Contrat de traitement des données

bexio AG

Le présent contrat de traitement des données (ci-après «CTD») précise les obligations en matière de protection des données résultant de la relation contractuelle entre bexio AG (ci-après le «Fournisseur») et ses clients (ci-après «Client» ou «Clients»). La base de la relation contractuelle entre les parties est constituée des Conditions générales (ci-après «CG») et la Politique de confidentialité (ci-après «PC»); celles-ci font donc partie intégrante du CTD. Le CTD s'applique à toutes les activités en lien avec la relation contractuelle entre les parties et dans le cadre desquelles des employés du Fournisseur ou des tiers mandatés par le fournisseur traitent des données à caractère personnel (ci-après «données») du Client. Pour tout problème relatif à la protection des données, le Client peut contacter le délégué à la protection des données du Fournisseur à l'adresse datenschutz@bexio.com.

1. Objet, durée et spécification du traitement des données personnelles

1.1. L'objet et la durée de la collecte des données ainsi que le type et la finalité de leur traitement sont déterminés par les CG, à moins que les dispositions suivantes n'entraînent des obligations supplémentaires.

1.2. L'objet, le type et la finalité du traitement des données sont précisés dans l'annexe A aux CTD.

2. Champ d'application et responsabilité

2.1. Le Fournisseur traite des données personnelles pour le compte du Client. Ceci inclut les activités spécifiées dans les CG, la PC, l'annexe A du CTD et dans la description actuelle du service consultable sur le site web du Fournisseur.

2.2. Dans le cadre de la relation contractuelle, 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.

2.3. En remplissant le formulaire d'inscription dans le cadre de l'enregistrement et de la souscription d'un compte utilisateur («compte bexio») sur le site web du Fournisseur, le Client donne au fournisseur les instructions correspondantes pour le traitement des données. Le Client peut compléter, modifier ou retirer ses instructions dans son compte bexio ou en informant le Fournisseur. Toute instruction non prévue dans les CG sera traitée comme une demande de modification de la 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

3.1. Le prestataire ne doit traiter les données à caractère personnel des personnes concernées que dans le cadre de la relation contractuelle conformément aux CG, à la PC et au présent CTD; sauf cas exceptionnel prévu par la loi.

3.2. Le Fournisseur doit faire en sorte que son organisation interne réponde aux exigences spécifiques de la protection des données. Il doit prendre des mesures techniques et organisationnelles conformes aux exigences légales permettant d'assurer la protection

adéquate des données du Client, notamment pour assurer sur le long terme la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement des données. 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.

3.3. Les mesures prises par le Fournisseur sont précisées dans l'annexe 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 à tout moment d'autres mesures adéquates. Les mesures prises par le Fournisseur ne doivent pas tomber en dessous du niveau de protection convenu contractuellement dans le présent CTD.

3.4. 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 touchant la protection des données des personnes concernées et dans le cadre du respect des obligations relatives à la protection des données. Conformément aux CG, le Fournisseur est en droit d'exiger une indemnité de frais pour ce service.

3.5. Les employés impliqués dans le traitement des données du Client et les tiers agissant pour le compte du Fournisseur traitent les données exclusivement dans le cadre de la relation contractuelle conformément aux CG, à la PC et au présent CTD, et sont tenus au secret.

3.6. Si le Fournisseur prend connaissance d'une violation de la protection des données personnelles, il prendra des mesures raisonnables pour sécuriser les données et réduire les éventuelles conséquences préjudiciables pour les personnes concernées. En outre, le Fournisseur respecte pleinement les dispositions légales applicables en matière de notification des violations de la protection des données.

3.7. Le Fournisseur respecte pleinement les dispositions légales applicables en matière de protection des données et vérifie régulièrement l'efficacité de ses mesures techniques et organisationnelles pour assurer la sécurité du traitement.

3.8. Le Fournisseur traite et stocke les données personnelles pour toute la durée de la relation contractuelle entre le Fournisseur et le Client. 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, à l'exception des données dont le traitement peut s'avérer nécessaire par la suite, par exemple en raison d'obligations légales de conservation ou à des fins internes absolument indispensables. La communication des données et les frais correspondants sont régis par les CG.

4. Obligations du Client

4.1. Le Client s'engage à informer par écrit ou via son compte bexio le Fournisseur dans le détail et les plus brefs délais s'il constate dans les résultats des travaux des erreurs ou des irrégularités concernant les dispositions relatives à la protection des données.

4.2. 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, si cette personne diffère de la personne de contact déjà désignée.

4.3. Le Client reconnaît qu'il est le seul responsable de l'information des personnes concernées par le traitement des données en ce qui concerne le stockage, l'utilisation, le traitement et le transfert éventuels des données par le Fournisseur conformément aux dispositions des CG, de la PC et du présent CTD. Si certaines personnes concernées s'opposent au traitement des données prévu, le Client est responsable de la suppression des données associées à ces personnes dans son compte bexio.

4.4. En acceptant les CG et la PC, le Client **déclare expressément son consentement au transfert de ses données à la société mère du Fournisseur** et aux sociétés affiliées à celle-ci. Le Client dégage le Fournisseur de toute réclamation éventuelle. L'obtention du consentement des personnes concernées est de la responsabilité du Client.

