Sous-traitant, s'engage à effectuer pour le compte du Client, en tant que Responsable de traitement, les opérations de traitement de Données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter 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 applicable à compter du 25 mai 2018 (ci-après, la « **Réglementation applicable** »).

II. Définitions

Les termes portant une majuscule au(x) Contrat(s) et réutilisés au sein du présent Accord ont la même signification que celle qui leur est donnée au(x) Contrat(s).

Pour rappel, « **Affilié** » : désigne toute société du groupe OCI, étant entendu que l'on entend par groupe toute société qui contrôle de manière directe ou indirecte l'entité signataire ou qui est contrôlée de manière directe ou indirecte par l'entité signataire ou qui est sous le contrôle d'une même société que l'entité signataire.

Les termes portant une majuscule et réutilisés au sein du présent Accord qui n'auront pas été définis au(x) Contrat(s) auront la même signification que celle qui leur est donnée dans la Réglementation applicable.

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

Le Sous-traitant est autorisé à agir selon les instructions du Responsable de traitement, à traiter les Données à caractère personnel du Responsable de traitement dans la mesure nécessaire à la fourniture des prestations qui sont définies dans le(s) Bon(s) de commande / Offre(s) commerciale(s) conclu(s) entre le Sous-traitant et le Responsable de traitement.

Les modalités de traitement sont décrites en **Annexe 1** du présent Accord de sous-traitance RGPD.

IV. Durée de l'Accord

Le présent Accord de sous-traitance entre en vigueur à la date de dernière signature par les Parties et expire à l'arrivée au terme pour laquelle raison que ce soit du/des Bon(s) de commande / Offre(s) commerciale(s).

V. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le Sous-traitant s'engage à :

1. Traiter les Données à caractère personnel **uniquement pour la ou les seule(s) finalité(s)** qui fait/ont l'objet de la sous-traitance ;
2. 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. En outre, 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'Etat 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 pour des motifs importants d'intérêt public ;
3. **Garantir la confidentialité** des Données à caractère personnel traitées dans le cadre du présent Accord ;
4. Veiller à ce que les **personnes autorisées à traiter les Données à caractère personnel** en vertu du présent Accord :
 - a. S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
 - b. Reçoivent la formation nécessaire en matière de protection des Données à caractère personnel.
5. 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**.

VI. Sous-traitance

Le Sous-traitant peut faire appel à un autre sous-traitant ultérieur (ci-après, le « **Sous-traitant** »).

Ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-traitant Ultérieur et les dates de l'accord de sous-traitance. Le Responsable de traitement dispose d'un délai maximum de quinze (15) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut 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 Prestataire peut proposer au Responsable de traitement un Sous-traitant Ultérieur alternatif.

A la date de signature du présent Accord, le Sous-traitant peut faire appel :

- Aux Sous-traitants Ultérieurs et qui sont considérés comme acceptés par le Responsable de traitement ;
- A ses Affiliés pour tout ou partie des Prestations ;
- A tous Sous-traitants Ultérieurs mentionnés sur une offre commerciale du Sous-traitant et / ou au contrat commercial (ex : éditeur).

Le Sous-traitant Ultérieur est tenu de respecter les obligations du présent Accord pour le compte et selon les instructions du Responsable de traitement. Il appartient au Sous-traitant de s'assurer que le Sous-traitant Ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la Réglementation applicable. Si le Sous-traitant Ultérieur ne remplit pas ses obligations en matière de protection des données, le Sous-traitant demeure pleinement responsable devant le Responsable de traitement de l'exécution par le Sous-traitant Ultérieur de ses obligations.

VII. 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. Lorsque cela est applicable, la formulation et le format de l'information doivent être convenus avec le Responsable de traitement avant la collecte de Données à caractère personnel.

