Ile iLe présent Accord de traitement de données (l'« Accord ») est conclu par et entre le **Client figurant sur le formulaire de commande** (ci-après dénommé le « Client ») et le sous-traitant, Ungerboeck Systems International GmbH, Kaiserstrasse 72, 76137 Karlsruhe, Allemagne (ci-après dénommé le « Prestataire »).

Préambule

Le présent Accord définit concrètement les obligations des parties en matière de protection des données, qui découlent de la relation contractuelle entre les parties, et est intégré par les présentes à tout Bon de commande/Offre/Contrat de service existant et en vigueur, y compris les conditions générales d'abonnement, le contrat de maintenance et/ou le contrat d'hébergement en cloud d'Ungerboeck ; ci-après dénommés collectivement le « Contrat de service ».

Le présent Accord s'applique à toutes les activités dans lesquelles les employés du Prestataire ou les personnes mandatées par le Prestataire traitent les données à caractère personnel du Client. Afin de garantir le respect des lois applicables en matière de protection des données concernant les transferts de données à caractère personnel d'un responsable du traitement ou d'un sous-traitant au sein de l'Espace économique européen (« EEE »), de la Suisse ou du Royaume-Uni (« RU ») vers un sous-traitant situé en dehors de l'EEE, de la Suisse ou du Royaume-Uni, et afin de refléter les modifications apportées à la législation en Europe, en Suisse et au Royaume-Uni à la suite de l'approbation des nouvelles clauses contractuelles types par la Commission européenne et de l'Addendum du RU par le Bureau du commissaire à l'information du Royaume-Uni, les parties modifient par la présente leurs mécanismes de transfert de données, tel qu'établi dans l'Accord, comme suit :

1. Objet et durée de la commande ou du contrat

(1) Objet

L'objet de la présente commande est défini dans le Contrat de service.

(2) Durée

La durée de la commande (durée du traitement de la commande) correspond à la durée du Contrat de service associé.

2. Spécification de l'objet du contrat

(1) Type et finalité du traitement des données envisagé

La portée, le type et la finalité de la collecte, du traitement et/ou de l'utilisation des données à caractère personnel par le Prestataire pour le Client sont spécifiquement décrits dans le Contrat de service. Il s'agit notamment de ce qui suit :

- Services en cloud (hébergement) de la base de données pour l'utilisation de la solution logicielle
- Traitement des données des serveurs web connexes stockées dans des bases de données par le Prestataire pour l'exécution de l'assistance, de la maintenance et du développement ultérieur (par exemple tickets d'assistance, dépannage, assistance opérationnelle, réunions à distance (GoToMeeting), etc.)
- Traitement des données à caractère personnel pour la cession de droits (exclusivement pour les serveurs web) après avoir été mandaté par le Client.
- Accès aux fichiers journaux pour la détection et la rectification des erreurs.
- Mise en œuvre des processus d'importation, d'exportation et de migration, y compris des données à caractère personnel (assistance technique et opérationnelle).
- Développement et mise en œuvre d'interfaces pour le transfert de données entre systèmes.

(2) Nature des données

Le traitement des données à caractère personnel implique les types/catégories de données suivants :

- Données de base personnelles, telles que le prénom, le nom de famille, le sexe, le titre universitaire, le département/poste.

- Données de communication, par exemple le numéro de téléphone, e-mail, fax, numéro de téléphone portable.
- Données essentielles des contrats (relation contractuelle, produit ou intérêt contractuel, segment de marché)
- Historique des clients
- Données de facturation et de paiement des contrats
- Données de planification et de contrôle
- Autorisations et droits d'accès au système
- Mots de passe
- Données statistiques
- Activités des utilisateurs (fichiers journaux)
- Données saisies par l'internaute
- Adresses IP des utilisateurs

(3) Catégories de personnes concernées

Les catégories de personnes concernées par le traitement sont les suivantes :

- Utilisateurs des sites Web du Client (par exemple les clients potentiels, clients avérés, partenaires contractuels, personnes de contact)
- Clients
- Prospects et prospects potentiels
- Abonnés
- Partenaires contractuels
- Employés
- Fournisseurs
- Personnes de contact

3. Mesures techniques et organisationnelles

(1) Le Prestataire s'engage à respecter vis-à-vis du Client les mesures techniques et organisationnelles nécessaires au respect de la réglementation applicable en matière de protection des données à caractère personnel. Cela inclut notamment les exigences de l'art. 32 du RGPD. Le Prestataire s'engage également à respecter les obligations qui lui incombent en vertu de l'art. 32(1)(d) du RGPD consistant à mettre en œuvre une procédure d'examen régulier de l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

(2) Le Prestataire doit établir la sécurité conformément aux art. 28 (3) c), 32 du RGPD, notamment en lien avec l'art. 5 (1), (2) du RGPD. Globalement, les mesures à prendre sont des mesures de sécurité des données et visent à assurer un niveau de protection adapté au risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes. Dans ce contexte, l'état de l'art, les coûts de mise en œuvre et la nature, la portée et les finalités du traitement, ainsi que la probabilité et la gravité variables du risque pour les droits et libertés des personnes physiques au sens de l'article 32 (1) du RGPD sont pris en considération.

(3) L'état des mesures techniques et organisationnelles existant au moment de la conclusion du contrat de service est joint en **Annexe 1**.

(4) Les mesures techniques et organisationnelles sont soumises au progrès technique et aux évolutions ultérieures. À cet égard, le Prestataire est autorisé à mettre en œuvre des mesures alternatives adéquates. Ce faisant, le niveau de sécurité des mesures spécifiées ne doit pas être affaibli. Les changements significatifs doivent être consignés par écrit. Le Client peut demander à tout moment une version actualisée des mesures techniques et organisationnelles prises par le Prestataire.

4. Correction, restriction et suppression des données

(1) Le Prestataire ne traitera les données à caractère personnel que (i) dans la mesure où cela est nécessaire pour fournir les Services, (ii) conformément aux instructions spécifiques qu'il a reçues du Client, y compris en ce qui concerne tout transfert, et (iii) dans la mesure où cela est nécessaire pour se conformer à la loi (auquel cas, le Prestataire informera préalablement le Client de cette exigence légale, sauf si la loi interdit cette divulgation).

(2) Dans la mesure où ils sont couverts par l'étendue des services, le concept d'effacement, le droit à l'oubli, la correction, la portabilité des données et l'information sont assurés directement par le Prestataire conformément aux instructions documentées du Client.

