Accord sur le traitement des données de commandes

bexio ag

Cet accord sur le traitement des données de commandes concrétise les obligations en matière de protection des données découlant de la relation contractuelle entre bexio AG (ci-après « fournisseur » ou « sous-traitant ») et ses clients (ci-après « client » ou « responsable »). Pour toute question relative à la protection des données, le client peut contacter le responsable de la protection des données du fournisseur à l'adresse datenschutz@bexio.com.

1. Objet

1.1. Il existe entre les parties une relation juridique pour l'exécution de laquelle des données personnelles sont transférées du responsable au sous-traitant (« contrat principal »). La relation juridique entre les parties est basée sur les conditions générales (« CG ») du fournisseur. Le présent contrat de traitement des commandes est conclu entre les parties afin d'assurer une protection adéquate lors du transfert de données personnelles.

1.2. Sauf disposition contraire dans le présent accord, tous les termes doivent avoir la même signification que dans la loi suisse sur la protection des données (« LPD »). En outre, cet accord aide les parties à se conformer au règlement général sur la protection des données de l'UE (« RGPD ») dans la mesure où les données personnelles protégées des clients de l'UE sont concernées à cet égard.

2. Description du traitement des données

2.1. Le fournisseur traite les données personnelles pour le compte du client. L'objet et la durée de la relation contractuelle ainsi que la nature et la finalité des traitements découlent en principe des CGV et de l'annexe A du contrat de traitement des commandes. Les traitements des données sont également concrétisés dans la description actuelle des services sur le site Web du fournisseur ainsi que dans la déclaration de protection des données (« DSE »).

2.2. En remplissant le formulaire d'inscription pour l'enregistrement et la commande 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. Les instructions qui ne sont pas prévues dans les CGV sont traitées comme une demande de modification des prestations. Les instructions orales doivent être fournies immédiatement par écrit ou par le client en effectuant la procédure correspondante sur le compte bexio.

3. Obligations du client

3.1. Dans le cadre de la relation contractuelle, le client est seul responsable du respect des dispositions légales des lois sur la protection des données, en particulier de la légalité de la transmission des données au fournisseur, ainsi que de la légalité du traitement des données.

3.2. Le client s'est assuré que les mesures techniques et organisationnelles (« TOM ») utilisées par le sous-traitant, décrites dans l'annexe B, sont suffisantes pour garantir une protection adéquate des données personnelles transférées.

3.3. Le client doit informer immédiatement et complètement le fournisseur par écrit ou via le compte bexio s'il constate des erreurs ou des irrégularités dans les résultats de la commande en ce qui concerne les dispositions relatives à la protection des données.

3.4. Le client indique au fournisseur l'interlocuteur pour les questions de protection des données dans le cadre de la relation contractuelle, dans la mesure où il diffère de l'interlocuteur mentionné.

3.5. Le client déclare qu'il est seul responsable de l'information des personnes concernées par le traitement des données concernant le stockage, l'utilisation, le traitement et la transmission possibles des données par le fournisseur conformément aux dispositions des CGV, de la DSE et du présent contrat de traitement des commandes. Si certaines personnes concernées ne sont pas d'accord avec le traitement des données prévu, le client est responsable de la suppression des données respectives dans le compte bexio en conséquence.

3.6. En acceptant les CGV et le contrat de traitement des commandes, le client **accepte expressément la transmission de ses données à la société mère du fournisseur** ainsi qu'aux sociétés affiliées. Le client libère le fournisseur de toutes les réclamations possibles. Il incombe au client d'obtenir le consentement des personnes concernées.

4. Obligations du fournisseur

4.1. Généralités

4.1.1. Le sous-traitant garantit, en ce qui concerne le traitement des données personnelles, qu'il

- traitera ces données personnelles conformément au présent contrat de traitement des commandes et exclusivement aux fins poursuivies par le responsable du traitement,
- les finalités poursuivies par le responsable du traitement découlent de l'annexe A, du compte bexio ou des instructions explicites du responsable du traitement ou sont déterminées par un autre accord avec le responsable du traitement,
- fournira au responsable du traitement les informations nécessaires au contrôle du respect des obligations énoncées dans le présent accord,

- prend en compte les principes de la protection des données par conception et par défaut dans ses équipements de travail, produits, applications ou services,

- informera le responsable s'il ne peut plus ou ne devrait plus être en mesure de respecter le présent accord, et

- coopérera avec les autorités de surveillance compétentes dans le cadre autorisé par la loi.

