

# Accord de sous-traitance WIMOVA for Business

## 1. Préambule

Cet accord de sous-traitance définit les droits et obligations du Client (ci-après le « **Responsable de Traitement** ») et de WIMOVA (ci-après le « **Sous-traitant** ») lorsque WIMOVA traite des données à caractère personnel pour le compte du Client.

L'accord de sous-traitance a été élaboré pour s'assurer du respect par les Parties de l'article 28(3) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (le « **RGPD** »).

Dans le cadre de la fourniture de son service **WIMOVA for Business**, le Sous-traitant traitera certaines données à caractère personnel pour le compte du Responsable de Traitement conformément aux stipulations convenues dans cet accord.

L'accord de sous-traitance a primauté sur toute autre stipulations similaires contenues dans d'autres accords conclus entre les Parties.

Trois sections sont jointes à ce document et font partie intégrante de l'accord de sous-traitance :

- La **Section A** qui contient des informations détaillées sur le traitement de données à caractère personnel sur lequel WIMOVA intervient en tant que sous-traitant, notamment la finalité et la nature de ce traitement, le type de données à caractère personnel, les catégories de personnes concernées et la durée du traitement.
- La **Section B** qui contient les règles imposées par le Responsable du Traitement autorisant le Sous-traitant à recourir à des sous-traitants ultérieurs ainsi que la liste des sous-traitants ultérieurs autorisés par le Responsable de Traitement.
- La **Section C** qui contient les mesures de sécurité minimales à mettre en œuvre par le Sous-traitant.

L'accord de sous-traitance ne s'applique pas aux traitements de données à caractère personnel réalisés par WIMOVA en tant que responsable de traitement (tels que les traitements décrits dans sa *Politique de confidentialité Clients* et *Politique de confidentialité Passagers*) et pour lesquels WIMOVA demeure seul responsable vis-à-vis des personnes concernées et de l'autorité de contrôle.

## 2. Les droits et obligations du Responsable de Traitement

Le Responsable de Traitement est chargé de veiller à ce que son traitement de données à caractère personnel soit conforme au RGPD (conformément à l'article 24 du RGPD), aux dispositions applicables au sein de l'UE ou des Etats membres en matière de protection des données à caractère personnel ainsi qu'aux stipulations de l'accord de sous-traitance.

Le Responsable de Traitement a le droit et le devoir de prendre des décisions sur les finalités et les moyens du traitement de données à caractère personnel.

Le Responsable de Traitement est notamment chargé de veiller à ce que le traitement de données à caractère personnel que le Sous-traitant est chargé d'effectuer, dispose d'une base légale.

## 3. Le Sous-traitant doit agir sur instructions

Le Sous-traitant traite les données à caractère personnel uniquement sur instructions documentées du Responsable de Traitement, à moins que le droit de l'Union européenne ou de l'Etat Membre auquel le Sous-traitant est soumis ne l'exige. Ces instructions sont précisées en **Section A**.

Des instructions ultérieures peuvent également être données par le Responsable de Traitement pendant toute la durée du traitement des données à caractère personnel, mais ces instructions doivent toujours être documentées, transmises et conservées par écrit, y compris sous forme électronique.

Le Sous-traitant informe immédiatement le Responsable de Traitement si les instructions données par le Responsable de Traitement contreviennent au RGPD ou au droit de l'Union européenne ou au droit de l'Etat membre applicable en matière de protection des données à caractère personnel.

#### 4. Confidentialité

Le Sous-traitant n'accorde l'accès aux données à caractère personnel traitées au nom du Responsable de Traitement qu'aux personnes placées sous son autorité et qui se sont engagées à respecter un engagement de confidentialité ou qui sont soumises à une obligation légale de confidentialité appropriée et uniquement lorsqu'elles ont besoin de connaître le contenu desdites données.

La liste des personnes à qui l'accès a été accordé fait l'objet d'un réexamen périodique. Sur la base de ce réexamen, cet accès aux données à caractère personnel peut être retiré s'il n'est plus nécessaire, et les données à caractère personnel ne sont alors plus accessibles à ces personnes.

#### 5. Sécurité du traitement

Compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de l'étendue, du contexte et des finalités du traitement ainsi que du risque de probabilité et de gravité variables pour les droits et libertés des personnes physiques, le Responsable de Traitement et le Sous-traitant mettent en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque.

