Annexe relative au Traitement des Données

1. Opérations de Traitement et Définitions

1) La présente Annexe relative au Traitement des Données s'applique à l'ensemble des opérations de Traitement de Données à Caractère Personnel et ce, dans tous les cas où Schindler (le « **Sous-traitant** »), ses salariés ou sous-traitants (selon le cas) peuvent entrer en contact avec des Données à Caractère Personnel Traitées par le Sous-traitant pour le compte du Client (le « **Responsable de Traitement** ») à l'occasion de la fourniture de services s'inscrivant dans le cadre du présent Contrat. L'objet, la durée, la nature et les finalités du Traitement, les types de Données à Caractère Personnel et les catégories de Personnes Concernées sont énumérés dans la **Pièce Jointe 1** à la présente Annexe, qui peut faire des différences entre les services et produits spécifiques fournis.
2) L'ensemble des termes et expressions comportant des majuscules, employés dans la présente Annexe, qui sont définis dans le Règlement général sur la protection des données (Règlement UE 2016/679 – « **RGPD** »), mais qui ne le sont pas dans la présente Annexe ou ailleurs dans le Contrat, ont la signification indiquée dans le RGPD.

2. Traitement pour le Compte du Responsable de Traitement

1) Le Sous-traitant ne devra Traiter les Données à Caractère Personnel que dans le cadre du Contrat, sur instructions documentées du Responsable de Traitement, à moins que des obligations légales n'obligent le Sous-traitant à traiter les Données à Caractère Personnel autrement.
2) Les instructions du Responsable du Traitement sont généralement dans le Contrat. Les instructions ultérieures sont données par l'utilisation des caractéristiques techniques et des options de configuration convenues des produits et services fournis par le Sous-traitant. Si des instructions supplémentaires émises autrement par le Responsable du Traitement entraînent des efforts de mise en œuvre supplémentaires de la part du Sous-traitant, ces efforts seront compensés par le Responsable du Traitement conformément aux tarifs alors en vigueur du Sous-traitant en fonction du temps passé et du matériel utilisé.
3) Les instructions supplémentaires doivent impérativement être données par écrit ou dans un format électronique (format texte). Les instructions supplémentaires orales doivent être immédiatement confirmées par le Responsable de Traitement, par écrit ou au format texte.
4) Si le Sous-traitant considère qu'une instruction est contraire aux lois applicables en matière de protection des données, il devra en informer le Responsable de Traitement immédiatement et sera en droit de suspendre l'exécution des instructions en question jusqu'à ce que le Responsable de Traitement les confirme ou les modifie.