5. Assurance qualité et autres obligations du Prestataire

Outre le respect des dispositions de la présente Commande, le Prestataire a des obligations légales en vertu des art. 28 à 33 du RGPD ; à cet égard, le Prestataire doit notamment veiller au respect des exigences suivantes :

- Nomination écrite d'un responsable de la protection de la vie privée qui exercera ses fonctions conformément aux art. 38 et 39 du RGPD. Les coordonnées du délégué externe à la protection des données peuvent être consultées à tout moment sur le site Internet du Prestataire à l'adresse https://ungerboeck.com/privacy-policy, qui est susceptible d'être modifiée de temps à autre.
- Le maintien de la confidentialité conformément à l'art. 28 para. 3 s. 2 lit. b, 29, 32 para. 4 du RGPD. Lors de l'exécution des travaux, le Prestataire ne fait appel qu'à des collaborateurs qui sont tenus de respecter la confidentialité et qui ont été familiarisés au préalable avec les dispositions relatives à la protection des données qui les concernent. Le Prestataire et toute personne subordonnée au Prestataire qui a accès aux données à caractère personnel peuvent traiter ces données exclusivement conformément aux instructions du Client, y compris les pouvoirs accordés dans le présent Accord, à moins qu'ils ne soient légalement obligés de les traiter.
- La mise en œuvre et le respect de toutes les mesures techniques et organisationnelles requises pour cette ordonnance, conformément à l'art. 28 para. 3 p. 2 lit. c, 32 du RGPD (voir annexe 1).
- La participation aux enquêtes de l'autorité de surveillance à l'égard du Client, dans la mesure où elles concernent le présent traitement des commandes.
- Informer immédiatement le Client des actions et mesures de contrôle de l'autorité de surveillance, dans la mesure où elles concernent le présent Accord. Cela s'applique également dans la mesure où une autorité compétente enquête sur le Prestataire dans le cadre d'une infraction administrative ou d'une procédure pénale en ce qui concerne le traitement des données à caractère personnel pendant le traitement de la commande.
- Dans la mesure où le Client est exposé à un contrôle de l'autorité de surveillance, à une infraction administrative ou à une procédure pénale, à des actions en responsabilité de la part d'une personne concernée ou d'un tiers ou à toute autre action en relation avec le traitement des commandes chez le Prestataire, ce dernier s'engage à soutenir le Client au mieux de ses possibilités.
- Le Prestataire contrôle régulièrement les processus internes ainsi que les mesures techniques et organisationnelles afin de veiller à ce que le Traitement dans son domaine de responsabilité soit effectué conformément aux exigences du droit applicable en matière de protection des données, et que la protection des droits de la Personne concernée soit assurée.
- Vérification des mesures techniques et organisationnelles prises vis-à-vis du Client dans le cadre de ses pouvoirs de contrôle conformément à la rubrique 7 du présent Accord.

6. Relations avec les sous-traitants secondaires

(1) Les relations de sous-traitance secondaire dans le cadre de cette disposition s'entendent des services qui se rapportent directement à la prestation du Service principal. Cela ne comprend pas les services auxiliaires auxquels le Prestataire a recours, par exemple en tant que services de télécommunications, services postaux/de transport, service de maintenance et d'utilisation ou élimination des supports de données ainsi que d'autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du contenu et du logiciel des systèmes de traitement des données. Toutefois, le Prestataire est tenu de mettre en œuvre des accords contractuels appropriés et conformes à la loi ainsi que des mesures de contrôle pour assurer la protection et la sécurité des données du Client, même dans le cas de services auxiliaires externalisés.

(2) Le Prestataire peut notamment recourir aux services de sociétés affiliées ou d'autres prestataires, en tant que sous-traitants secondaires, pour remplir ses obligations en vertu du présent Accord. Le Prestataire tiendra à jour une liste des sous-traitants secondaires utilisés dans le cadre de tous les services, y compris le nom du sous-traitant secondaire et la finalité de son traitement. Le Client peut recevoir des notifications de nouveaux sous-traitants secondaires en envoyant un email à privacy@ungerboeck.com avec le sujet

« Subscribe » et une fois inscrit de cette manière, le Client recevra une notification de nouveaux sous-traitants secondaires avant que ces sous-traitants secondaires ne soient autorisés à traiter les données à caractère personnel pour le compte du Prestataire. Le Client peut raisonnablement s'opposer au recours par le Prestataire d'un nouveau sous-traitant secondaire en le notifiant par écrit au Prestataire dans les 14 jours suivant la réception de l'avis d'intention d'autoriser à l'adresse privacy@ungerboeck.com. Cet avis doit expliquer les motifs raisonnables d'objection (par exemple si le recours à ce sous-traitant secondaire violerait les lois applicables ou affaiblirait les protections des données à caractère personnel applicables). Le Prestataire fera des efforts commercialement raisonnables pour résoudre l'objection du Client.

(3) Le Prestataire ne transfère aucune donnée à caractère personnel (et ne permet pas à ses sous-traitants secondaires de transférer des données à caractère personnel) sans le consentement préalable du Client. Le Prestataire comprend que le Client doit approuver et être en mesure de prouver le fait qu'une protection adéquate des données à caractère personnel existera après le transfert, en utilisant des contrats qui offrent des garanties suffisantes (telles que des clauses contractuelles standard), à moins qu'une autre base juridique pour le transfert existe. Le Client consent par la présente à ce que le Prestataire transfère des données à caractère personnel aux sous-traitants secondaires décrits dans la présente section 6. En outre, le Client comprend, reconnaît et accepte que le Prestataire est (et ses sous-traitants peuvent être) basé aux Etats-Unis, au Royaume-Uni, en Australie, en Nouvelle-Zélande ou en Inde et que le Prestataire fournit (et les sous-traitants peuvent fournir) des Services à partir de ces pays, et le Client consent par la présente au transfert de données à caractère personnel vers ces pays pour traitement par le Prestataire et ses sous-traitants secondaires conformément au présent Accord. Le Client approuve par la présente le mandat des sous-traitants secondaires énumérés à l'**Annexe 2**.

7. Droits de contrôle du Client

(1) Le Client a le droit, en concertation avec le Prestataire, d'effectuer ou de faire effectuer des contrôles par des inspecteurs à désigner dans des cas individuels en envoyant un e-mail à privacy@ungerboeck.com.

