Annexe Traitement des données personnelles aux Conditions générales

Accord

entre

le client

– ci-après dénommé le «Client» –

et

bexio SA

Alte Jonastrasse 24

8640 Rapperswil

Suisse

– ci-après dénommé le «Fournisseur» –

relatif au traitement des données personnelles.

Préambule

Cette annexe précise les obligations des parties relatives à la protection des données découlant du contrat conclu entre les parties (Conditions générales du Fournisseur). Elle s'applique à toutes les activités liées au contrat dans le cadre desquelles les données personnelles du Client (ci-après dénommées «Données») sont traitées par les employés du Fournisseur ou un sous-traitant mandaté par ce dernier.

1 Objet, durée et spécification du traitement des données personnelles

(1) Les modalités relatives au service fourni par le Fournisseur sont détaillées dans le contrat conclu entre le Fournisseur et le Client (ci-après dénommé «Contrat»); ce Contrat comprend les Conditions générales du Fournisseur.

(2) L'objet et la durée de la commande sont spécifiés dans le Contrat, de même que la nature et l'objectif du traitement, sauf disposition contraire de l'addendum A.

(3) La durée de validité de cette annexe est déterminée par la durée du Contrat, pour autant qu'aucune obligation supplémentaire ne découle des dispositions de cette annexe.

2 Champ d'application et responsabilité

(1) Le Fournisseur traite les données décrites dans l'addendum A pour le compte du Client aux fins et dans la mesure spécifiées dans celui-ci. Ceci inclut les activités spécifiées dans le Contrat.

(2) Dans le cadre du présent Contrat, le Client est seul responsable du respect des dispositions légales en matière de protection des données, et notamment de la légalité du transfert des données au Fournisseur ainsi que de la légalité du traitement des données.

(3) Les instructions sont initialement spécifiées dans le Contrat et peuvent être modifiées, complétées ou remplacées ultérieurement par le Client au moyen d'instructions additionnelles, sous forme écrite ou électronique (sous forme textuelle), adressées au service désigné par le Fournisseur (instruction individuelle). Toute instruction non prévue dans le contrat sera traitée comme une demande de modification de prestation. Les instructions orales doivent être formulées par écrit ou sous forme textuelle dans les plus brefs délais par le client.

3 Obligations du Fournisseur

(1) Le Fournisseur ne peut traiter les données des personnes concernées que dans le cadre de la commande et des instructions du Client, sauf exceptions prévues par la loi. Le Fournisseur informe immédiatement le Client si, selon lui, une instruction constitue une violation aux lois applicables. Le Fournisseur peut suspendre la mise en œuvre de l'instruction jusqu'à ce qu'elle ait été confirmée ou modifiée par le Client.

(2) Dans son domaine de responsabilité, le Fournisseur adaptera l'organisation interne de l'entreprise de manière à répondre aux exigences spécifiques de la protection des données. Il prendra des mesures techniques et organisationnelles conformes aux exigences légales pour assurer la protection adéquate des données du Client. Le Fournisseur doit prendre des mesures techniques et organisationnelles pour assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement des données sur une base permanente. Ces mesures techniques et organisationnelles sont connues du Client, qui a la responsabilité de s'assurer qu'elles offrent un niveau de protection adéquat pour les risques des données à traiter.

(3) Les mesures prises par le Fournisseur sont décrites plus en détail dans l'addendum B. Les mesures techniques et organisationnelles font l'objet de progrès techniques et de développements ultérieurs. À cet égard, le Fournisseur est autorisé à mettre en œuvre d'autres mesures adéquates, à condition que le niveau de sécurité apporté par ces mesures ne soit pas être inférieur au niveau antérieur. Tout changement important doit être documenté.

(4) S'il en est ainsi convenu, le Fournisseur assiste le Client dans la mesure de ses possibilités en cas de demande de renseignements et de réclamation des personnes concernées et dans le cadre du respect des obligations relatives à la protection des données.