Le Responsable de Traitement évalue les risques pour les droits et libertés des personnes physiques inhérents au traitement et met en œuvre des mesures pour atténuer ces risques.

Les mesures techniques et organisationnelles mises en œuvre par le Sous-traitant sont spécifiées en **Section C**.

#### 6. Sous-traitants ultérieurs

Le Sous-traitant doit satisfaire aux exigences spécifiées à l'article 28, paragraphes 2 et 4 du RGPD pour pouvoir engager un autre sous-traitant (ci-après désigné "**sous-traitant ultérieur**").

Le Sous-traitant a l'autorisation générale du Responsable de Traitement pour engager des sous-traitants ultérieurs, c'est-à-dire que le Sous-traitant informe par écrit le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement de sous-traitants ultérieurs au moins quinze (15) jours à l'avance, donnant ainsi au responsable du traitement la possibilité de s'opposer à ces changements avant d'engager le(s) sous-traitant(s) ultérieur(s) concerné(s).

La liste des sous-traitants ultérieurs déjà autorisés par le responsable du traitement figure en **Section B**.

Lorsque le Sous-traitant engage un sous-traitant ultérieur pour effectuer des activités de traitement spécifiques pour le compte du Responsable de Traitement, les mêmes obligations en matière de protection des données que celles énoncées dans le présent accord de sous-traitance s'imposent à ce sous-traitant ultérieur par le biais d'un contrat ou d'un autre acte juridique en vertu du droit de l'Union Européenne ou d'un Etat membre, et doit notamment garantir la mise en œuvre de mesures techniques et organisationnelles appropriées de telle sorte que le traitement réponde aux exigences du présent accord de sous-traitance et du RGPD.

Il incombe donc au Sous-traitant d'exiger que le sous-traitant ultérieur respecte *a minima* des obligations similaires auxquelles le Sous-traitant est soumis en vertu du présent accord de sous-traitance et du RGPD.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Sous-traitant reste responsable envers le responsable du traitement en ce qui concerne le respect des obligations du sous-traitant ultérieur.

## 7. Transfert de données vers des pays tiers ou des organisations internationales

Tout transfert de données à caractère personnel vers des pays tiers ou vers des organisations internationales par le Sous-traitant ne doit avoir lieu que sur la base d'instructions documentées du Responsable de Traitement et doit toujours se faire conformément au chapitre V du RGPD.

L'existence d'un transfert de données vers des pays tiers ou vers des organisations internationales et l'outil de transfert prévu au chapitre V du RGPD sur lequel il se fonde sont indiqués en **Section B**.

## 8. Assistance apportée au Responsable de Traitement

En prenant en considération la nature du traitement couvert par l'accord de sous-traitance, le Sous-traitant assiste le Responsable de Traitement par des mesures techniques et organisationnelles appropriées, et pour autant que cela soit possible, dans l'accomplissement des obligations du Responsable de Traitement de répondre aux demandes d'exercice des droits des personnes concernées tel que prévu au chapitre III du RGPD.

En outre, compte tenu de la nature du traitement et des informations dont il dispose, le Sous-traitant assiste le Responsable de Traitement pour s'assurer le respect des règles suivantes :

- a. l'obligation pour le Responsable de Traitement de notifier une violation de sécurité à l'autorité de contrôle compétente, conformément à l'article 33 du RGPD ;
- b. l'obligation pour le Responsable de Traitement de communiquer une violation de sécurité aux personnes concernées, conformément à l'article 34 du RGPD ;
- c. l'obligation du Responsable de Traitement de procéder à une évaluation de l'impact des traitements envisagés sur la protection des données à caractère personnel (ci-après « AIPD »), conformément à l'article 35 du RGPD ;
- d. l'obligation du Responsable de Traitement de consulter l'autorité de contrôle compétente avant de procéder au traitement lorsqu'une AIPD conclue que le traitement envisagé entraînerait un risque élevé en l'absence de mesures prises par le Responsable de Traitement pour atténuer le risque conformément à l'article 36 du RGPD.