(2) Après réception d'une telle demande, les parties discuteront et conviendront à l'avance de la portée, de la date de début et de la durée raisonnables de l'audit, ainsi que de tout contrôle de sécurité et de confidentialité applicable qui pourrait être requis. Le Prestataire peut facturer des honoraires (sur la base des coûts raisonnables du Prestataire) pour un tel audit. Le Prestataire fournira au Client des détails supplémentaires sur ces frais, y compris la base de leur calcul, avant l'audit. En outre, le Client sera responsable de tous les frais facturés par tout auditeur tiers désigné par le Client pour cet audit.

8. Notification des violations par le Prestataire

(1) Le Prestataire aide le Client à se conformer aux obligations énoncées aux articles 32 à 36 du RGPD concernant la sécurité des données à caractère personnel, les obligations de notification des violations de données, les évaluations d'impact sur la protection des données et les consultations préalables. Il s'agit notamment de ce qui suit :

a) assurer un niveau de protection approprié par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des finalités du traitement, ainsi que de la probabilité et de la gravité prévues d'une violation potentielle de la sécurité, et permettre la détection rapide des violations
b) L'obligation de notifier les violations de données à caractère personnel à l'autorité contractuelle sans délai excessif
c) L'obligation d'assister l'autorité contractuelle dans son devoir d'informer la personne concernée et, dans ce contexte, de lui fournir toutes les informations pertinentes sans délai excessif.
d) Le soutien au Client pour son évaluation d'impact sur la protection des données.
e) Le soutien au Client dans le cadre des consultations préalables avec l'autorité de contrôle.

(2) Le Prestataire peut demander une rémunération raisonnable pour les services de soutien qui ne figurent pas dans la description du service ou qui ne sont pas dus à une faute du Prestataire.

9. Autorité du Client pour émettre des instructions

(1) Le Client a le droit de donner à tout moment des instructions au Prestataire concernant le type, la portée et la procédure du traitement des données. Les instructions du Client sont initialement stipulées dans les Contrats de service et peuvent ensuite être modifiées, complétées ou remplacées par les parties dans un avenant.

(2) Les règlements concernant la rémunération éventuelle des dépenses supplémentaires encourues par le Prestataire en raison d'instructions supplémentaires du Client ne sont pas affectés.

(3) Le Prestataire s'engage à informer le Client sans délai s'il estime qu'une instruction viole les règles de protection des données ou s'il n'est pas en mesure de s'y conformer. Le Prestataire a le droit de suspendre l'exécution de l'instruction correspondante jusqu'à ce qu'elle soit confirmée ou modifiée par le Client ou le Client peut suspendre son transfert de données à caractère personnel au Prestataire et/ou le cas échéant résilier son Contrat de service avec le Prestataire (conformément aux termes du Contrat de service).

10. Suppression et restitution des données à caractère personnel

(1) Aucune copie ou duplication des données ne doit être effectuée à l'insu du Client. Font exception à cette règle les copies de sauvegarde, dans la mesure où elles sont nécessaires pour garantir le traitement correct des données, ainsi que les données requises pour respecter les obligations légales de conservation.

(2) Après l'achèvement des travaux convenus contractuellement ou plus tôt sur demande du Client, au plus tard à la fin du contrat de service, le Prestataire doit remettre au Client tous les documents qui sont entrés en sa possession, les résultats de traitement et d'utilisation créés, ainsi que les fichiers de données qui sont liés à la relation contractuelle, ou les détruire conformément aux exigences de la protection des données après accord préalable du Client.

(3) La documentation qui sert de preuve du traitement correct des données conformément à l'Accord doit être par le Prestataire au-delà de la fin du contrat de service, conformément aux périodes de conservation respectives. Le Prestataire peut la remettre au Client à la fin du contrat de service, afin de se décharger.

(4) Le Prestataire peut conserver les données à caractère personnel traitées dans le cadre de la commande au-delà de la fin du contrat de service, si et dans la mesure où le Prestataire est soumis à une obligation légale de conserver les données. Dans ce cas, les données ne peuvent être traitées que dans le but d'appliquer les obligations légales de conservation respectives. Après l'expiration de l'obligation de conservation, les données doivent être immédiatement effacées et, sur demande, il sera nécessaire de certifier au Client que cela a été fait.

11. **ADDENDUM CCS DE L'UE ET DU RU**

(1) Si le Prestataire traite des données à caractère personnel couvertes par l'EEE, la Suisse ou le Royaume-Uni dans un pays situé hors de l'EEE, de la Suisse ou du Royaume-Uni qui n'a pas reçu de décision d'adéquation de la part des autorités compétentes, ce transfert aura lieu sur la base des CCS de l'UE et/ou de l'Addendum du Royaume-Uni, selon le cas. Dans le cas où les CCS de l'UE et/ou l'Addendum du Royaume-Uni ne sont pas applicables, les parties conviennent de travailler de bonne foi sans délai excessif pour mettre en œuvre un mécanisme de transfert alternatif approprié autorisé par les Lois applicables sur la protection des données.

(2) Dans la mesure où le Prestataire traite des données à caractère personnel couvertes par les lois de protection des données de l'UE, le RGPD et/ou les lois de protection des données du Royaume-Uni, selon le cas, dans un pays qui n'a pas reçu de décision d'adéquation de la part de la Commission européenne ou des autorités suisses ou britanniques, selon le cas, les parties intègrent par les présentes les CCS de l'UE (pour les données à caractère personnel couvertes par les lois de protection des données de l'UE ou le RGPD, selon le cas) et l'Addendum du Royaume-Uni (pour les données à caractère personnel couvertes par les lois de protection des données du Royaume-Uni), par référence.