3. Obligations du Sous-traitant

1) Le Sous-traitant ne saurait utiliser les Données à Caractère Personnel du Responsable de Traitement dans le champ d'application de cette Annexe à d'autres fins que celles indiquées dans le Contrat et que celle d'exécuter les obligations lui incombant aux termes de ce dernier.
2) A tout moment pendant le traitement, le Sous-traitant devra rectifier, effacer ou bloquer les Données à Caractère Personnel s'inscrivant dans le champ d'application de la présente Annexe lorsque le Responsable de Traitement lui en donnera l'instruction..
3) Les salariés du Sous-traitant prenant part à des opérations de Traitement s'inscrivant dans le cadre de la présente Annexe ont pris un engagement de confidentialité ou sont soumis à une obligation légale de confidentialité appropriée.
4) Le Sous-traitant devra indiquer au Responsable de Traitement son interlocuteur pour toutes les questions liées à la protection des données s'inscrivant dans le champ d'application du Contrat.
5) Le Sous-traitant devra périodiquement contrôler les processus internes ainsi que les mesures techniques et organisationnelles, afin de faire en sorte que le Traitement relevant de sa responsabilité soit conforme aux lois applicables en matière de protection des données.
6) Le Sous-traitant devra assister raisonnablement le Responsable de Traitement, aux frais de ce dernier (selon les tarifs du Sous-traitant en vigueur au moment considéré, fixés en fonction du temps passé et du matériel utilisé), à se conformer aux obligations lui incombant en vertu des Articles 32 à 36 du RGPD ou les obligations correspondantes en vertu d'autre législations applicables en matière de protection des données.
7) Le Sous-traitant pourra Traiter les Données à Caractère Personnel dans ou en dehors d'un État membre de l'Union européenne (« **UE** ») ou de l'Espace économique européen (« **EEE** »). Des Données à Caractère Personnel ne pourront être transférées à destination d'un État qui n'est pas membre de l'UE ou de l'EEE que si les conditions spécifiques énoncées aux Articles 44 et suivants du RGPD ou dans les dispositions correspondantes d'autres législations applicables en matière de protection des données ont été satisfaites. À cet effet, le Sous-traitant pourra conclure – si nécessaire, en qualité de mandataire pour le compte du Responsable de Traitement – des contrats intégrant les clauses types relatives à la Protection des Données adoptées par la Commission de l'UE sur le fondement de la Directive UE 95/46CE ou RGPD (les « **Clauses Contractuelles Types** ») avec ses propres sous-traitants établis dans des pays tiers (n'assurant pas un niveau de protection des données adéquat) et prenant part au Traitement de Données à Caractère Personnel s'inscrivant dans le cadre de la présente Annexe. Ces Clauses Contractuelles Types pourront être complétées dans la mesure nécessaire pour respecter les lois applicables en matière de protection des données, y compris, la Section 28(3) du RGPD, dès lors que ces compléments ne seront pas contraires au Contrat (en ce compris la présente Annexe) ni aux Clauses Contractuelles Types en leur forme initiale. Le Sous-traitant pourra exercer les droits que les Clauses Contractuelles Types intégrées à des contrats conclus pour le compte du Responsable de Traitement confèrent à ce dernier en matière d'instructions et de contrôle.

4. Obligations du Responsable de Traitement

1) Le Responsable de Traitement devra veiller au respect des lois applicables en matière de protection des données, en particulier à la licéité du Traitement des Données à Caractère Personnel effectué par le Sous-traitant pour le compte du Responsable de Traitement.
2) Le Responsable de Traitement devra informer le Sous-traitant immédiatement et à défaut dans un délai

maximum de quarante-huit (48) heures, s'il constate des erreurs ou des irrégularités dans les opérations de Traitement, qui affectent le respect des lois applicables en matière de protection des données.

5. Droits des Personnes Concernées

1) Le Sous-traitant n'est pas tenu de répondre directement aux demandes d'information des Personnes Concernées. Il devra inviter ces personnes à s'adresser au Responsable de Traitement si les informations fournies par celles-ci permettent d'identifier le Responsable de Traitement concerné par la demande. Il en sera de même si une Personne Concernée demande au Sous-traitant de rectifier, d'effacer ou de bloquer des données.
2) Si le Responsable de Traitement est tenu de répondre à une demande d'information d'une Personne Concernée relative au Traitement de Données à Caractère Personnel, le Sous-traitant devra l'aider raisonnablement à fournir les informations demandées. Le Sous-traitant ne sera tenu de fournir ces informations que sur instruction documentée du Responsable de Traitement et à condition que ce dernier rembourse au Sous-traitant les coûts et dépenses (déterminés selon les tarifs du Sous-traitant en vigueur au moment considéré, fixés en fonction du temps passé et du matériel utilisé) qu'il aura supportés en lui apportant cette aide. Le Sous-traitant n'encourt aucune responsabilité dans le cas où le Responsable de Traitement manquerait de répondre de manière adéquate ou dans les délais à la demande de la Personne Concernée, ou dans le cas où le Responsable de Traitement n'apporterait aucune réponse aux demandes d'information.
3) Si la Personne Concernée introduit une réclamation à l'encontre du Sous-traitant sur le fondement de l'Article 82 du RGPD ou des dispositions correspondantes d'autres législations applicables en matière de protection des données, le Responsable de Traitement s'engage à assister raisonnablement le Sous-traitant aux fins de la défense que ce dernier opposera à la réclamation en question.

6. Mesures techniques et organisationnelles

1) Le Sous-traitant prendra les mesures techniques et organisationnelles indiquées dans la **Pièce Jointe 2** à la présente Annexe, qui peut faire des différences entre les services et produits spécifiques fournis.
2) Ces mesures techniques et organisationnelles sont susceptibles d'évoluer en fonction des progrès techniques et de faire l'objet de perfectionnement. Le Sous-traitant pourra les modifier à condition que le niveau de sécurité assuré par les nouvelles mesures ne soit pas inférieur à celui assuré par celles auxquelles celles-ci se substitueront. Les changements importants devront être documentés.