4.1.2. Les personnes habilitées à donner des instructions du responsable du traitement sont informées par écrit ou sur le compte bexio du sous-traitant au début du traitement de la commande. En cas de changement ou d'empêchement à long terme de la personne de contact, le fournisseur doit être informé immédiatement par écrit ou dans le compte bexio du successeur ou du représentant. Les instructions orales ne sont contraignantes qu'avec la confirmation écrite directe de la personne responsable. L'e-mail est suffisant pour être considéré comme forme écrite.

4.1.3. Le fournisseur doit informer immédiatement le client s'il estime qu'une instruction viole les dispositions légales. Le fournisseur est en droit de suspendre l'exécution de l'instruction correspondante jusqu'à ce que sa légalité soit confirmée par le responsable ou que l'instruction soit modifiée.

4.2. Sécurité des données

4.2.1. Dans son domaine de responsabilité, il conçoit l'organisation interne de manière à ce qu'elle réponde aux exigences particulières de la protection des données. Il prend des mesures techniques et organisationnelles pour assurer une protection adéquate des données personnelles du client, qui répondent aux exigences légales respectives. Le sous-traitant a tenu compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de l'étendue et des finalités du traitement, ainsi que de la probabilité et de la gravité du risque pour les droits fondamentaux et la personnalité des personnes concernées. Les mesures sont décrites dans l'annexe B et sont vérifiées périodiquement. Les modifications des mesures sont autorisées, à condition que le niveau de sécurité actuel ne soit pas inférieur. Le client connaît ces mesures techniques et organisationnelles et il est responsable de s'assurer qu'elles offrent un niveau de protection adéquat pour les risques des données à traiter.

4.2.2. Lors de l'exécution des travaux, le fournisseur ne recourra qu'à des employés qui sont tenus à la confidentialité et qui ont déjà été familiarisés avec les dispositions relatives à la protection des données concernées.

4.2.3. Dans la mesure du possible, le fournisseur aide le client à répondre aux demandes et aux demandes des personnes concernées en matière de protection des données et à se conformer aux obligations en matière de protection des données. Conformément aux CGV, le fournisseur est en droit d'exiger une indemnité pour cela.

4.2.4. Si le fournisseur a connaissance d'une violation de la protection des données personnelles, il prend les mesures raisonnables pour protéger les données et pour atténuer les conséquences négatives possibles pour les personnes concernées. En outre, le fournisseur se conforme pleinement aux dispositions légales en vigueur concernant la notification des violations de la protection des données.

5. Sous-traitants (autres sous-traitants)

5.1. Le fournisseur peut faire appel à des sous-traitants pour exécuter la prestation contractuelle. Le sous-traitant ne peut transférer le traitement à un tiers qu'avec l'autorisation préalable du responsable. La commande de sous-traitants en tant que sous-traitants par le fournisseur est autorisée, dans la mesure où ils remplissent les exigences du présent contrat de traitement des commandes dans le cadre de la sous-traitance. Le fournisseur conclut des accords avec les sous-traitants dans la mesure nécessaire pour assurer des mesures appropriées de protection des données et de sécurité de l'information. Les sous-traitants qui n'ont pas accès aux données personnelles ou qui ne traitent pas les données personnelles en tant que sous-traitants sont exclus de ce chapitre. Une liste des sous-traitants actuels dans le sens d'un sous-traitant (ci-après dénommés « sous-traitants » pour plus de commodité) peut être consultée ici :

https://www.bexio.com/de-CH/richtlinien/subunternehmer

5.2. Le client accepte que le fournisseur fasse appel aux sous-traitants mentionnés sur le site Web du fournisseur. Avant de faire appel à d'autres sous-traitants, le fournisseur informe le client en mettant à jour son site Web. L'aperçu sur le site Web doit être mis à jour au moins 14 jours avant l'utilisation. Le client consultera régulièrement l'aperçu. Le client peut s'opposer à la modification dans les 14 jours suivant sa prise de connaissance pour une raison importante. En l'absence d'opposition dans le délai imparti, le consentement à la modification est réputé acquis. S'il existe un motif important de protection des données et si une solution amiable n'est pas possible entre les parties, un droit de résiliation spécial est accordé au fournisseur.