(5) Le Fournisseur garantit que les employés et les autres personnes travaillant pour le Fournisseur impliqués dans le traitement des données du Client ne sont pas autorisés à traiter les données en dehors de l'instruction. En outre, le Fournisseur garantit que les personnes autorisées à traiter les données personnelles sont liées par une obligation légale de confidentialité ou de secret professionnel. L'obligation de confidentialité ou de secret professionnel subsiste après l'exécution de la commande.

(6) Lorsqu'une violation de données à caractère personnel est constatée par le Fournisseur, il en informe immédiatement le Client. Le Fournisseur prend les mesures nécessaires pour sécuriser les données et minimiser les éventuelles conséquences négatives pour les personnes concernées; il en informe le Client dans les plus brefs délais.

(7) Le Fournisseur met à la disposition du Client l'interlocuteur suivant pour toute question relative à la protection des données dans le cadre du Contrat: le responsable de la protection des données de bexio SA, datenschutz@bexio.com.

(8) Le Fournisseur s'engage à satisfaire ses obligations relatives à la protection des données, à établir une procédure en vue de contrôler périodiquement l'efficacité des mesures techniques et organisationnelles visant à assurer la sécurité du traitement.

Le Fournisseur corrige ou supprime les données faisant l'objet du contrat si le Client le lui demande et que cela est compris dans le cadre de l'instruction. Si un effacement conforme à la protection des données ou une restriction correspondante du traitement des données ne s'avère pas possible, le Fournisseur procède à la destruction conforme à la protection des données des supports de données et autres matériels sur la base d'un mandat individuel par le Client, ou restitue ces supports au Client, à moins qu'il en ait été convenu autrement dans le Contrat.

Dans certains cas particuliers à déterminer par le Client, un stockage, une remise, des mesures de compensation et de protection doivent être convenus séparément, à moins que le contrat ne les prévoie déjà.

(9) Les données, les supports de données ainsi que tous les autres documents doivent être remis ou supprimés après l'exécution de la commande sur demande du Client. Si des coûts supplémentaires résultent de spécifications divergentes dans le cadre de la communication ou de l'effacement des données, ces frais sont à la charge du Client.

(10) Dans le cas d'une réclamation du client par une personne concernée portant sur le traitement des données, le Fournisseur s'engage à assister le Client, dans la limite de ses possibilités, dans la défense de la réclamation en question.

(11) Les services correspondant aux points 3, 5, 6(2) et 6(3) (remise des supports de données, prise de contact avec les personnes concernées et vérifications, par exemple) doivent être remboursés au Fournisseur selon ses taux horaires actuels ou en fonction de ses dépenses externes.

4 Obligations du Client

(1) Le Client s'engage à informer le Fournisseur en détail et dans les plus brefs délais s'il constate dans les résultats de la commande des erreurs ou des irrégularités concernant les dispositions relatives à la protection des données.

(2) Le Client doit indiquer au Fournisseur la personne à contacter pour toute question relative à la protection des données survenant dans le cadre du contrat; cette personne doit être différente des interlocuteurs déjà indiqués par le Client.

5 Demandes des personnes concernées

Si une personne concernée informe le Fournisseur de son souhait d'exercer son droit d'accès, de rectification ou d'effacement, le Fournisseur renverra cette personne au Client, à condition qu'une mise en relation avec ce dernier soit possible en fonction des indications de la personne concernée. Le Fournisseur transmet immédiatement la demande de la personne concernée au Client. Le Fournisseur assiste le Client sur les instructions de ce dernier dans le cadre de ses possibilités et dans la mesure convenue. Le Fournisseur ne saurait être tenu responsable si la

demande de la personne concernée ne fait l'objet d'aucune réponse ou fait l'objet d'une réponse inexacte ou tardive de la part du Client.

6 Moyens de preuve

(1) Le Fournisseur doit être en mesure de démontrer au Client le respect des obligations énoncées dans la présente annexe par des moyens appropriés, à savoir un audit interne ou une certification selon ISO 27001.