## 9. Notification d'une violation de données à caractère personnel

En cas de violation de données à caractère personnel, le Sous-traitant doit, sans délai indu après en avoir eu connaissance, notifier le Responsable de Traitement de cette violation.

La notification du Sous-traitant au Responsable de Traitement doit, si possible, avoir lieu dans les quarante-huit (48) heures suivant la date à laquelle le Sous-traitant a eu connaissance de la violation des données à caractère personnel afin de permettre au Responsable de Traitement de respecter l'obligation qui lui incombe de notifier la violation à l'autorité de contrôle compétente.

Le Sous-traitant assiste le Responsable de Traitement pour notifier la violation des données à caractère personnel à l'autorité de contrôle compétente, ce qui signifie que le Sous-traitant est tenu d'aider le Responsable de Traitement à obtenir les informations devant être fournies à l'autorité de contrôle compétente conformément à l'article 33 (3) du RGPD et qui sont énumérées ci-dessous :

- a. La nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de données à caractère personnel concernés ;
- b. Les conséquences probables de la violation des données à caractère personnel ;
- c. Les mesures prises ou proposées par le Responsable de Traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures visant à atténuer ses potentiels effets négatifs.

## **10. Effacement et restitution des données**

A la fin de la fourniture des prestations de services, le Sous-traitant est tenu de supprimer toutes les données à caractère personnel traitées pour le compte du Responsable de Traitement.

## **11. Audit et inspection**

Le Sous-traitant met à disposition du Responsable de Traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD, dans le présent accord de sous-traitance et autorise et participe aux audits, y compris les inspections, conduits par le Responsable de Traitement ou par un autre auditeur mandaté par le Responsable de Traitement.

Le Responsable de Traitement informe le Sous-traitant de la réalisation d'un audit quinze (15) jours avant la date prévue pour sa réalisation, en précisant, le cas échéant, le tiers auditeur mandaté pour cet audit. Le Sous-traitant peut formuler toutes réserves objectives à l'encontre du tiers auditeur mandaté (notamment si ce dernier est un concurrent).

En tout état de cause, tout audit ne peut être réalisé qu'après la signature d'un accord de confidentialité entre le Sous-traitant et le tiers auditeur.

Le Sous-traitant est tenu de fournir aux autorités de contrôle et leurs représentants qui, conformément à la législation applicable peuvent accéder aux locaux, un accès aux installations physiques du Sous-traitant sur présentation préalable de leur qualité.

## **12. Points de contact du Responsable de Traitement et du Sous-traitant**

Les Parties peuvent se contacter en utilisant les coordonnées des points de contact indiqués en **Section A**. Les Parties sont tenues de s'informer en permanence des modifications apportées à leur point de contact.

## **13. Durée de l'accord de sous-traitance**

L'accord de sous-traitance s'applique pour toute la durée de fourniture des prestations de services WIMOVA for Business par le Sous-traitant.

Pendant la durée des prestations de services WIMOVA for Business, l'accord de sous-traitance ne peut pas être résilié à moins qu'un autre accord de sous-traitance régissant la fourniture des prestations de services WIMOVA for Business ait été convenu entre les Parties. Les Parties sont autorisées à solliciter une renégociation de l'accord de sous-traitance si des changements de législation ou des changements de situation s'appliquent.

Si la fourniture des prestations de services WIMOVA for Business cesse et que les données à caractère personnel ont été détruites ou retournées au Responsable de Traitement, l'accord de sous-traitance peut être résilié par notification écrite de l'une ou l'autre des Parties.

## Section A. Informations concernant le traitement

### A.1. Traitement des données à caractère personnel

Le traitement faisant l'objet de la sous-traitance est le suivant :

