Convention par rapport au traitement des données personnelles dans la commande au sens de l'article 28 du RGPD

Entre

le client ou le responsable

et

moveIT Software GmbH

(Ci-après dénommé «**moveIT**»)

(Le sous-traitant ou l'exécutant de la commande)

1. SUJET ET DURÉE DE LA CONVENTION

1.1 Dans le cadre de l'exécution du contrat conclu (contrat de licence), le sous-traitant traite des données à caractère personnel («**Données**») en tant qu'exécuteur de la commande de la part du client dans le sens de l'article 28 du règlement relatif à la protection des données (UE) 2016/679 («**RGPD**»).

1.2 La durée de cette convention commence par la signature de la convention et termine accessoirement par la terminaison ou la résiliation des contrats valables (p.ex. le contrat de maintenance des licences moveIT) et / ou après la réalisation de tous les services conclus par contrat.

1.3 Sujet et traitement : **Produits de licence moveIT**

1.4 Manière et but du traitement :

- **Installation et établissement des produits de licence moveIT dans le système du client via maintenance à distance.**
- **D'autres services via maintenance à distance par rapport aux produits de licence moveIT dans le système du client (Configuration, mises à jour du programme ou des données de base, correction d'erreurs)**

2. PORTEE DU TRAITEMENT DE L'ORDRE

2.1 Catégories de personnes concernées

Les catégories de personnes concernées par le traitement de données sont:

- **Clients**
- **Fournisseurs**
- **Parties interessées**
- **Employés**
- **Interlocuteurs**

2.2 Genres de données traitées

Les genres de données suivants sont sujet du traitement de données personnelles :

- **Données de base relatives aux personnes** (p.ex. nom, prénom, sexe, adresse)
- **Indication sur la formation et la profession** (p.ex. titre académique, titre de profession)
- **Données de communication** (p.ex. numéro de téléphone, adresse mail)
- **Histoire des clients** (p.ex. offres, ordres, réclamations)

3. OBLIGATIONS DU SOUS-TRAITANT

3.1 Les données seront traitées uniquement dans le cadre d'une commande écrite passée par le client. Le traitement de ces données par le sous-traitant s'effectue uniquement avec le but de fournir les services indiqués dans le contrat. Le client permet l'accès aux données dans les limites de l'exécution du contrat.

3.2 Si moveIT est chargé par les autorités publiques de transmettre des données de la part du client et cette demande est légale et se réfère à une commande passée, le sous-traitant est obligé de communiquer cette transmission immédiatement au client. À l'égard d'une autorité de contrôle dans le cas mentionné, le sous-traitant fera référence au client.

3.3 Le sous-traitant n'a pas le droit de modifier ou supprimer les données traitées et collectionnées dans le cadre du traitement de la commande sans disposer d'une instruction explicite et documentée de la part du client. Également, le sous-traitant ne doit pas borner le traitement des données mentionnées sans l'instruction mentionnée. Si une personne affectée à l'égard du cas mentionné s'adresse directement au sous-traitant, le sous-traitant passera cette demande au client immédiatement. Par la suite, le client est responsable pour le traitement de la demande de la personne concernée.

3.4 Le sous-traitant le déclare juridiquement contraignant selon § 6 DSG 2018 (Loi sur la protection des données d'Autriche, ci-après dénommé «DSG») qu'il oblige à toutes les personnes responsables pour le traitement de données de conclure un accord de confidentialité et de connaître les directives pertinentes dans le cadre de leur responsabilité par rapport à la protection de données avant l'exécution de cette commande. En outre, cette obligation de confidentialité de la part des personnes responsables pour le traitement de données subsiste même après la terminaison de la commande et la cessation des fonctions chez le sous-traitant.

3.5 Le sous-traitant s'oblige à prendre des mesures techniques et organisationnelles selon les exigences décrites dans l'article 32 du RGPD afin de protéger les données. Dans ce cadre, moveIT respecte les exigences techniques et organisationnelles décrites plus en détail dans **l'annexe** de cette convention. À part du règlement de cette convention sur le traitement de données personnelles dans la commande, le client et le sous-traitant respectent les obligations légales selon les art. 28-36 du RGPD.