7. Communication en cas de violation de Données à Caractère Personnel

Le Sous-traitant avisera sans retard le Responsable de Traitement s'il a connaissance d'une violation de Données à Caractère Personnel concernant les Données à Caractère Personnel du Responsable de Traitement et fournira les informations raisonnablement disponibles dont le Responsable de Traitement a besoin pour remplir ses obligations de notification à l'égard de la Personne Concernée et/ou ses obligations de déclaration aux autorités compétentes en matière de protection des données. Le Responsable de Traitement donne au Sous-traitant l'instruction de prendre toutes les mesures que celui-ci jugera nécessaires ou utiles afin de protéger les Données à Caractère Personnel traitées pour le compte du Responsable de Traitement et d'atténuer dans toute la mesure du possible toutes éventuelles conséquences négatives pour la Personne Concernée.

8. Sous-traitance

1) Le Sous-traitant ne peut confier à des sous-traitants tout ou partie du Traitement des Données à Caractère Personnel sans l'accord spécifique ou général écrit préalable du Responsable de Traitement. Le Responsable de Traitement consent spécifiquement par les présentes à ce que le Sous-traitant fasse lui-même appel à des sous-traitants dans le cadre du Traitement des Données à Caractère Personnel pour le compte du Responsable de Traitement, comme énumérés dans la **Pièce Jointe 3** à la présente Annexe, qui peut faire des différences entre les services et produits spécifiques fournis. Par la présente, le Responsable du Traitement consent de manière générale à ce que le Sous-traitant engage d'autres sous-traitants qui fournissent des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le Traitement des Données à caractère personnel réponde aux exigences du GDPR ou aux exigences correspondantes d'autres législations applicables en matière de protection des données. Si le Responsable du Traitement a conclu des contrats intégrant des Clauses Contractuelles Types visées à la Section 3(7) ci-dessus, le consentement ci-dessus constitue le consentement écrit préalable du Responsable de Traitement à ce que le Traitement des Données à Caractère Personnel effectué pour son compte dans le cadre des Clauses Contractuelles Types en question soit confié à un ou plusieurs sous-traitants.
2) Le Sous-traitant informera le Responsable de Traitement avant de faire usage du consentement général pour engager d'autres sous-traitants et indiquera comment une non-réponse sera interprétée, donnant ainsi au Responsable de Traitement la possibilité de s'opposer au changement. Le Responsable de Traitement devra rapidement informer le Sous-traitant, par écrit, dans un délai de quatorze (14) jours à compter de la réception de la notification émanant de ce dernier, s'il s'oppose à ce changement ou à l'intervention du nouveau sous-traitant, en lui indiquant les motifs raisonnables de cette opposition.
3) Si le Responsable de Traitement ne s'oppose pas en temps utile, il sera réputé avoir renoncé à son droit correspondant. Si le Responsable de Traitement s'y oppose en temps utile le Sous-traitant sera en droit de résilier la présente Annexe moyennant un préavis de trente (30) jours adressé par écrit au Responsable de Traitement, ou de déployer des efforts raisonnables pour proposer à ce dernier une modification des opérations de traitement permettant d'éviter que les Données à Caractère Personnel soient Traitées par le sous-traitant supplémentaire ou de substitution. La modification suggérée ne saurait faire peser sur le Responsable de Traitement une charge déraisonnable.
   Si le Sous-traitant choisit de suggérer qu'une modification soit apportée aux opérations de Traitement et s'il n'est ensuite pas en mesure de procéder à cette modification dans un délai raisonnable, ou si le Responsable de Traitement n'approuve pas la modification suggérée – laquelle ne saurait être refusée sans motif raisonnable – chaque partie pourra mettre un

terme à la présente Annexe moyennant le respect d'un préavis de trente (30) jours adressé par écrit à l'autre partie .