(2) Si, dans certains cas individuels, des inspections par le Client ou un auditeur mandaté par ce dernier s'avèrent nécessaires, elles devront être effectuées pendant les heures de bureau normales sans occasionner de perturbation dans le fonctionnement de l'entreprise, après notification préalable et en tenant compte d'un délai raisonnable. Le Fournisseur peut les subordonner à une notification préalable avec un délai raisonnable et à la signature d'un accord de confidentialité portant sur les données des autres clients et les mesures techniques et organisationnelles mises en place. Si l'auditeur mandaté par le Client est en relation de concurrence avec le Fournisseur, le Fournisseur dispose contre celui-ci d'un droit d'opposition.

(3) Si une autorité de contrôle de la protection des données ou une autorité de contrôle publique de l'État membre du Client procèdent à une inspection, le paragraphe 2 s'applique en conséquence. La signature d'un accord de confidentialité n'est pas requise si cette autorité de contrôle est soumise à une obligation légale de secret professionnel ou de confidentialité dont le non-respect est punissable conformément au Code pénal.

7 Sous-traitants (autres sous-traitants)

(1) Le Fournisseur est autorisé à faire appel à des sous-traitants, à condition que ces derniers satisfassent eux-mêmes aux exigences de la présente annexe dans le cadre du contrat de sous-traitance. Une liste des sous-traitants actuels peut être consultée sur la page suivante: https://www.bexio.com/de-CH/richtlinien/subunternehmer

(2) Le Client accepte que le Fournisseur fasse appel à des sous-traitants dans le cadre de l'exécution de la commande. Le Fournisseur informe le Client avant tout recours à ou remplacement d'un sous-traitant. Le Fournisseur est tenu d'informer le Client du recours aux services d'un sous-traitant en mettant à jour la liste mentionnée ci-dessus. Cette liste doit être mise à jour au moins 14 jours à l'avance. Le client consultera régulièrement la liste. Le client peut s'opposer au changement prévu par le Fournisseur dans un délai de 14 jours et pour des raisons importantes. Si aucune objection n'est formulée dans les délais, l'acceptation du changement est considérée comme donnée. S'il existe un motif important relatif à la protection des données, et si une solution à l'amiable ne peut pas être trouvée entre les parties, le Fournisseur dispose d'un droit spécial de résiliation.

(3) Un contrat de sous-traitance soumis à approbation existe à partir du moment où le Fournisseur mandate d'autres fournisseurs pour l'exécution de tout ou partie de la prestation convenue dans cette annexe. Le Fournisseur conclura le cas échéant des accords avec ces tierces parties afin de garantir que des mesures adéquates de protection de la vie privée et de l'information soient prises. Les sous-traitants n'ayant pas accès aux données du Client ou ne traitant pas les données de celui-ci sont exclus de ce chapitre et n'ont pas à apparaître pas dans la liste mentionnée ci-dessus.

(4) Si le Fournisseur passe des commandes à des sous-traitants, il lui incombe de transférer à ces derniers ses obligations relatives à la protection des données telles que définies dans cette annexe.

8 Obligations en matière d'information

Si les données du Client sont compromises en raison d'une saisie ou d'une confiscation, d'une procédure concordataire ou d'insolvabilité ou d'autres événements ou mesures de tiers, le Fournisseur doit informer le Client dans les plus brefs délais. Le Fournisseur doit immédiatement informer toutes les personnes responsables concernées de ce que la souveraineté et la propriété des données appartiennent exclusivement au Client en tant que «responsable du traitement» au sens du règlement général sur la protection des données.

9 Responsabilité

La responsabilité est régie par le Contrat.

10 Divers

(1) Les dispositions du Contrat s'appliquent par ailleurs. En cas de contradiction entre les dispositions de la présente annexe et les dispositions du Contrat, la présente annexe prévaudra. Si telle ou telle disposition de la présente annexe devait être nulle, la validité du Contrat et de l'annexe n'en sera pas affectée.

(2) Les addenda A et B font partie intégrante de la présente annexe.