<b>Finalités du traitement :</b>	<ul style="list-style-type: none"><li>▪ Gestion de la liste des collaborateurs du Responsable de Traitement autorisés à utiliser les services de transport de WIMOVA for Business.</li><li>▪ Gestion de la liste des collaborateurs du Responsable de Traitement autorisés à accéder au Back-Office de la plateforme WIMOVA for Business.</li><li>▪ Gestion des rôles, droits et privilèges attribués par le Responsable de Traitement à ses collaborateurs (Administrateur, Gestionnaire, Passager) sur la plateforme WIMOVA for Business.</li><li>▪ Gestion des centres de coûts du Responsable de Traitement sur la plateforme WIMOVA for Business.</li><li>▪ Gestion des politiques de voyage du Responsable de Traitement sur la plateforme WIMOVA for Business.</li></ul>
<b>Nature du traitement :</b>	<ul style="list-style-type: none"><li>▪ Collecte ou importation des données, organisation et structuration des données, enregistrement et conservation des données, mise à jour, modification et adaptation des données saisies ou transmises par le Responsable de Traitement sur la plateforme WIMOVA for Business.</li><li>▪ Consultation des données en cas de nécessité de maintenance ou de support technique.</li><li>▪ Consultation, duplication, modification, adaptation, extraction, transfert, effacement ou destruction des données dans le cadre des instructions générales du Responsable de Traitement ou dans le cadre de demandes spécifiques adressées par le Responsable de Traitement.</li></ul>
<b>Catégories de données à caractère personnel :</b>	<ul style="list-style-type: none"><li>▪ <b>Données d'identité :</b> Nom, prénom du collaborateur</li><li>▪ <b>Coordonnées professionnelles :</b> Courriel, numéro de téléphone du collaborateur</li><li>▪ <b>Fonctions professionnelles :</b> fonction occupée, société et centre(s) de coûts auxquels le collaborateur est rattaché</li><li>▪ <b>Groupe :</b> nom et description du groupe sur la plateforme WIMOVA for Business, groupe(s) au(x)quel(s) le collaborateur est rattaché</li><li>▪ <b>Rôle attribué au collaborateur (déterminant ses droits et privilèges) :</b> Administrateur du Back-Office WIMOVA for Business, Gestionnaire du Back-Office WIMOVA for Business, Passager uniquement de l'application Rider (WIMOVA for Business)</li><li>▪ <b>Activation/désactivation du collaborateur sur la plateforme WIMOVA for Business :</b> statut d'invitation (envoyée/acceptée), statut du compte (activé, désactivé)</li><li>▪ <b>Centres de coûts :</b> nom et description du centre de coûts, adresse du centre de coûts, moyen de paiement associé au centre de coûts</li><li>▪ <b>Politique de voyage :</b> Nom et description de la politique de voyage, horaires et jours autorisés, secteur géographique autorisé, groupes bénéficiant de la politique de voyage, plafond budgétaire.</li></ul>

<b>Le traitement comprend les catégories suivantes de personnes concernées :</b>	<ul style="list-style-type: none"> <li>▪ Collaborateurs du Responsable de Traitement invités à utiliser les services WIMOVA for Business.</li> </ul>
<b>Durée du traitement :</b>	La durée du contrat par lequel le Responsable de Traitement utilise les services WIMOVA for Business fournis par le Sous-traitant

## A.2. Points de contact

Les Parties peuvent se contacter mutuellement en utilisant les points de contact suivants :

<p><b>Point de contact du Sous-Traitant :</b></p> <p><b>Nom :</b> Karim GALLOUL  <b>Fonction :</b> CDO  <b>Téléphone :</b> 04 72 32 94 68  <b>Courriel :</b> <a href="mailto:galloul.karim@WIMOVA.com">galloul.karim@WIMOVA.com</a></p> <p><b>Nom :</b> Gaëtan BOURDAIS – SHIFT avocats  <b>Fonction :</b> Délégué à la protection des données externalisé  <b>Téléphone :</b> 04 78 928 928  <b>Courriel :</b> <a href="mailto:gb@shift-avocats.com">gb@shift-avocats.com</a></p>	<p><b>Point de contact du Responsable de Traitement :</b></p> <p><b>Le Responsable de Traitement communique son Point de contact par l'intermédiaire de la plateforme WIMOVA for Business.</b></p>
--	--

## Section B. Sous-traitants ultérieurs autorisés et instructions relatives aux transferts de données vers des pays tiers ou des organisations internationales

### B.1. Sous-traitants ultérieurs autorisés

Dès l'entrée en vigueur de l'accord de sous-traitance, le Responsable de Traitement autorise le Sous-traitant à recourir aux sous-traitants ultérieurs suivants :