(3) Lorsque les CCS de l'UE s'appliquent, elles seront réputés s'appliquer comme suit :

- Le module 2 (du responsable du traitement au sous-traitant) s'appliquera lorsque le Client est un responsable du traitement de données à caractère personnel et que le Prestataire est un sous-traitant de données à caractère personnel, les CCS de l'UE seront réputés s'appliquer comme suit :
    - La clause 7 des CCS de l'UE, la « clause d'amarrage (facultative) », est réputée incorporée ;
    - dans la clause 9(a) des CCS de l'UE, les parties choisissent l'option 2, « autorisation écrite générale », avec un délai de quatorze (14) jours ;

- le libellé facultatif de la clause 11 des CCS de l'UE est réputé ne pas s'appliquer ;
- dans la clause 12, toute réclamation introduite en vertu des CCS de l'UE sera soumise aux conditions énoncées dans le Contrat de service. En aucun cas une partie ne doit limiter sa responsabilité à l'égard des droits des Personnes concernées en vertu des CCS de l'UE ;
- dans la clause 17 des CCS de l'UE, l'Exportateur de données et l'Importateur de données conviennent que les CCS de l'UE seront régis par le droit de la République fédérale d'Allemagne et choisissent l'option 1 à cet effet ;
- dans la clause 18 des CCS de l'UE, l'Exportateur de données et l'Importateur de données conviennent que tout litige sera résolu par les tribunaux de la République fédérale d'Allemagne ;
- Les annexes I.A, I.B, II et III des CCS de l'UE sont réputées complétées par les informations figurant aux annexes I et II du présent Accord, dont le contenu est convenu par les parties ; et
- aux fins de l'annexe I.C des CCS de l'UE, l'autorité de contrôle compétente est l'autorité de contrôle du pays où l'Exportateur de données est établi. Si l'Exportateur de données n'est pas établi dans l'EEE mais le Traitement est soumis au RGPD, l'autorité compétente est l'autorité de contrôle de la République fédérale d'Allemagne.

(4) Dans la mesure où les transferts de données à caractère personnel sont soumis au RGPD, les dispositions suivantes s'appliquent :

- Les références au RGPD doivent être comprises comme des références à la LPD et, une fois entré en vigueur, à la LPD révisée dans la mesure où les transferts de données à caractère personnel sont soumises à la LPD ou à la LPD révisée.
- Le terme « État membre » tel qu'il est utilisé dans les CCS de l'UE approuvées ne doit pas être interprété comme limitant la possibilité pour les Personnes concernées en Suisse d'intenter une action en justice pour faire valoir leurs droits dans leur lieu de résidence habituel (Suisse), conformément à la clause 18(c) des CCS de l'UE. Lorsque la LPD s'applique au Traitement, les CCS de l'UE protègent également les données des personnes morales, jusqu'à l'entrée en vigueur de la LPD révisée (la version promulguée le 25 septembre 2020, telle que modifiée).
- Aux fins de l'Annexe I.C des CCS de l'UE, lorsque le Client est l'Exportateur de données et que les données à caractère personnel transférées sont exclusivement soumises au RGPD, le Préposé fédéral suisse à la protection des données et à la transparence (le « PFPDT ») est l'Autorité de contrôle compétente. Lorsque les Données à caractère personnel transférées sont soumises à la fois à la LPD et au RGPD, une surveillance parallèle doit s'appliquer : pour la LPD (révisée), le PFPDT est l'Autorité de contrôle compétente dans la mesure où le transfert est régi par la LPD (révisée) ; et pour le RGPD, l'Autorité de contrôle compétente est (a) l'Autorité de contrôle du pays où l'Exportateur de données est établi si l'Exportateur de données est établi dans l'EEE, ou (b) l'Autorité de contrôle de l'Irlande si l'Exportateur de données n'est pas établi dans l'EEE.

(5) Lorsque l'Addendum du RU s'applique, il sera réputé s'appliquer comme suit :

- Le tableau 1 est réputé complété par les informations figurant à l'annexe I du présent Addendum, le cas échéant, dont le contenu est convenu par les parties ;
- Dans le tableau 2, les parties cochent la case suivante : « Les CCS de l'UE approuvés, y compris les informations de l'annexe et avec seulement les modules, clauses ou dispositions facultatives suivants des CCS de l'UE approuvés mis en vigueur aux fins du présent addendum », et le tableau d'accompagnement est réputé être complété selon les préférences des parties décrites dans la clause 11.4. Aux fins de la clause 9 de l'addendum du RU, la loi applicable est réputée être celle de l'Angleterre & Pays de Galles.

- Le tableau 3 est réputé complété par les informations figurant aux annexes I et II du présent Addendum, dont le contenu est convenu par les parties ;

- Dans le tableau 4, les parties conviennent que l'une ou l'autre des parties peut mettre fin à l'Addendum comme indiqué à la section 19 de l'Addendum du RU.

(6) Afin d'éviter tout doute, le présent Addendum aux CCS de l'UE/RU s'applique indépendamment à toutes les sociétés affiliées du Client dans l'EEE et au Royaume-Uni (lorsque la clause 1.6 s'applique) qui peuvent utiliser les services fournis par le Prestataire (tels que définis dans l'annexe aux présents CCS de l'UE, qui ont été incorporés au présent Accord). Aux fins de l'Addendum des CCS de l'UE et du RU, les sociétés affiliées du Client EEE et du Royaume-Uni (où la clause 11(5) s'applique) susmentionnées seront chacune considérées comme un Exportateur de données et le Prestataire sera considéré comme l'Importateur de données.

12. Changements dans les politiques

(1) Le Prestataire communiquera toutes les modifications apportées à l'Accord (y compris les raisons qui justifient les modifications) ou à la liste des membres du groupe liés par l'Accord :

- aux membres du groupe du Prestataire liés par l'Accord, par un avis écrit (qui peut inclure un e-mail ou un affichage sur un intranet interne accessible à tous les membres du groupe) ; et
- au Client et aux personnes qui bénéficient de l'Accord par une publication en ligne sur le site Internet du Prestataire (et, si les modifications sont importantes par nature, le Prestataire doit également communiquer activement les modifications importantes au Client avant qu'elles ne prennent effet, conformément au paragraphe 12.3 ci-dessous).

(2) Si le Prestataire apporte des changements importants à l'Accord ou à la liste des membres du groupe liés par l'Accord qui affectent le niveau de protection offert par l'Accord ou qui affectent autrement l'Accord de manière significative, le Prestataire signalera rapidement ces changements (y compris les raisons qui les justifient) à tous les autres membres du groupe du Prestataire. Si une proposition de modification de l'Accord affecte sensiblement le traitement par le Prestataire des données à caractère personnel pour le compte d'un Client, le Prestataire doit également :

- communiquer activement la modification proposée au Client concerné avant qu'elle ne prenne effet, et avec un préavis d'au moins 14 jours pour permettre au Client concerné de soulever des objections ; et
- le Client peut alors suspendre le transfert des données à caractère personnel au Prestataire et/ou le cas échéant résilier le Contrat de service, conformément aux termes du Contrat de service avec le Prestataire.