3.6 Le sous-traitant contrôle les processus internes et les mesures techniques et organisationnelles régulièrement afin d'assurer que le traitement sous sa responsabilité s'effectue conformément au règlement sur la protection des données en vigueur et que la protection des droits de la personne concernée est sauvegardée.

3.7 Le sous-traitant a le droit d'amplifier et d'améliorer les mesures conformément au contrat. Ainsi, il peut prendre de nouvelles mesures qui sont également ou plus effectives que les mesures d'avant et qui ont le même but. Pour effectuer des modifications intégrantes, le sous-traitant a besoin d'une convention écrite avec le client.

3.8 Si le sous-traitant reçoit une demande d'un renseignement et le demandeur pense par erreur que le sous-traitant est le client de l'application des données, le sous-traitant transmettra la demande au client et communiquera cette transmission au demandeur. Si ces demandes se réfèrent à une commande de traitement des données du client auprès du sous-traitant, le sous-traitant s'oblige à soutenir le client, si possible, par des mesures techniques et organisationnelles en respectant les droits de la personne concernée selon le chapitre III du RGPD pour que le client puisse répondre aux demandes des personnes concernées.

3.9 Le client et le sous-traitant coopèrent dans l'accomplissement de leurs tâches s'il y a une telle demande de la part d'une autorité de contrôle.

4. AUTORISATION DE DONNER DES INSTRUCTIONS ET DROITS DU CLIENT

4.1 Le sous-traitant traitera les données uniquement selon les instructions documentées de la part du client. Si le client donne une instruction orale, il s'oblige de l'affirmer immédiatement par écrit. Si le sous-traitant estime qu'une instruction implique une entorse au RGPD, DSG 2018 ou d'autre règlement pour la protection des données personnelles, il en informe le client immédiatement. Le client n'est pas obligé de suivre des instructions illégales.

4.2 Le client a le droit de s'assurer de l'accomplissement du règlement sur la protection des données auprès du sous-traitant à tout moment. Le client s'oblige à minimiser l'impact des contrôles sur les activités du sous-traitant.

5. SUPPRESSION DES DONNEES

5.1 La conclusion des travaux sous contrat doit être prouvée par une confirmation écrite de la part du client. Après l'achèvement de la commande ou à la demande du client, le sous-traitant rend les données enregistrées pour le traitement ou il les supprime complètement et professionnellement au nom du client, s'il n'y pas d'autre convention au sujet. Le sous-traitant doit confirmer la suppression des données auprès du client.

5.2 L'obligation par rapport à la suppression n'est pas valide si le sous-traitant a une obligation légale par rapport à l'enregistrement des données personnelles. Dans ce cas, le sous-traitant peut garder celles-ci après l'achèvement du contrat pendant la période de conservation (en considérant les droits commerciaux et fiscaux). Néanmoins, il est obligé de supprimer les données conformément au règlement sur la protection des données après l'expiration de la période de conservation.

6. RELATIONS DE SOUS-TRAITANCE

6.1 Si l'exécutant de la commande commissionne à un autre exécutant pour le traitement de la commande passée par le client (dans le cas particulier), il a besoin de l'autorisation écrite par le responsable. L'exécutant supplémentaire est également obligé par contrat de respecter les devoirs pour la protection des données qui étaient sujet de la convention sur le traitement des données personnelles dans la commande selon l'art. 28 du RGPD.

6.2 Les services suivants ne représentent pas de relations de sous-traitance au sens de ce règlement: Des services de télécommunication, de poste ou transfert, de maintenance, le service utilisateur ou l'élimination des supports de données ou d'autres mesures qui ont le but de protéger la confidentialité, la disponibilité, l'intégrité et la résistance du hardware et software des installations de traitement des données.

7. DISPOSITIONS FINALES

7.1 Le sous-traitant peut exiger une rémunération pour des services de soutien qui ne sont pas inclus dans la description des services de la commande passée par le client ou qui ne sont pas la conséquence d'une faute de la part du sous-traitant.

7.2 moveIT n'a pas mandaté de responsable de la protection des données dans l'entreprise. Selon l'article 37 RGPD, cela n'est pas obligatoire.