4) Lorsqu'il fera appel à des sous-traitants dans le cadre du Traitement des Données à Caractère Personnel pour le compte du Responsable de Traitement, le Sous-traitant devra veiller à respecter les conditions suivantes :
   - le contrat de sous-traitance devra intégrer les stipulations relatives à la protection des données arrêtées d'un commun accord entre le Responsable de Traitement et le Sous-traitant dans le cadre de la présente Annexe ;
   - le Sous-traitant sera responsable de la conduite et des prestations de chacun de ses sous-traitants approuvés, et sera l'unique interlocuteur du Responsable de Traitement en rapport avec le Traitement de Données à Caractère Personnel par les sous-traitants en question.

9. Droits d'audit

1) Sur demande écrite préalable, le Sous-traitant certifiera au Responsable de Traitement qu'il respecte la présente Annexe en lui fournissant des preuves adéquates sous forme de résultats d'une auto-évaluation, de règles internes, y compris des justificatifs de conformité de source externe, des certificats relatifs à la protection des données et/ou à la sécurité informatique (par exemple, dans le cadre de la norme ISO 27001), des codes de conduite approuvés ou d'autres attestations appropriées. La preuve de la mise en œuvre de mesures non spécifiques à la présente Annexe pourra être apportée sous forme d'attestations et de rapports à jour ou d'extraits de tels rapports ou attestations émanant d'organes indépendants (par exemple, d'auditeurs externes, d'un service de contrôle interne, du délégué à la protection des données, du département en charge de la sécurité informatique ou de contrôleurs qualité) ou sous la forme d'une certification adéquate produite à la suite d'un contrôle portant sur la sécurité informatique ou la protection des données.
2) Le Responsable de Traitement est en droit de vérifier le respect de la présente Annexe par le Sous-traitant s'il estime, sur la base de motifs raisonnables à notifier au Sous-traitant, que les droits conférés aux termes du paragraphe 1 ne suffisent pas dans un cas spécifique, ou si une autorité compétente en matière de protection des données demande un contrôle. Le contrôle en question sera effectué au cours des heures normales d'activité, sans perturber l'activité du Sous-traitant, en observant un préavis raisonnable qui ne saurait en aucun cas être inférieur à trente (30) jours. Le Sous-traitant pourra subordonner le contrôle à la signature d'un accord de confidentialité concernant les données des autres clients et les mesures techniques et organisationnelles prises.
3) Le Responsable de Traitement ne saurait désigner un contrôleur se trouvant être dans une relation de concurrence avec le Sous-traitant ou de ses affiliées ou ne possédant pas les qualifications adéquates pour procéder au contrôle. Le Responsable de Traitement ne saurait exercer ses droits de contrôle plus d'une fois par période de douze (12) mois sauf i) si une autorité en charge de la protection des données ou un autre organe de régulation à la compétence de laquelle ou duquel il est soumis lui en donne l'instruction, ou ii) si le Responsable de Traitement considère raisonnablement qu'un contrôle supplémentaire est nécessaire en raison d'une infraction à la sécurité subie par le Sous-traitant ou dont il est considéré qu'il pourrait l'avoir subie.
4) Le Sous-traitant pourra prétendre, en contrepartie de ses efforts visant à permettre la réalisation des contrôles du Responsable de Traitement, à une rémunération déterminée selon les tarifs du Sous-traitant en vigueur au moment considéré, fixés en fonction du temps passé et du matériel utilisé.
5) Le Sous-traitant n'est pas tenu de divulguer ou de donner accès i) à des données relatives à d'autres clients (x) du Sous-Traitant (y) de ses affiliées ou (z) de ses propres sous-traitants, ii) à des informations internes, comptables ou financières, ou des secrets d'entreprise du Sous-traitant, de ses affiliées ou de ses propres sous-traitants, ni iii) à des informations qui pourraient compromettre la sécurité de systèmes ou de locaux du Sous-traitant, de ses affiliées ou de ses propres sous-traitants.