13. DÉFINITIONS

(1) Lois applicables en matière de protection des données : désigne, la ou les lois suivantes en matière de protection des données, selon le cas, y compris tous les amendements, modifications et révisions ultérieurs : (i) le règlement de l'UE 2016/679 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » (RGPD) et toutes les lois nationales applicables mises en œuvre par les pays membres de l'EEE ; (ii) la loi fédérale suisse du 19 juin 1992 sur la protection des données (telle qu'elle peut être modifiée ou remplacée) ; et (iii) la loi de 2018 sur la protection des données (c. 12) du Royaume-Uni.

(2) Lois de l'UE sur la protection des données : désigne la législation de l'Union européenne (« UE ») sur la protection des personnes concernées par le traitement des données à caractère personnel et sur la libre circulation de ces données, y compris, en particulier, le RGPD (ainsi que la législation nationale associée) et la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE, et telle qu'elle peut être à nouveau modifiée ou remplacée de temps à autre, dans les pays qui sont membres de l'UE ou de l'EEE, et toute autre législation relative à la protection des données ou de la vie privée (y compris toute législation substantiellement similaire qui remplace le RGPD ou la législation nationale associée), en vigueur de temps à autre dans les pays qui sont membres de l'UE ou de l'EEE, selon le cas.

(3) CCS de l'UE : désigne les clauses contractuelles standard pour le transfert de données à caractère personnel, conformément au droit applicable en matière de protection des données, à des responsables du traitement et des sous-traitants établis dans des pays tiers, approuvées par la Commission européenne de

temps à autre, dont la version approuvée en vigueur à la date de signature du présent accord est celle figurant dans la décision 2021/914 de la Commission européenne du 4 juin 2021, comme ces clauses contractuelles standard sont disponibles sur https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en et telles qu'elles peuvent être modifiées ou remplacées par la Commission européenne de temps à autre.

(4) LPD : désigne la loi fédérale suisse sur la protection des données du 19 juin 1992 (RS 235.1) et les ordonnances RS 235.11 et RS 235.13, telles que modifiées et applicables, et, une fois entrée en vigueur le 1er septembre 2023 (ou toute autre date fixée par le droit suisse), la version révisée de la LPD du 25 septembre 2020, telle que modifiée et applicable.

(5) données à caractère personnel : désigne toute information relative, directement ou indirectement, à une personne physique identifiée ou identifiable qui est traitée par le Prestataire ou les sous-traitants secondaires dans le cadre du Contrat de service. Sans limiter la généralité de ce qui précède, les « données à caractère personnel » comprennent, sans s'y limiter, les « informations personnelles », les « données personnelles » et les termes similaires tels que définis par les Lois applicables en matière de protection des données, dans la mesure où ces données sont traitées dans le cadre de l'Accord.

(6) Groupe de sous-traitants : désigne le Prestataire et toute entité qui contrôle, est contrôlée par, ou est sous contrôle commun avec le Prestataire.

(7) Services : désigne les fonctions que le Prestataire exécute pour le compte du Client, comme indiqué dans le Contrat de service.

(8) Addendum du RU : désigne l'Addendum britannique sur le transfert international de données aux clauses contractuelles types de la Commission européenne, disponible à l'adresse https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, tel qu'adopté, modifié ou mis à jour par le bureau du commissaire à l'information, le Parlement ou le secrétaire d'État du Royaume-Uni.

(9) Lois du Royaume-Uni sur la protection des données : désigne la loi sur la protection des données de 2018 (DPA 2018), telle que modifiée et le RGPD de l'UE, tel qu'incorporé dans le droit britannique en tant que RGPD du RU, tel que modifié, et toute autre loi du Royaume-Uni applicable à la protection des données, ou les codes de conduite réglementaires ou autres orientations qui peuvent être publiés de temps à autre.

(10) Tous les autres termes commençant par une majuscule qui ne sont pas définis dans les présentes auront la signification prévue par l'Accord ou les Lois applicables en matière de protection des données. Une référence à un terme ou à une section des Lois applicables en matière de protection des données désigne la version modifiée.

EN FOI DE QUOI, les parties ont signé le présent Accord par leurs représentants dûment autorisés, avec effet à la date du Contrat de service.

Annexe 1

La présente annexe décrit les types de données transférées par les Exportateurs de données et les finalités pour lesquelles ces données peuvent être traitées par les Sous-traitants/Importateurs de données. La présente annexe est soumise aux conditions de l'Accord. Les termes en majuscules qui ne sont pas définis dans la présente annexe ont le sens qui leur est attribué dans l'Accord ou dans les Lois applicables en matière de protection des données.

Exportateur de données :

- L'Exportateur de données est : le Client comme indiqué dans le Contrat de service.
- Nom (nom légal complet) : Tel qu'indiqué dans le Contrat de service.
- Nom commercial (si différent) : Comme indiqué dans le Contrat de service.
- Adresse : Tel qu'indiqué dans le Contrat de service.
- Numéro d'enregistrement officiel (le cas échéant) (numéro d'entreprise ou identifiant similaire) : Comme prévu dans le Contrat de service.
- Nom, fonction et coordonnées de la personne de contact : Tel qu'indiqué dans le Contrat de service.
- Activités relatives aux données transférées en vertu des présentes clauses : Comme prévu dans le présent Accord et le Contrat de service.
- Signature et date : Signé le même jour que l'Accord, qui sera considéré comme signé à la date de son acceptation par signature via DocuSign.
- Rôle (responsable du traitement/sous-traitant) : Lorsque le Client détermine les finalités et les moyens du traitement des données à caractère personnel, son rôle est celui de responsable du traitement. Lorsque le Client agit pour le compte et selon les instructions d'un responsable du traitement, son rôle est celui de sous-traitant.