VIII. Exercice des droits des personnes

Dans la mesure du possible, le Sous-traitant doit aider le Responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Le Responsable de traitement doit répondre, en son nom et pour son compte, et dans les délais prévus par la Réglementation applicable aux demandes des

personnes concernées en cas d'exercice de leurs droits, s'agissant des Données à caractère personnel faisant l'objet de la sous-traitance prévue par le présent Accord.

Lors de l'exercice des droits des personnes, le Sous-traitant informe dans les meilleurs délais le Responsable de traitement de la demande exercée.

IX. Notification des violations de Données à caractère personnel

Le Sous-traitant notifie au Responsable de traitement toute violation de Données à caractère personnel dans les meilleurs délais et au plus tard quarante-huit (48) heures sur les jours ouvrés après avoir pris connaissance de la violation et par les moyens suivants :

- Par téléphone, auprès des contacts privilégiés définis par les Parties, pour information complète des symptômes.
- Confirmé par e-mail à l'adresse e-mail du DPO du Responsable de traitement.

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 transmis au Responsable de traitement.

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 ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de Données à caractère personnel ;
- La description des mesures prises ou que le Responsable de traitement peut proposer 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.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

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.

Le Responsable de traitement notifie à l'autorité de contrôle compétente (la CNIL) les violations de Données à caractère personnel dans les meilleurs

délais et, si possible, 72 heures au plus tard après en avoir pris connaissance.

Il est rappelé au Responsable de traitement ses obligations quant à son devoir de communication auprès des personnes concernées conformément à l'article 34 RGPD.

X. Aide du Sous-traitant dans le cadre du respect par le Responsable de traitement de ses obligations

Sur le périmètre des Prestations qui lui a été confié, le Sous-traitant aide le Responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le Sous-traitant aide le Responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

Le Sous-traitant garantit l'information (et son assistance) au Responsable de traitement concernant des opérations de contrôle et des mesures de l'autorité de contrôle, dès lors qu'elles se réfèrent aux Prestations confiées. Il en est de même lorsqu'une autorité compétente sollicite des informations de la part du Sous-traitant, par exemple dans le cadre d'une procédure d'infraction ou d'une procédure pénale relative au traitement de Données à caractère personnel lors de la sous-traitance.

XI. 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.

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.

Ces éléments de preuve doivent permettre au Responsable de traitement de vérifier la conformité du Sous-traitant vis-à-vis des exigences de la

Réglementation applicable et que la protection des droits de la personne concernée est garantie.

XII. Sort des Données à caractère personnel

Au terme des services impliquant le traitement de Données à caractère personnel, et éventuellement afin d'assurer le délai prévu de la phase de réversibilité, le Sous-traitant s'engage, conformément au délai indiqué par le Bon de commande / Offre commerciale, ou éventuellement, selon les modalités convenues entre les parties à :

- Renvoyer toutes les Données à caractère personnel au Responsable de traitement sous un format sécurisé ;
- Détruire toutes les Données à caractère personnel.

XIII. Délégué à la protection des données

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 l'article 37 RGPD.

XIV. Registre des catégories d'activités de traitement

Le Sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement comprenant :

- Le nom et les coordonnées du Responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du Responsable du traitement ;
- Le cas échéant, les transferts de Données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49 §1 al. 2 RGPD, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres :
 - o Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - o Des 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 ;
 - o Une procédure visant à tester, à analyser et à évaluer

régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;

- 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.

XV. Transfert de Données à caractère personnel hors de l'Union Européenne

Le Sous-traitant s'engage à ce que pendant toute la durée de l'Accord les Données à caractère personnel soient traitées et en particulier hébergées au sein de l'Union Européenne, directement par ses soins ou en ayant recours à des sociétés relevant exclusivement du droit européen.

Sauf consentement préalable et écrit du Responsable de traitement, le Sous-traitant s'interdit tout transfert de Données à caractère personnel hors de l'Union Européenne ou à destination de sociétés ne relevant pas exclusivement du droit européen.