5.3. En règle générale, les services auxiliaires ne sont pas considérés comme un traitement de sous-traitance pour le fournisseur sans référence aux données du responsable conformément à l'annexe A (par exemple, services de télécommunication, services postaux/de transport, maintenance et services aux utilisateurs ou élimination des supports de données et autres mesures visant à assurer la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels). Cependant, le fournisseur est tenu de prendre des mesures de contrôle appropriées pour assurer la protection et la sécurité des données du client, même pour les services auxiliaires.

6. Communication à l'étranger

6.1. Le traitement des données conformément à l'annexe A a généralement lieu en Suisse ou dans un État membre de l'Union européenne ou dans un autre État contractant de l'accord sur l'Espace économique européen. Tout transfert vers un autre pays tiers ne peut avoir lieu que si les conditions légales correspondantes sont remplies.

6.2. Si le sous-traitant fait appel à des sous-traitants dans des États qui ne disposent pas d'un niveau adéquat de protection des données selon le Préposé fédéral à la protection des données et à la transparence, à l'annexe de la VDSG ou à la Commission européenne, le sous-traitant garantit l'admissibilité de la divulgation en vertu de la loi sur la protection des données par des mesures appropriées et appropriées au transfert de données respectif.

7. Droits des personnes concernées

7.1. Si une personne concernée s'adresse au fournisseur avec des demandes de correction, de suppression ou d'information, le fournisseur dirigera la personne concernée vers le client, dans la mesure où une affectation au client est possible selon les informations de la personne concernée. Le fournisseur transmet la demande de la personne concernée au client dans un délai raisonnable. Le fournisseur peut aider le client avec les demandes en matière de protection des données d'une personne concernée dans la mesure du possible. Dans ce cas, le fournisseur est en droit d'exiger une indemnité. Le fournisseur n'est pas responsable si le client ne répond pas, ne répond pas correctement ou ne répond pas dans les délais à la demande de la personne concernée.

8. Possibilités de preuve

8.1. Le fournisseur démontre au client le respect des obligations énoncées dans cette annexe par des moyens appropriés. Cela se fait par un auto-audit et/ou une certification ISO.

8.2. Si des inspections sont nécessaires dans des cas individuels par le client ou un inspecteur mandaté par celui-ci (par exemple en raison de l'assujettissement au RGPD), elles sont effectuées aux heures d'ouverture habituelles sans perturber le fonctionnement de l'entreprise après l'inscription, en tenant compte d'un délai raisonnable. Le fournisseur peut les faire dépendre de l'inscription préalable avec un délai raisonnable et de la signature d'une déclaration de confidentialité concernant les données d'autres clients et les mesures techniques et organisationnelles mises en place. Si l'inspecteur mandaté par le client est dans une relation concurrentielle avec le fournisseur, le fournisseur peut le refuser et proposer une personne neutre. Le fournisseur peut facturer au client d'éventuels frais liés à l'inspection, en particulier si aucune irrégularité n'a pu être détectée.

8.3. Si une autorité de surveillance de la protection des données ou une autre autorité de surveillance gouvernementale du client effectue une inspection, le présent chapitre s'applique en conséquence. Une signature d'une obligation de confidentialité n'est pas nécessaire si cette autorité de surveillance est soumise à une confidentialité professionnelle ou légale dans laquelle une violation est punie par le code pénal.

9. Obligations d’information

9.1. Si les données du client sont menacées par la saisie ou la confiscation, par une procédure d'insolvabilité ou de règlement ou par d'autres événements ou mesures de la part de tiers, le fournisseur doit en informer le client sans délai. Le fournisseur informera immédiatement tous les responsables dans ce contexte que la souveraineté et la propriété des données appartiennent exclusivement au client.