Importateurs de données :

- L'importateur de données est : Ungerboeck Systems International GmbH, ou comme prévu autrement dans le bloc de signature de l'Accord.
- Nom (nom légal complet) : Ungerboeck Systems International GmbH
- Adresse : Kaiserstrasse 72, 76133 Karlsruhe, Allemagne
- Numéro d'enregistrement officiel (le cas échéant) (numéro d'entreprise ou identifiant similaire) : Tel qu'indiqué dans le Contrat de service.
- Nom, fonction et coordonnées de la personne de contact :
    - M. Casey Jessmon, responsable de la sécurité des informations et de la protection des données (au niveau mondial) ; privacy@ungerboeck.com
    - Mme Dorothee Schaeufele, coordinatrice de la protection des données (EMEA) ; privacy@ungerboeck.com
- Activités relatives aux données transférées en vertu des présentes clauses : Traitement tel que précisé dans l'Accord, le Contrat de service et selon les instructions écrites au nom du Client.
- Signature et date : Signé le même jour que l'Accord, qui sera considéré comme signé à la date de son acceptation par signature via DocuSign.
- Rôle (responsable du traitement/sous-traitant) : Sous-traitant

Catégories de personnes concernées. Cette rubrique sera réputée remplie comme décrit dans l'Accord.

Type de données à caractère personnel. Cette rubrique sera réputée remplie comme décrit dans l'Accord.

Données à caractère personnel sensibles. Cette rubrique sera réputée remplie comme décrit dans l'Accord.

Fréquence du traitement : Ce traitement aura lieu de manière continue.

Nature et finalité du traitement : Le Prestataire doit recueillir, traiter et utiliser toutes les données à caractère personnel uniquement aux fins du traitement tel que précisé dans l'Accord et conformément aux instructions écrites données pour le compte du Client.

Durée. La durée du traitement des données dépend de la durée du Contrat de service.

Période de conservation. La période de conservation des données à caractère personnel correspond à la durée de l'Accord ou à une autre période décrite dans celui-ci.

Sous-traitants. Cette rubrique sera réputée complétée comme décrit dans l'Accord, Annexe II, et modifiée de temps à autre.

Mesures techniques et organisationnelles

Pour plus d'informations sur les mesures de sécurité dans l'environnement en cloud d'Ungerboeck, veuillez consulter les pages suivantes. Pour plus d'informations sur la protection de la vie privée chez Ungerboeck Systems International GmbH, veuillez consulter notre politique de confidentialité à l'adresse suivante : https://ungerboeck.com/privacy-policy. Pour plus d'informations sur les mesures de sécurité du prestataire de services en cloud d'Ungerboeck, Amazon Web Services, veuillez consulter le site Web d'AWS à l'adresse suivante : https://aws.amazon.com/de/compliance/gdpr-center/.

A. Mesures technico-organisationnelles sur les sites d'Ungerboeck.

1. Confidentialité (Art. 32 para. 1 lit. b du RGPD)

- Gestion et contrôle des accès
  - L'entrée principale est verrouillée. Les personnes autorisées à accéder aux locaux sont en possession soit d'une carte à puce, soit d'une clé. L'émission des cartes ou clés est centralisée, y compris l'enregistrement.
  - Surveillance vidéo à l'entrée principale des locaux.
  - Les pièces à protéger (par exemple, la salle des serveurs) sont toujours fermées à clé. Seuls les employés qui ont besoin d'accéder à ces pièces pour leurs tâches professionnelles y ont accès.
- Gestion électronique des accès
  - Lorsqu'ils accèdent au système CRM, les utilisateurs s'identifient à l'aide de leur identifiant d'utilisateur et de leur mot de passe.
  - La connexion WiFi disponible pour les locaux est protégée par un mot de passe.
  - Une erreur déclenchée par une autorisation incorrecte au système entraînera le blocage de l'accès au système après un nombre défini de tentatives.
  - Les identifiants et les mots de passe sont créés conformément à la politique d'Ungerboeck en matière de mots de passe (caractères spéciaux, longueur minimale et changement régulier des mots de passe).
  - Des règles s'appliquent aux employés travaillant à domicile, sur des appareils mobiles ou sur le site du client.
  - Des politiques et des concepts de sécurité pour les mesures décrites ci-dessous sont en place et sont revus et mis à jour chaque année.
- Contrôle de la séparation
  - Ungerboeck applique les principes de la séparation des tâches et du principe du moindre privilège (le moins de droits possible). Le respect de ces règles est assuré, entre autres, par des demandes et examens d'accès.
  - Les environnements de développement et de production sont séparés, et les autorisations sont accordées par environnement.
- Pseudonymisation (Art. 32 para. 1 lit. a du RGPD ; Art. 25 para. 1 du RGPD).
  - La pseudonymisation des clients est possible sur demande auprès du système CRM et est effectuée manuellement si nécessaire. Dans le cas contraire, les données peuvent être bloquées ou rendues anonymes.
  - Si Ungerboeck utilise des données agrégées à des fins internes, ces informations sont pseudonymisées.
  - Il existe des règles et des concepts de sécurité pour les mesures décrites ci-dessous, et ceux-ci sont revus et mis à jour chaque année.

2. Intégrité (Art. 32 para. 1 lit. b DSGVO)

- Contrôle du transfert
  - Il existe des méthodes autorisées pour le transfert de données (MediaShuttle, SFTP). Les procédures sont consignées par écrit.
  - La demande et la transmission de copies de la base de données sont consignées dans le ticket d'assistance correspondant.
  - L'accès à Internet est protégé contre l'écoute clandestine par des mécanismes de chiffrement VPN et TSL/SSL. L'intégrité des fichiers transférés est vérifiée régulièrement et de manière aléatoire.
  - Les e-mails contenant des informations très sensibles sont chiffrées (chiffrement des e-mails dans Office 365).
  - Des politiques et des concepts de sécurité pour les mesures décrites ci-dessous sont mis en place et sont revus et mis à jour chaque année.
- Contrôle des entrées
  - La saisie et la modification des données de base sont consignées dans des fichiers journaux dans le système CRM.
  - Toutes les entrées sont résumés de manière centralisée via un outil interne SIEM.
  - L'accès au système CRM est contrôlé par une configuration personnalisée des paramètres du logiciel (rôles des utilisateurs, droits d'accès, chiffrement ou masquage des champs, etc.)
  - Des politiques et des concepts de sécurité concernant les mesures décrites ci-dessous sont en place et sont revus et mis à jour chaque année.