Dans le cas où le Sous-traitant est autorisé à procéder au transfert de Données à caractère personnel hors de l'Union Européenne, notamment dans le cadre du recours à un Sous-traitant Ulérieur et/ou à des logiciels de visioconférence, partage de fichiers, travail collaboratif et autres opérant de tels transferts, et que 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 aura l'obligation – préalablement à tout transfert – de formaliser :

- Une convention de transfert conforme aux clauses contractuelles types émises par la Commission Européenne ou aux codes de conduite prévus aux articles 46 §2 c), d) et e) RGPD, ou tout autre document équivalent qui viendrait à les remplacer, entre le Sous-traitant, agissant en qualité de mandataire du Responsable de traitement, et d'« **Exportateur de Données à caractère personnel** » et le Sous-traitant Ulérieur, qualifié d'« **Importateur de Données à caractère personnel** » ; et
- Un accord avec le Sous-traitant Ulérieur, mettant à la charge du celui-ci des obligations au moins égales à celles auxquelles s'engage le Sous-traitant aux termes du présent Accord.

XVI. Droit d'audit

Le Responsable de traitement ou tout auditeur mandaté par lui ne concurrençant pas les activités commerciales du Sous-traitant, pourra procéder à toute vérification qui lui paraîtrait utile pour s'assurer du respect des obligations fixées par le présent Accord.

Le Responsable de traitement pourra procéder à cet audit sur le site convenu avec le Sous-traitant dans les conditions prévues dans les relations entre le Sous-traitant et les Sous-traitants Ulérieurs (ex. interdiction de réaliser un audit physique) et dans la limite d'un (1) audit par an et uniquement après avoir fait une demande écrite de communication de documentation sur les traitements mis en œuvre pour le compte du Responsable de traitement et si ceux-ci laissent apparaître l'éventualité d'un manquement aux obligations du Sous-traitant.

Pour mettre en œuvre un tel audit, le Responsable de traitement s'engage à informer par écrit le Sous-traitant du démarrage de la vérification avec un délai de préavis minimum de dix (10) jours ouvrés avant la date effective d'audit, en lui indiquant :

- L'objet et le périmètre de l'audit qui ne sauraient être plus larges que ce qui est couvert par le présent Accord définissant la relation contractuelle des parties ;
- La durée de l'audit ne pourra pas excéder deux (2) jours ;
- 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 Ulérieur 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 Ulérieur ayant collaboré à l'audit et dans la limite du taux horaires pratiqué entre les parties.

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.

L'audit se déroulera pendant les jours ouvrés et aux heures de travail du Sous-traitant ou du Sous-traitant Ulérieur concerné, et ne devra en aucune façon porter atteinte au secret des affaires du Sous-traitant ni lui causer une quelconque désorganisation au-delà de la mise à disposition par le Sous-traitant ou du Sous-traitant Ulérieur des ressources humaines, logiques ou matérielles permettant la réalisation de l'audit.

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.

XVII. Documentation

Le Sous-traitant met à la disposition du Responsable de traitement **la documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le Responsable de traitement ou un

autre auditeur qu'il a mandaté, et contribuer à ces audits.

XVIII. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le Responsable de traitement s'engage à :

1. Fournir au Sous-traitant les Données à caractère personnel visées au présent Accord ;
2. Documenter par écrit toute instruction concernant le traitement des Données à caractère personnel par le Sous-traitant ;
3. 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 ;
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.

ANNEXE 1

La présente Annexe a pour objectif de décrire les traitements qui vont être réalisés dans le cadre de l'exécution du présent Accord.