10. Durée et résiliation

10.1. Le fournisseur traite et stocke les données personnelles tant que la relation contractuelle entre le fournisseur et le client existe. Le fournisseur corrige ou supprime les données contractuelles si le client l'ordonne et si cela est inclus dans le cadre des instructions. Sont

exclues les données qui sont nécessaires pour un traitement ultérieur en raison de dispositions légales ou à des fins internes obligatoires. Le fournisseur est en droit de suspendre l'exécution d'éventuelles instructions abusives jusqu'à ce que leur légalité soit prouvée. La remise des données et la rémunération correspondante sont régies par les CGV.

11. Responsabilité

11.1. La responsabilité est régie par les dispositions correspondantes des CGV.

12. Divers

12.1. Pour le reste, les dispositions des CGV et de la DSE s'appliquent. En cas de contradiction entre le contrat de traitement des commandes et les CGV, les dispositions des CGV prévalent. Si certaines parties du contrat de traitement des commandes sont invalides, cela n'affecte pas la validité des CGV et des autres dispositions du contrat de traitement des commandes.

12.2. Les annexes A et B sont des éléments essentiels du présent contrat de traitement des commandes.

Dernière version : septembre 2023

bexio ag

Alte Jonastrasse 24

8640 Rapperswil

Suisse

Annexe A Objet, nature et finalité

Annexe B Mesures techniques et organisationnelles (TOM)

1. Annexe A – Objet, nature et finalité

Objet de la commande :	Traitement des données personnelles du client dans le cadre de son utilisation des services du fournisseur en tant que logiciel en tant que service.
Nature et finalité du traitement des données prévu :	Les données personnelles traitées par le client sont transférées au fournisseur dans le cadre des services de logiciel en tant que service. Le fournisseur traite ces données exclusivement conformément aux CGV et à la description des services correspondants 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, etc.).
Type de données personnelles :	Les types de données dépendent des données transmises par le client. Celles-ci sont notamment (en fonction de la commande) : ● Données de base personnelles (nom, date de naissance, adresse, employeur), y compris les coordonnées (par exemple, téléphone, e-mail) ● Données contractuelles, y compris la facturation et les données de paiement ● Historique des données du contrat
catégories de personnes concernées ;	Les catégories de personnes concernées dépendent des données transmises par le client. Celles-ci sont notamment (en fonction de la commande) : ● Employés (y compris les candidats et les anciens employés) du client ● Clients du client ● Personnes intéressées par le client ● Prestataire de services du client ● Coordonnées des personnes de contact
Suppression, blocage et correction des données :	Les demandes de suppression, de blocage et de correction doivent être adressées au client ; pour le reste, les dispositions des CGV, de la DSE et du présent contrat de traitement des commandes s'appliquent.

2. Annexe B - Mesures techniques et organisationnelles (TOM)

I. Contrôle des entrées :

Mesures pour empêcher les personnes non autorisées d'accéder aux installations de traitement des données avec lesquelles les données personnelles sont traitées ou utilisées :

- Système d'alarme
- Contrôle des entrées automatisé
- Capteurs photoélectroniques/détecteurs de mouvement
- Gestion des clés (remise des clés, etc.)
- Cartes à puce / système de fermeture par transpondeur
- Système de fermeture manuel (utilisation limitée aux personnes clés en cas d'erreurs dans les systèmes de contrôle d'accès)
- Vidéosurveillance dans la zone d'entrée
- Port du badge visible et obligatoire
- Définition des zones de sécurité
- Détermination des personnes autorisées à entrer
- Un contrôle séparé et documenté pour l'accès aux centres de données et aux salles des serveurs uniquement pour le personnel spécialement autorisé est mis en œuvre. L'entrée par le personnel autorisé est enregistrée avec le nom et le numéro de carte ou de jeton. Il existe des contrôles d'accès séparés pour les centres de données.