7.3 L'application du RGPD se base sur la loi autrichienne (DSG 2018). Le lieu de juridiction est Wels.

7.4 Cette convention complète le contrat auquel elle se réfère.

7.5 S'il est ou sera nécessaire d'adapter cette convention afin d'accomplir les exigences du RGPD ou des lois sur la protection des données nationaux qui le complètent ou concrétisent, les deux parties s'obligent à effectuer ces modifications. Tout(e) modification, complément, annulation ou résiliation de cette convention ainsi que la modification de cette clause doit s'effectuer par écrit.

Pour le client:	**Pour le sous-traitant:**
_____	moveIT Software GmbH
Entreprise	Entreprise
_____	Wels, 18. April 2018
Lieu | Date	Lieu | Date
_____	_____
Signature	Signature
_____	Kevin Hornung, MSc, Verantwortlicher für Datenschutz
Nom en copie conforme	Nom en copie conforme

APPENDICE A L'ANNEXE

Mesures techniques et organisationnelles selon l'article 32 (1) RGPD

1. Garantie de confidentialité

a) Contrôle d'accès à l'édifice

Des mesures techniques ou organisationnelles qui empêchent l'accès non autorisé aux locaux où les données sont traitées :

- Des visiteurs sont accueillis par la personne à laquelle ils rendent visite directement au foyer d'entrée. La personne visitée les accompagne dans la maison pendant la visite et les conduit à la sortie à la fin de la visite.
- L'entrée principale, qui mène aux bureaux de moveIT, est fermée. On a besoin d'une clé pour l'ouvrir. Uniquement le personnel en informatique qui dispose de la clé a accès aux locaux où se trouvent les serveurs. Les locaux de serveurs sont toujours fermés.
- Sécurité d'alarme aux fenêtres et portes d'entrée.

b) Contrôle d'accès aux systèmes

Des mesures techniques et organisationnelles qui empêchent l'utilisation des systèmes de traitement des données par des personnes non autorisées.

- L'accès aux systèmes de traitement des données s'effectue uniquement par un code d'utilisateur et un mot de passe individuel parmi le domaine.
- La saisie de cinq mots de passe faux provoque le blocage de l'identifiant. Uniquement l'administrateur du système peut enlever ce blocage dans le cadre d'un processus d'authentification définie. Tous les blocages d'identifiants seront enregistrés et contrôlés régulièrement par l'administrateur du système.
- Un pare-feu empêche tout accès au serveur de l'extérieur.

c) Contrôle d'accès

Des mesures techniques et organisationnelles visant à assurer que les personnes autorisées à utiliser un système de traitement des données n'ont accès qu'aux données soumises à leur autorisation d'accès et que les données personnelles ne sont pas lues, copiées, modifiées ou supprimées par des personnes non autorisées pendant le traitement, l'utilisation et après l'enregistrement :

- Le règlement d'accès s'effectue par des programmes spéciaux en utilisant un ID d'employé personnel avec un mot de passe individuel de l'employé. Chaque employée reçoit l'accès aux processus de logiciel nécessaires selon ses compétences.
- L'administrateur du système assigne des identifiants d'employé individuels afin de contrôler les droits d'accès.
- Si ordonné, l'administrateur du système peut contrôler l'accès par la suppression ou la modification des mots de passe ou par l'attribution de priorités.
- Uniquement les employés qui disposent des droits d'administrateur ont accès aux systèmes serveur.
- Dans le cadre de la maintenance à distance, on utilise un jeton de sécurité - si le client en dispose-, ou un outil de télémaintenance afin de se connecter au système du client. Les jetons sont maintenus verrouillés.

d) Contrôle de transmission

Des mesures techniques et organisationnelle qui empêchent que les données personnelles soient lues, copiées, modifiées ou supprimées pendant la transmission électronique, pendant le transfert ou l'enregistrement à un support de données par des personnes non autorisées. En outre, ce sont des mesures qui permettent de contrôler et de vérifier où il y aura/a eu une transmission de données personnelles par des institutions afin de passer les données.

- Les supports de données (papiers inclus) qui ne sont plus nécessaires seront détruits physiquement par une entreprise spécialisée dans le cadre du règlement sur la protection des données et ils seront mis au rebut conformément au règlement sur la protection des données.
- Uniquement les employés en informatique avec les droits adéquats ont accès aux supports de données.
- Les bandes avec les fichiers de sauvegarde sont générées quotidiennement par le système.
- Les supports de données sauvegardées sont stockés extérieurement et sont supprimés régulièrement.