10. Responsabilité et dommages-intérêts

Les stipulations relatives à la Responsabilité, telles que convenues entre les parties au Contrat, s'appliquent à toute responsabilité découlant ou en rapport avec toute Clause Contractuelle Type intégrée à un contrat conclu pour le compte du Responsable de Traitement conformément à la Section 3(7) ci-dessus. Les dommages-intérêts qui seraient recouvrés par une partie au Contrat (en ce compris la présente Annexe) ou à un contrat intégrant des Clauses Contractuelles Types, viennent en déduction du montant des demandes de dommages-intérêts correspondantes formulées par la partie en question sur le fondement de l'un quelconque des autres accords susmentionnés.

11. Restitution ou suppression des données à Caractère Personnel

À la fin de la présente Annexe, le Sous-traitant, au choix du Responsable du Traitement, supprimera les Données à Caractère Personnel traitées en vertu des présentes ou renverra ces données et supprimera les copies existantes, sauf si et aussi longtemps que la législation applicable exige la conservation de ces données.

12. Divers

En cas de contradiction, les stipulations de la présente Annexe prévaudront sur les autres stipulations du Contrat

PIÈCE JOINTE 1 À L'ANNEXE RELATIVE AU TRAITEMENT DES DONNÉES

INFORMATIONS RELATIVES AUX DONNÉES À CARACTÈRE PERSONNEL ET À LEUR TRAITEMENT

Objet du Traitement des Données à Caractère Personnel	Fourniture de services au Responsable de Traitement dans le cadre du Contrat.
Nature du Traitement des Données à Caractère Personnel	Traitement de Données à Caractère Personnel destiné à fournir des services dans le cadre du Contrat, conformément aux termes de celui-ci, y compris les opérations décrites à l'Article 4 Section 2 du RGPD.
Types de Données à Caractère Personnel	Données relatives à des personnes physiques, fournies au Sous-traitant par le Responsable de Traitement ou par des personnes autorisées par ce dernier, par le biais de l'utilisation des services dans le cadre du Contrat. Ces données peuvent comprendre, par exemple, des noms, des numéros de téléphone et de télécopie, des adresses électroniques, des adresses postales, des identifiants d'utilisateurs, des autorisations d'accès, des préférences ou d'utilisation de systèmes, des adresses IP, des fuseaux horaires, des langues, des dénominations sociales et d'autres informations relatives à des entités juridiques.
Finalité du Traitement des Données à Caractère Personnel	Fourniture de services dans le cadre du Contrat, conformément aux termes de celui-ci.
Catégories de Personnes Concernées auxquelles se rapportent les Données à Caractère Personnel	Personnes physiques relativement auxquelles des données sont fournies au Sous-traitant par le Responsable de Traitement ou par des personnes autorisées par celui-ci, par le biais de l'utilisation des services dans le cadre du Contrat. Il peut s'agir, par exemple, du Responsable de Traitement, de ses fournisseurs, de ses prestataires de services ou autres partenaires contractuels, leurs employés respectifs et d'autres personnes, telles que les utilisateurs des propriétés immobilières du Responsable de Traitement .
Durée du Traitement des Données à Caractère Personnel	Durée du Contrat et période débutant à l'expiration de celui-ci et s'achevant au moment de l'effacement des Données à Caractère Personnel par le Sous-traitant, auquel celui-ci procède selon les termes du Contrat.

PIECE JOINTE 2 A L'ANNEXE RELATIVE AU TRAITEMENT DES DONNEES

MESURES TECHNIQUES ET ORGANISATIONNELLES

Les mesures d'ordre administratif, physique, organisationnel et technique prises par le Sous-traitant devront comprendre au minimum les suivantes :

1. Confidentialité

- Contrôle physique des accès
  Le Sous-traitant se dote de règles relatives au contrôle physique des accès, conçues afin d'empêcher tout accès physique non autorisé à des installations ou équipements dédiés au stockage et au traitement des données. Les points d'entrée sont contrôlés par des dispositifs de verrouillage électroniques et mécaniques. En outre, des services de sécurité des installations et équipements sont en place. Les règles internes du Sous-traitant garantissent que les autorisations d'accès des salariés sont révoquées et que les badges et/ou clés d'accès sont restitués au moment de la résiliation de leur contrat de travail.
- Contrôle électronique des accès
  L'accès électronique à l'ensemble des systèmes dédiés au stockage et au traitement des données est protégé par mot de passe. L'expiration et le niveau de sécurité des mots de passe (constitués au minimum de 10 caractères alphanumériques) sont régis par les règles internes du Sous-traitant. L'accès depuis l'extérieur du réseau du Sous-traitant n'est possible que par le biais de réseaux privés virtuels (VPN) grâce à une authentification à deux facteurs. Les jetons permettant un accès à distance sont révoqués lorsque cet accès n'est plus nécessaire.
- Contrôle interne des accès
  Un concept et un mécanisme d'autorisation fondés sur les besoins ont été mis en place pour tous les systèmes dédiés au traitement et au stockage des données, dans le but d'empêcher tout accès non autorisé aux Données à Caractère Personnel. Les autorisations d'accès sont subordonnées à des validations régulières, selon les indications contenues dans les règles internes du Sous-traitant.