Nom du responsable du traitement des données	Lieu de stockage	Mesures de protection appropriées prises
<b>Acronis</b>	Etats-Unis, Inde	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne
<b>Cisco</b>	Etats-Unis, Pays Tiers	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne
<b>Google Firebase Crashlytics</b>	Etats-Unis, Pays Tiers	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne
<b>Instana</b>	Pays Tiers	Clauses contractuelles types adoptées par la Commission européenne
<b>Microsoft</b>	Serveurs situés dans l'UE Logiciels Office 365 : Europe, Etats-Unis, Pays tiers	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne
<b>The Rocket Science Group LLC d/b/a Mailchimp</b>	Etats-Unis, Pays Tiers	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne
<b>ZenDesk</b>	Etats-Unis, Pays Tiers	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne
<b>HubSpot</b>	Etats-Unis, Allemagne	Clauses contractuelles types adoptées par la Commission européenne, Décision d'adéquation de la Commission européenne

Le Responsable de Traitement autorise, dès l'entrée en vigueur de l'accord de sous-traitance, le recours aux sous-traitants ultérieurs mentionnés ci-avant pour les opérations de traitement confiées. Le Sous-traitant n'a pas le droit – sans l'autorisation écrite explicite du Responsable de Traitement – d'engager un sous-traitant ultérieur pour un traitement « différent » de celui qui a été convenu ou de faire exécuter le traitement décrit par un autre sous-traitant ultérieur.

### B.2. Instructions sur le transfert de données à caractère personnel

Le Responsable de Traitement reconnaît et accepte le transfert de données à caractère personnel vers des pays tiers par les sous-traitants énumérés au point **B.1.**

## Section C. Mesures de sécurité

Conformément à l'article 32 du RGPD, le Sous-traitant met en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, compte tenu de l'état de l'art, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement.

À ce titre, le Sous-traitant s'efforce de couvrir les domaines de sécurité suivants, de manière proportionnée aux risques identifiés :

Domaine de sécurité	Objectif
Pilotage de la sécurité	Structurer la gouvernance de la sécurité de l'information et assurer un suivi régulier des mesures déployées.
Encadrement contractuel de la sécurité	Formaliser les règles de sécurité applicables au personnel et aux tiers intervenant sur les systèmes d'information.
Sensibilisation des collaborateurs	Informar et former les personnes autorisées aux bonnes pratiques de protection des données et aux risques associés.
Authentification des utilisateurs	Vérifier l'identité des utilisateurs accédant aux systèmes et aux données par des moyens d'authentification adaptés.
Gestion des habilitations	Attribuer, réviser et retirer les droits d'accès selon le principe du moindre privilège et les besoins opérationnels.
Sécurité des postes de travail	Protéger les équipements utilisés pour le traitement des données contre les menaces logicielles et les accès non autorisés.
Protection du réseau informatique	Sécuriser les communications et cloisonner les environnements pour limiter la propagation d'éventuelles compromissions.
Sécurité des serveurs	Protéger les systèmes hébergeant les données contre les intrusions, les défaillances et les accès non autorisés.
Sécurité des sites web	Garantir la confidentialité et l'intégrité des échanges et prévenir les vulnérabilités applicatives des services exposés sur Internet.
Sécurité des locaux	Contrôler l'accès physique aux zones hébergeant des équipements ou données sensibles et prévenir les risques environnementaux.
Encadrement de la sous-traitance ultérieure	S'assurer que les sous-traitants ultérieurs présentent des garanties suffisantes et sont contractuellement engagés sur la sécurité.
Journalisation	Tracer les accès et opérations sur les systèmes afin de détecter les anomalies et de faciliter les investigations en cas d'incident.
Sauvegardes	Assurer la disponibilité des données par des copies régulières, protégées et stockées de manière sécurisée.
Gestion des incidents et des violations	Détecter, documenter et traiter les incidents de sécurité, et notifier le Responsable du traitement dans les délais requis.
Chiffrement	Recourir à des techniques cryptographiques pour protéger la confidentialité et l'intégrité des données sensibles.
Sécurité des applications mobiles	Protéger les données traitées par les applications mobiles et sécuriser leurs communications avec les serveurs.

Le Sous-traitant adapte les mesures mises en œuvre dans chaque domaine en fonction de l'évolution des menaces, des technologies disponibles et des traitements concernés.