5. Demandes des personnes concernées

5.1. Si une personne concernée informe le Fournisseur de son souhait d'exercer son droit d'accès, de rectification ou de suppression, 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 dans un délai raisonnable la demande de la personne concernée au Client. Dans la mesure de ses possibilités, le Fournisseur peut assister le Client dans le cadre d'une demande d'une personne concernée concernant la protection des données. Dans ce cas, le Fournisseur est en droit d'exiger une indemnité de frais. 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

6.1. Le Fournisseur doit être en mesure de démontrer au Client le respect des obligations énoncées dans le présent contrat par des moyens appropriés, par le biais d'un audit interne et/ou d'une certification ISO.

6.2. Si, dans certains cas particuliers, des inspections par le Client ou un auditeur mandaté par ce dernier s'avèrent nécessaires (sous le régime du RGPD, par exemple), 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 peut exercer à l'encontre de celui-ci un droit d'opposition et suggérer une personne neutre. Le Fournisseur est en droit de facturer au Client tous les frais associés au contrôle, en particulier si aucune irrégularité n'a pu être constatée.

6.3. 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 point 6.2 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)

7.1. Le Fournisseur peut faire appel à des sous-traitants dans le cadre de l'exécution de la prestation contractuelle. Le Fournisseur est autorisé à faire appel à des sous-traitants à condition que ces derniers satisfassent eux-mêmes aux exigences du présent CTD dans le cadre du contrat de sous-traitance. Le Fournisseur conclura le cas échéant dans la mesure nécessaire des accords avec ces sous-traitants afin de garantir que des mesures adéquates de protection de la vie privée et de l'information soient prises. Les sous-traitants qui n'ont pas accès aux données des Clients ou qui ne traitent pas les données personnelles en tant que sous-traitants sont exclus de ce chapitre. Une liste des sous-traitants actuels est disponible sous le lien suivant: https://www.bexio.com/fr-CH/directives/sous-entrepreneur

7.2. Le Client accepte que le Fournisseur fasse appel aux sous-traitants spécifiés sur son site web. Le Fournisseur informe le Client avant tout recours à un sous-traitant en mettant à jour son site web. La liste des sous-traitants actuels doit être mise à jour au moins 14 jours à l'avance sur le site web. Le Client consultera régulièrement la liste. Le Client peut s'opposer au changement prévu par le Fournisseur jusqu'à 14 jours après avoir pris connaissance dudit changement et pour des motifs importants. 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.

8. Obligations en matière d'information

8.1. 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.

9. Responsabilité

9.1. Les clauses de responsabilité applicables sont régies par les dispositions pertinentes des CG.

10. Divers

10.1. Pour le reste, les dispositions des CG et de la PC s'appliquent. En cas de contradiction entre le CTD et les CG, les dispositions des CG prévaudront. Si telle ou telle disposition du CTD devait être nulle, la validité des CG et des autres dispositions du CTD n'en sera pas affectée.

10.2. Les annexes A et B font partie intégrante du présent CTD.

Dernière version: Juin 2022

bexio AG

Alte Jonastrasse 24
8640 Rapperswil
Suisse

Annexe A Objet, nature et objectif
Annexe B Mesures techniques et organisationnelles (MTO)

Annexe A – Objet, nature et objectif

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 sur la base des CG et de la description de service correspondante sur le site web du fournisseur (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 particulier (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 particulier (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 de suppression, d'opposition et de rectification doit être adressée au Client; les dispositions des CG, de la PC et du présent CTD s'appliquent.

Annexe B - Mesures techniques et organisationnelles (MTO)

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

I. Contrôle d'accès aux locaux et aux installations:

- Définition de zones de sécurité
- Mise en place d'une protection d'accès efficace
- Définition des personnes autorisées
- Gestion et documentation des autorisations d'accès du personnel sur l'ensemble du cycle de vie
- Surveillance des espaces en dehors des heures de fermeture
- Journalisation des accès physiques

II. Contrôle d'accès aux systèmes:

- Protection de l'accès (authentification)
- Authentification simple des collaborateurs (par nom d'utilisateur et mot de passe) avec un haut niveau de protection
- Blocage en cas d'échec d'authentification ou d'inactivité et processus de réinitialisation des identifiants d'accès bloqués
- Définition des personnes autorisées
- Gestion et documentation des supports d'authentification du personnel et des autorisations d'accès
- Blocage d'accès automatique
- Blocage d'accès manuel
- Transmission sécurisée des identifiants d'authentification (credentials) dans le réseau
- Journalisation des accès

III. Contrôle d'accès aux données:

- Elaboration d'un concept d'autorisation
- Mise en œuvre de restrictions d'accès
- Attribution d'autorisations minimales
- Gestion et documentation des autorisations d'accès aux données
- Journalisation des accès aux données

IV. Contrôles des transports et des transferts:

- Transfert de données sécurisé entre le serveur et le Client
- Sauvegarde de la transmission dans le back-end
- Sécurisation de la transmission vers des systèmes externes
- Implémentation de passerelles sécurisées au niveau des points de transmission du réseau
- Renforcement des systèmes back-end
- Description de toutes les interfaces et des champs de données personnelles transmis
- Authentification machine-machine
- Gestion des disques (procédure)
- Procédure de collecte et d'élimination
- Procédure de suppression/effacement respectueuse dans le respect de la protection des données

V. Contrôle des saisies:

- Documentation automatique des autorisations de saisie
- Journalisation des saisies

VI. Contrôle des commandes:

- Documentation des autorisations de saisie
- Journalisation des saisies

VII. Contrôle des disponibilités:

- Concept de sauvegarde
- Plan d'urgence
- Stockage des sauvegardes
- Contrôle des systèmes de secours

VIII. Principe de séparation:

- Modération dans la collecte des données
- Traitement séparé