Addendum A de l'accord relatif au traitement des données personnelles

Objet du contrat:	Traitement des données personnelles du Client dans le cadre de son utilisation des services du Fournisseur en tant que Software as a Service (SaaS).
Nature et objectif du traitement prévu des données:	Les données personnelles du Client sont transférées au Fournisseur dans le cadre des services du Software as a Service. Le Fournisseur traite ces données exclusivement en fonction de l'accord conclu (gestion des commandes, gestion des contacts (CRM), comptabilité, e-banking, comptabilité des salaires, gestion des stocks, gestion des projets).
Type des données personnelles:	Les types de données dépendent des données transmises par le Client. Ce sont (en fonction de la commande): • Des données personnelles de base (nom, date de naissance, adresse, employeur), y compris des coordonnées (téléphone et e-mail, par exemple) • Des données relatives au contrat, y compris les données relatives à la facturation et au paiement • L'historique des données relatives au contrat
Catégories de personnes concernées:	Les types de personnes concernées dépendent des données transmises par le Client. Ce sont (en fonction de la commande): • Les collaborateurs (y compris les candidats et les anciens collaborateurs) du Client, • Les clients du Client • Les prospects du Client • Les fournisseurs de service du Client • Les coordonnées des personnes de contact
Effacement, blocage et rectification des données:	Toute demande d'effacement, de blocage et de rectification doit être adressée au Client; les dispositions du Contrat s'appliquent par ailleurs.

Addendum B

Au contrat relatif au traitement des données de la commande

Mesures techniques et organisationnelles (MTO)

1 Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles (abrégées en MTO) suivantes sont indispensables pour le traitement des données

(1) Contrôle d'accès aux locaux et aux installations:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle d'accès:

1) Définition de zones de sécurité
2) Mise en place d'une protection d'accès efficace
3) Définition des personnes autorisées
4) Gestion et documentation des autorisations d'accès du personnel sur l'ensemble du cycle de vie
5) Accompagnement des visiteurs et du personnel externe
6) Surveillance des espaces en dehors des heures de fermeture
7) Journalisation des accès physiques

(2) Contrôle d'accès aux systèmes:

1) Protection de l'accès (authentification)
2) Authentification simple des collaborateurs (par nom d'utilisateur et mot de passe) avec un haut niveau de protection
3) Blocage en cas d'échec d'authentification ou d'inactivité et processus de réinitialisation des identifiants d'accès bloqués
4) Pas de fonction de mémorisation possible pour les mots de passe et/ou la saisie de formulaires
5) Définition des personnes autorisées
6) Gestion et documentation des supports d'authentification du personnel et des autorisations d'accès
7) Blocage d'accès automatique
8) Blocage d'accès manuel
9) Transmission sécurisée des identifiants d'authentification (credentials) dans le réseau
10) Journalisation des accès

(3) Contrôle d'accès aux données:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle d'accès aux données:

1) Elaboration d'un concept d'autorisation
2) Mise en œuvre de restrictions d'accès
3) Attribution d'autorisations minimales
4) Gestion et documentation des autorisations d'accès aux données
5) Journalisation des accès aux données

(4) Contrôles des transports et des transferts:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des transferts

1) Transfert de données sécurisé entre le serveur et le Client
2) Sauvegarde de la transmission dans le back-end
3) Sécurisation de la transmission vers des systèmes externes

4) Implémentation de passerelles sécurisées au niveau des points de transmission du réseau
5) Renforcement des systèmes back-end
6) Description de toutes les interfaces et des champs de données personnelles transmis
7) Authentification machine-machine
8) Gestion des disques (procédure)
9) Procédure de collecte et d'élimination
10) Procédure de suppression/effacement respectueuse dans le respect de la protection des données

(5) Contrôle des saisies:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des saisies:

1) Documentation des autorisations de saisie
2) Journalisation des saisies

(6) Contrôle des commandes:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des saisies:

3) Documentation des autorisations de saisie
4) Journalisation des saisies

(7) Contrôle des disponibilités:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des disponibilités:

1) Concept de sauvegarde
2) Plan d'urgence
3) Stockage des sauvegardes
4) Contrôle des systèmes de secours

(8) Principe de séparation:

Les mesures suivantes sont mises en place en ce qui concerne le contrôle des usages:

1) Modération dans la collecte des données
2) Traitement séparé