2. Garantie d'intégrité

a) Contrôle de saisie et d'enregistrement

Des mesures techniques et organisationnelles qui permettent de contrôler et de vérifier ultérieurement si et par qui les données personnelles étaient saisies, modifiées ou supprimées dans les systèmes de traitement des données :

- Uniquement un groupe de personnes autorisées peut supprimer les données enregistrées.

b) Contrôle de separation ou d'affectation

Des mesures techniques et organisationnelles visant à garantir que les données enregistrées pour des buts différents peuvent être traitées séparément :

- Les données collectées pour des clients différents et aux fins différents seront séparées logiquement dans les systèmes de banque de données de moveIT. Cela entraîne que les données ne seront lues, traitées et modifiées que par les employé(e)s avec les droits d'accès adéquats.

3. Disponibilité et capacité

a) Contrôle de disponibilité

Le sous-traitant prend les mesures techniques ou organisationnelles suivantes afin de garantir que les données personnelles seront protégées de la destruction ou la perte par erreur :

- L'édifice et le centre informatique sont assurés contre le dommage causé par un coup de foudre.
- Il y a une installation de détection d'incendie centrale connecté aux pompiers et la police par un service de sécurité engagé 24 heures et 364 jours qui annonce les incendies.
- Dans le cadre de la sauvegarde des données, on génère et enregistre des copies de sauvegarde des données collectées des systèmes productifs. En cours de travail, l'enregistrement des données s'effectuent sur des systèmes Raid ou des systèmes de banque de données miroités.

- Détecteur d'incendie, ASI dans le centre informatique

b) Récupération rapide (Art. 32 alinéa 1 lit. c RGPD);

- Sauvegarde du système CRM par moveIT une fois par jour sur un ordinateur virtuel. Récupération et sauvegarde de bande faciles et rapides.
- Le stockage de fichiers client interne avec la protection d'accès selon les directives de groupe s'effectue une fois par jour (triple sauvegarde) : sur deux serveurs virtuels différents et sur bande, récupération rapide grâce aux sauvegardes de clichés instantanés.
- Le client est responsable pour tout stockage de fichiers central (p.ex. Transfer Cloud) mis à la disposition.

c) Capacité

Mesures qui garantissent la capacité des systèmes et services en relation avec le traitement :

Tous les jeux de données qui sont stockés dans le système du client sont déjà enregistrés lors de la saisie dans la banque de données au fond (on Demand).

4. Pseudonymisation et codage

- L'accès à nos systèmes de banque de données (CRM, projets, erreurs, etc.) en dehors de l'entreprise s'effectue exclusivement par une connexion VPN protégée. En outre, notre entreprise doit donner accès à l'utilisateur à la connexion VPN avant que celui-ci puisse se connecter. Par ailleurs, nos systèmes de banque de données internes sont signés par un certificat de Lotus Notes.
- Les ordinateurs portatifs de l'entreprise sont protégés par un Bitlocker (Codification du disque dur) et ne peuvent pas être lus en cas de perte ou de vol.
- Les portables de l'entreprise et les tablettes peuvent être bloqués ou supprimés en cas de perte ou de vol.
- Les emails envoyés dans le cadre de moveIT sont chiffrés.

5. Processus de vérification et d'évaluation régulières par rapport à l'efficacité des mesures techniques et organisationnelles

- Incident-Response-Management
- Formation des employées
- Les banques de données au fond de moveIT@ISS+ sont toujours à la pointe de la technologie ce qui est garanti par des contrats de maintenance valables avec le fournisseur de software Progress (versions actuelle Progress 11.7). Les frameworks (composants Windows) utilisés par moveIT@ISS+ sont également à la pointe de la technologie, également assuré par des contrats de maintenance valables (Visual C++ 2015 et .Net 4.X). En outre, moveIT a une assurance de qualité interne qui effectue des tests setup régulièrement.
- Aucun traitement des données de commande dans le sens de l'art. 28 du RGPD sans directive conforme de la part du client, par exemple une conception de contrat précise.