3. Disponibilité et résilience (article 32, paragraphe 1, point b) du RGPD)

- Contrôle des disponibilités
  - Une protection antivirus à jour est installée. Des systèmes de pare-feu sont utilisés.
  - Tests d'intégrité réguliers et aléatoires sur les sauvegardes des serveurs locaux.
- Possibilité de récupération rapide (article 32, paragraphe 1, point c) du RGPD).
  - Le concept de sauvegarde des données à caractère personnel pour les serveurs locaux a été mis en place.
  - Un plan de crise mondial (« plan de reprise après sinistre mondial ») est en place, couvrant tous les bureaux et centres de données. Les RTO et RPO sont consignés dans notre plan de continuité des activités et de reprise après sinistre.
  - Des politiques et des concepts de sécurité concernant les mesures décrites ci-dessous sont en place et sont revus et mis à jour chaque année.

4. Procédures de révision, d'appréciation et d'évaluation régulières (art. 32 (1) (d) du RGPD ; art. 25 (1) du RGPD).

- Gestion de la protection des données à caractère personnel
  - Formation régulière à la protection des données pour les employés du Prestataire.
  - Formation régulière des employés du Prestataire à la cybersécurité
  - Manuel interne de l'employé composé de politiques internes de protection des données et d'informatique sur les mesures de sécurité de l'information et de protection des données dans l'organisation EMEA, y compris les politiques pour les employés travaillant à domicile, sur des appareils mobiles ou directement chez le Client.
  - En plus du responsable externe de la protection des données, un coordinateur interne de la protection des données a été désigné pour l'organisation EMEA.
  - Formation d'une équipe mondiale de protection des données pour renforcer la sécurité informatique et la gestion de la protection des données à l'échelle de l'entreprise.
- Gestion de la réponse aux incidents
  - Le plan de réponse aux incidents est consigné par écrit et revu chaque année.

- Le plan de réponse aux incidents est testé au moins une fois par an dans le cadre des tests BC/DR.
- Nous avons une équipe de réponse aux incidents qui est consciente de ses responsabilités.
- Des directives et des concepts de sécurité pour les mesures décrites ci-dessous sont mis en place, et sont revus et mis à jour chaque année.

- Paramètres par défaut respectueux de la protection des données à caractère personnel (art. 25, al. 2 du RGPD)
  - Ungerboeck Systems International GmbH soutient les solutions logicielles conformes au RGPD grâce à la « protection des données par la conception technologique » et à la « protection des données par des paramètres par défaut respectueux de la vie privée ». Un niveau approprié de protection des données peut être atteint par les paramètres de la solution logicielle et par la configuration individuelle des paramètres en fonction de la fonction respective (par exemple, par des droits d'accès, le chiffrement ou le masquage des champs, etc.)
- Obligations contractuelles
  - De plus amples détails sur les obligations contractuelles sont contenus dans le Contrat de service respectif avec le Client.
  - L'obligation de suivre les instructions, les obligations de notification et les droits d'audit sont réglementés dans le présent Accord.
  - Les employés du Client qui peuvent donner des instructions au Prestataire sont désignés par la direction du Client dans le Contrat de service.

B. Mesures technico-organisationnelles dans les environnements en cloud d'Ungerboeck

Pour les environnements en cloud, Ungerboeck a recours au prestataire de cloud leader du secteur, Amazon Web Services (« AWS »), pour une évolutivité et une fiabilité maximale des environnements en cloud ainsi qu'une sauvegarde hors site et une reprise après sinistre.

« Dans le cadre du modèle de responsabilité partagée d'AWS, AWS fournit une infrastructure mondiale sécurisée et des services de base de calcul, de stockage, de mise en réseau et de base de données, ainsi que des services de niveau supérieur. AWS propose un ensemble de services et de fonctionnalités de sécurité que les clients d'AWS (Ungerboeck) peuvent utiliser pour sécuriser leurs actifs. Les clients d'AWS (Ungerboeck) sont responsables de la protection de la confidentialité, de l'intégrité et de la disponibilité de leurs données dans le cloud, ainsi que du respect des exigences commerciales particulières en matière de protection des données. »
(Source : Amazon Web Services - Security Best Practices Whitepaper)

« Amazon Web Services (AWS) exploite, gère et contrôle les composants depuis le système d'exploitation hôte et la couche de virtualisation, jusqu'à la sécurité physique des installations dans lesquelles les services AWS fonctionnent. Le client (Ungerboeck) est responsable de la gestion du système d'exploitation invité (y compris les mises à jour et les correctifs de sécurité du système d'exploitation invité) et des logiciels d'application associés, ainsi que de la configuration du pare-feu du groupe de sécurité fourni par AWS et d'autres fonctions liées à la sécurité. »
(Source : Amazon Web Services - Livre blanc sur la protection des données dans l'UE)

Veuillez noter : Les mesures décrites ci-dessous sont susceptibles d'être modifiées en fonction de la disponibilité des services AWS et de l'état de l'art. La liste suivante ne contient pas l'intégralité des mesures techniques et organisationnelles prises par le Prestataire, mais vise uniquement à donner au Client un aperçu des mesures prises. Des détails supplémentaires sur l'utilisation d'Amazon Web Services par Ungerboeck et les contrôles de sécurité sont disponibles sur demande.

1. Infrastructure AWS :
   - Pour plus d'informations sur les mesures de sécurité et de conformité du prestataire de services en cloud d'Ungerboeck, Amazon Web Services, veuillez consulter le Site Web d'AWS.

2. Mesures de sécurité dans l'environnement Ungerboeck en cloud :
   - Les bases de données destinées aux clients de l'UE sont hébergées dans l'UE.