I. DESCRIPTION DU (DES) TRAITEMENT(S)

Eu égard à l'article III « *Description du traitement faisant l'objet de la sous-traitance* » du présent Accord, les modalités de traitement se présentent de la manière suivante :

Nature des opérations réalisées sur les Données à caractère personnel	Fonction des Prestations souscrites par le Responsable de traitement sur tout ou partie des solutions dans le domaine de l'informatique et des télécom proposées par le Sous-traitant. Il est précisé que pour toute prestation réalisée par un tiers et pour laquelle le Prestataire n'intervient que dans la mise à disposition (ex : fourniture d'un équipement, d'une solution etc.), le Responsable de traitement est en lien direct avec le tiers. Par exemple, en cas de mise à disposition de licences pour une solution par le Prestataire, le Responsable de traitement est, pour l'utilisation voire pour le support, en lien direct avec l'éditeur de ladite solution qui intervient en tant que Sous-traitant. A titre de clarification, le présent Accord entre les Parties ne couvre alors, outre les autres Prestations, que le traitement relatif à la mise à disposition entre le Responsable de traitement et le Sous-traitant.
Finalité(s) du traitement	Fourniture des Prestations prévues au(x) Bons de commande / Offres commerciales.

	Si le traitement effectué par le Responsable de traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, le Responsable de traitement doit choisir les Prestations qu'il confie avec précaution. Lors de l'évaluation du risque, il est notamment tenu compte des critères suivants, sans toutefois s'y limiter : évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques ; prise de décision automatisée ayant des effets juridiques ou pouvant affecter de manière significative la personne concernée ; suivi systématique des personnes concernées ; traitement de catégories particulières de données ou de données sensibles ; traitement à grande échelle ; croisement de données ; combinaison de données ; traitement de données concernant des personnes vulnérables ; utilisation de nouvelles technologies innovantes méconnues du public pour le traitement. En sus de la fourniture des Prestations, le Sous-traitant est autorisé à conserver les Données à caractère personnel, notamment à des fins statistiques (dans la mesure où celles-ci contiennent des Données à caractère personnel), commerciales, marketing, publicitaires et de développement interne (dans la mesure où ce dernier contiendrait de la Donnée à caractère personnel), et dans le cadre du respect des obligations légales auxquelles le Sous-traitant est soumis.
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. Dans le cadre de la réalisation des Prestations, le Sous-traitant a besoin de certaines informations, ce que le Responsable de traitement prend en compte et accepte de fournir. Ces informations sont en principe les suivantes : - Nom ; - Prénom ; - Fonction ; - Adresse e-mail ; - Fax ; - Numéro de téléphone (fixe ou mobile) ; - Adresse professionnelle ; - Adresse IP, et données techniques de manière générale (ex : logs,

	identifiants, nature d'une problématique dès que lors que celle-ci se rapporte à de la donnée à caractère personnel) Ainsi que celles qui seraient nécessaires à la fourniture des Prestations.
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 ne doivent, en principe, pas être collectées ni traitées (cf. le site de la CNIL pour obtenir des informations complémentaires). Données particulières traitées par le Sous-traitant : - Donnée sensible (ex : données de santé, données de religion, données sur l'orientation sexuelle etc.) : aucune - Infractions, condamnations : aucune
Catégories de personnes concernées	Les catégories de personnes concernées sont déterminées et contrôlées par le Responsable de traitement.
Durée du traitement	Durée de la fourniture des Prestations souscrites par le Responsable de traitement auprès du Sous-traitant, augmentée de la durée précisée à l'article XII « <i>Sort des Données à caractère personnel</i> ». 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 durant laquelle le Sous-traitant est soumis à ladite obligation légale).

II. SOUS-TRAITANCE ULTERIEURE

Le cas échéant, les Parties peuvent convenir que des Sous-traitants Ultérieurs (autres que ceux évoqués à l'article VI « *Sous-traitance* ») suivants peuvent intervenir.

Au cours de l'exécution du présent Accord, les Parties pourront compléter la liste par échanges simples entre elles et / ou par voie d'avenant.

III. POINTS DE CONTACT RGPD

Chaque Partie a désigné un référent RGPD au sein de sa structure.

Le référent RGPD du Sous-traitant peut être contacté à l'adresse suivante : dpoci@oci.fr

Les Parties s'engagent à communiquer immédiatement et par écrit à l'autre tout changement concernant l'identité ou les coordonnées de ses référents RGPD.