II. Contrôle d'accès :

Mesures pour empêcher l'utilisation des systèmes de traitement des données par des personnes non autorisées :

- Attribution des droits des utilisateurs
- Attribution du mot de passe
- Authentification avec nom d'utilisateur / mot de passe / MFA
- Verrouillage automatique de l'accès
- Verrouillage manuel de l'accès
- Enregistrement de l'accès
- Utilisation des pare-feu matériels
- Utilisation des profils utilisateur
- Mesures supplémentaires : pare-feu pour applications Web, analyses régulières des vulnérabilités, tests de pénétration réguliers, gestion des correctifs, exigences minimales pour

la complexité des mots de passe et le changement forcé des mots de passe, utilisation de scanners antivirus.

- Affectation des profils utilisateur aux systèmes informatiques
- Utilisation de la technologie VPN
- Cryptage des supports de stockage mobiles
- Utilisation d'une gestion des appareils mobiles (par exemple : verrouillage et réinitialisation à distance des smartphones)
- Cryptage matériel pour les ordinateurs portables

III. Contrôle d'accès

Mesures garantissant que les personnes autorisées à utiliser un système de traitement des données ne peuvent accéder qu'aux données soumises à leur autorisation d'accès et que les données personnelles ne peuvent pas être traitées, utilisées et stockées sans autorisation, lues, copiées, modifiées ou supprimées :

- Création d'un concept d'autorisation (gestion des accès à l'identité)
- Nombre d'administrateurs réduit au « minimum absolu »
- Attribution restrictive des autorisations
- Mise en œuvre des restrictions d'accès
- Nettoyage des médias en toute sécurité avant réutilisation
- Cryptage matériel (bandes de sauvegarde, ordinateurs portables)
- Gestion des droits par les administrateurs système
- Politique de mot de passe avec spécifications sur la longueur du mot de passe, gestion des changements de mot de passe
- Stockage sécurisé des supports de données

IV. Contrôle de la divulgation

Mesures garantissant que les données personnelles ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation lors de la transmission électronique ou pendant leur transport ou leur stockage sur des supports de données et qu'il est possible de vérifier et de déterminer à quels endroits une transmission de données personnelles par des installations de transmission de données est prévue :

- Création d'une ligne auxiliaire ou d'une connexion VPN
- Cryptage (sauvegarde pour le stockage hors site)
- Cryptage TLS pour toutes les communications (client Web, API, applications mobiles)
- Sécurisation de la transmission dans le backend

- Sécurisation de la transmission aux systèmes externes
- Mise en œuvre de passerelles de sécurité aux points d'échange du réseau
- Durcissement des systèmes de back-end
- Description de toutes les interfaces et des champs de données personnelles transmis
- Authentification machine-machine
- Procédure d'effacement/destruction conforme à la protection des données

V. Contrôle de saisie

Mesures garantissant qu'il est possible de vérifier ultérieurement si et par qui les données personnelles peuvent être saisies, modifiées ou supprimées dans les systèmes de traitement des données :

- Attribution de droits de la saisie, la modification et la suppression de données sur la base d'un concept d'autorisation
- Documentation automatique des autorisations de saisie
- Enregistrement des entrées

VI. Contrôle de disponibilité

Mesures garantissant que les données personnelles sont protégées contre la destruction ou la perte accidentelle :

- Alimentation sans interruption (UPS)
- Dispositifs pour surveiller la température et l'humidité dans les salles de serveurs
- Systèmes de détection d'incendie et de fumée
- Alarme en cas d'accès non autorisé aux salles de serveurs
- Création de concepts de sauvegarde et de restauration
- Création de sauvegardes de données
- Test de récupération de données
- Stockage hors site sécurisé des sauvegardes de données
- Systèmes de climatisation dans les salles de serveurs
- Systèmes d'extinction dans les salles de serveurs
- Plan d'urgence
- Stockage des sauvegardes
- Contrôle des dispositifs d'urgence

VII. Commandement de la séparation

Mesures garantissant que les données personnelles collectées à des fins différentes sont traitées séparément :

- Création d'un concept d'autorisation
- Droits de base de données accordés et documentés
- Logical Client Separation/séparation client logique (au niveau logiciel)
- Séparation des systèmes de production et de test
- Économie dans la collecte de données