2. Intégrité

- Contrôle des transferts de données
  Toutes les Données à Caractère Personnel transférées depuis un équipement collectant ce type de données à destination des systèmes du Sous-traitant sont chiffrées et transférées par un canal sécurisé.
- Contrôle des entrées de données
  Le Sous-traitant enregistre et contrôle les entrées de Données à Caractère Personnel dans les systèmes dédiés à la conservation et au traitement de ce type de données. Il enregistre notamment la personne procédant à ces intégrations ainsi que le moment où les données en question sont modifiées ou effacées.

3. Disponibilité et résilience

- Contrôle de la disponibilité
  Toutes les Données à Caractère Personnel font l'objet d'une sauvegarde. Des copies de sauvegarde des informations et logiciels sont produites et testées régulièrement conformément aux règles internes du Sous-traitant.
- Récupération rapide
  Des mesures de récupération sont en place dans le cadre des différents systèmes dédiés au stockage et au traitement des données et font régulièrement l'objet de nouvelles validations. Les procédures et mesures destinées à assurer la continuité de l'activité sont exposées dans le cadre des règles internes du Sous-traitant. Des vérifications relatives à la continuité de l'activité sont régulièrement effectuées. Les sous-traitants qui traitent des données pour le compte du Sous-traitant sont certifiés par un tiers afin de garantir une complète redondance et un temps de disponibilité maximum.

4. Tests et évaluations réguliers

- Gestion de la protection des données
  Des procédures de gestion des incidents, des modifications et des tests, y compris des procédures de test automatisées, sont en place et font régulièrement l'objet de nouvelles validations. Des tests de sécurité et de sûreté supplémentaires sont effectués à certains endroits sensibles en termes de qualité au cours du processus de développement d'applications par le Département cybersécurité du Sous-traitant, ainsi que par des tiers, sur demande. Lors de leur déploiement et à l'occasion de chaque changement, les applications sont analysées en tenant compte de tout changement de leur domaine d'utilisation.

5. Protection des données dès la conception et par défaut
   L'ensemble des exigences relatives à la sécurité sont identifiées et documentées durant la phase de conception d'un projet, conformément aux règles internes du Sous-traitant, de façon à ce que les systèmes soient conçus pour assurer le respect des règles relatives à la protection des données et la sécurité de ces dernières.

6. Contrôle des instructions et des sous-traitants du Sous-traitant

- Contrôle des instructions
  Le Traitement des Données à Caractère Personnel pour le compte du Responsable de Traitement n'est effectué que dans le cadre du Contrat et selon les instructions documentées du Responsable de Traitement. Les instructions complètes et définitives de ce dernier relatives au Traitement des Données à Caractère Personnel sont définies par le Responsable de Traitement et par ses utilisateurs autorisés des services dans le cadre du Contrat.
- Contrôle des sous-traitants du Sous-Traitant
  Le Sous-traitant ne confiera à un tiers le soin de prendre part au Traitement des Données à Caractère Personnel pour le compte du Responsable de Traitement qu'après avoir obtenu l'accord de ce dernier et sur la base d'accords contractuels clairs relatifs à la sécurité, à la confidentialité et à la protection de la vie privée.

PIÈCE JOINTE 3 À L'ANNEXE RELATIVE AU TRAITEMENT DES DONNÉES

LISTE DES SOUS-TRAITANTS DU SOUS-TRAITANT

Veuillez vous référer à la liste séparée de la Pièce Jointe 3.