- Ungerboeck utilise plusieurs couches de pare-feu et d'outils de sécurité réseau pour protéger les données.
- Tous les points d'accès accessibles au public sont isolés des composants centraux par des listes de contrôle d'accès. Seuls les ports entrants et sortants nécessaires des environnements hébergés sont ouverts.
- L'accès aux applications est contrôlé par une authentification LDAP intégrée et tous les points d'accès sont protégés par chiffrement SSL/TSL.
- L'accès via les systèmes IP est déconnecté au bout d'un certain temps lorsqu'il n'est pas utilisé, ce qui est appelé le délai d'expiration de la session. Les sessions du serveur Web sont achevées par le serveur après une durée définie.
- Un logiciel antivirus et un anti-malware sont déployés sur tous les serveurs, mis à jour quotidiennement et analysés régulièrement.
- Tous les serveurs sont protégés par un système de prévention des intrusions (IPS) à la pointe du secteur qui analyse le trafic réseau et identifie les méthodes permettant de détecter les fichiers malveillants sur le réseau.
- Les données sensibles, telles que les informations relatives aux mots de passe et aux cartes de crédit dans la base de données, sont chiffrées à l'aide de la méthode AES 256 bits à clé partagée.
- La transmission des données en entrée et en sortie de l'application est protégée par chiffrement TLS 1.2 ou supérieur.
- Les données du Client sont logiquement séparées et sécurisées sur un schéma de base de données et une instance d'application non partagés.
- Les services et applications inutilisés sont supprimés ou désactivés dans la mesure du possible.
- Les dernières mises à jour et les correctifs de sécurité sont installés dans les systèmes lors de la maintenance régulière.
- L'authentification multifactorielle est requise pour accéder aux consoles de gestion, lorsqu'elle est disponible.
- L'accès aux composants et aux données du système est limité aux personnes dont le travail nécessite un tel accès, ainsi qu'aux privilèges d'accès minimaux nécessaires pour effectuer les tâches correspondantes.
- Ungerboeck applique des politiques de mots de passe complexes, comme l'exige la conformité PCI-DSS.
- Ungerboeck utilise des services de sécurité et de conformité entièrement administrés et basés sur le cloud computing pour surveiller, détecter et répondre immédiatement aux incidents de sécurité indésirables.
- Ungerboeck dispose d'une surveillance, d'une analyse et d'un examen des journaux 24 heures sur 24 et 7 jours sur 7, afin de recueillir, d'agréger et de rechercher les données des journaux provenant des actifs du cloud, des serveurs, des applications, de la sécurité et du réseau dans le cloud Ungerboeck.
- Ungerboeck dispose d'un vSOC 24 heures sur 24, 7 jours sur 7, qui assure une surveillance continue de tous les systèmes de production.
- Ungerboeck assure une surveillance 24 heures sur 24 et 7 jours sur 7 des systèmes de production en utilisant des pratiques standard du secteur qui alertent le personnel responsable d'Ungerboeck sur les performances du système et l'utilisation des ressources.
- Ungerboeck utilise une combinaison de technologies telles que l'équilibrage des charges, le farming des serveurs, le mirroring et les plans de maintenance des bases de données pour obtenir une haute disponibilité, une redondance et un basculement.

Annexe 2 - Sous-traitant

Sous-traitant / Pays	Services
Amazon Web Services, Inc. (« AWS »), États-Unis d'Amérique	Services de cloud (hébergement) de la base de données permettant d'utiliser la solution logicielle, ainsi que des bases de données de test dans le cloud pour les clients ayant un plan de réussite client approprié. Utilisation des centres de données AWS en Europe.
Affiliés d'Ungerboeck • Ungerboeck Systems International, LLC ; États-Unis d'Amérique et Nouvelle-Zélande • Ungerboeck Software International, Pty Ltd ; Australie et Nouvelle-Zélande • Oletha Pyt Ltd ; Inde • Ungerboeck Systems International GmbH ; Royaume-Uni	Soutien à l'exécution du contrat : • Services de soutien (« Follow-the-Sun ») et services techniques ; • Programme alpha/ beta/ adoption précoce ; • Sessions web et réunions en ligne ; • Services à distance ou sur site ; • Surveillance technique de l'environnement en cloud (surveillance de la disponibilité et des performances et dépannage en cas de dysfonctionnement ou de panne en dehors des heures de bureau habituelles du Client) ; • S'applique uniquement aux clients non hébergés (sur site) : Pour les tests de soutien, il peut être nécessaire de tester avec les données réelles du Client, afin de pouvoir reproduire une erreur. À cette fin, il est demandé au Client de fournir une copie de sa base de données via MediaShuttle (le Client peut également télécharger la copie de la base de données sur le serveur FTP sécurisé de l'UE).
Zendesk, Inc., États-Unis d'Amérique	Centre d'assistance et base de connaissances Système de tickets pour le traitement des tickets de support pour le logiciel Ungerboeck, mise à disposition de la plateforme, les serveurs sont situés aux États-Unis.
LogMeIn, Inc., États-Unis d'Amérique	GoToMeeting, GoToWebinar
NITOR Infotech Pvt. Ltd, Inde	Développements techniques, tests de qualité
Altaa Vistaa Business Solutions Pvt Ltd, Inde	Services de réussite client, autres services contractuels (principalement affectés aux projets anglophones, mais pas seulement)
OuiYou Lyon, France	Formations techniques et services similaires pour les clients francophones
Datajust B.V. (Storecove), Pays-Bas	Intégration de la facturation électronique dans le logiciel Ungerboeck (PEPPOL) / Accesspoint en tant que service
Stripe, Inc, États-Unis d'Amérique	Lors de la souscription des services proposés (Paiements Ungerboeck / Services de traitement des paiements par le logiciel Ungerboeck)
Rossum Czech Republic s.r.o., République tchèque	Lors de la souscription des services proposés (automatisation des comptes créditeurs par le logiciel Ungerboeck)
DocuSign Inc, États-Unis d'Amérique	Lors de la souscription des services proposés (intégration de la signature électronique dans le logiciel Ungerboeck, y compris, le cas échéant, la fourniture d'enveloppes)
Jotform, Inc, États-Unis d'Amérique	Lors de la souscription des services proposés (mise en place de formulaires en ligne)
Twilio Inc, États-Unis d'Amérique	À la demande du Client ou après approbation de la proposition de solution personnalisée (SendGrid Emails dans Ungerboeck Software)
Signiant Inc, États-Unis d'Amérique	Utilisation du service MediaShuttle pour télécharger et transférer des copies de bases de données dans l'environnement en cloud d'Ungerboeck ; utilisé par les clients sur site à la demande d'Ungerboeck.

Dynatrace, LLC, États-Unis d'Amérique	Plateforme tierce de surveillance et de consignation qu'Ungerboeck utilise pour ingérer, analyser, interroger et effectuer des analyses sur les journaux des applications et de l'infrastructure d'Ungerboeck.
Azure (Microsoft), États-Unis d'Amérique	Prestataire de services en cloud pour l'hébergement de projets de services partagés dans l'ensemble du portefeuille de produits d'Ungerboeck.
Okta, Inc, États-Unis d'Amérique	Fournisseur d'identité
AC PM LLC (Postmark), États-Unis d'Amérique	Prestataire de services de courrier électronique
Spreedly, Inc, États-Unis d'Amérique	Plateforme de traitement des paiements