Contrat de traitement des données personnelles par un sous-traitant (ADV) inkl. (TOM)

Table des matières:

Dans le cadre du présent contrat de traitement des données personnelles (le « Contrat »), les parties règlent le traitement de données personnelles par ou pour le prestataire de services dans le cadre du contrat-cadre sous-jacent. L'étendue du traitement des données (objet, finalité, catégories de données, etc.) découle directement du contrat-cadre, sauf indication et disposition contraires dans le présent document.

La durée du traitement est déterminée par la durée du contrat-cadre sous-jacent et ne peut être résiliée qu'en même temps que celui-ci, de manière ordinaire ou extraordinaire.

Dispositions relatives au traitement des données sur mandat

Les parties ont conclu un contrat-cadre dans le cadre duquel le prestataire de services traite des données personnelles pour le compte du responsable du traitement. Le présent Accord vise à encadrer ce traitement de données personnelles au regard du DSG et, le cas échéant, de la DSGVO.
Le transfert de données personnelles vers un pays ne disposant pas d'un niveau de protection adéquat des données (conformément à l'annexe 1 de l'ordonnance sur la protection des données – DSG) n'est pas autorisé.
Tout traitement de données personnelles par le prestataire de services à ses propres fins nécessite un accord explicite et distinct, et est par ailleurs interdit.

1) Définitions:

Les termes suivants sont utilisés avec la signification définie dans le présent Accord. Pour le reste, les termes doivent être compris tels que définis dans le DSG et, le cas échéant, dans la DSGVO, notamment les termes « données personnelles », « traitement », « sous-traitant » et « responsable du traitement ».

"DSG" la loi fédérale sur la protection des données, dans sa version en vigueur, y compris ses ordonnances

"DSGVO" le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, abrogeant la directive 95/46/CE.

"EWR" l'Espace économique européen.

"Pays disposant d'un niveau de protection adéquat": pays ou territoire figurant à l'annexe 1 de l'ordonnance sur la protection des données (DSV).

"Entreprise affiliée": personne morale directement ou indirectement contrôlée par le responsable du traitement, ou qui contrôle directement ou indirectement celui-ci, ou qui est sous le contrôle commun d'une même entité juridique.

2) Traitement sur mandat:

1. Champ d'application et caractéristiques du traitement des données sur mandat

Le présent Accord régit, dans le cadre de l'exécution du contrat principal, le traitement de données personnelles par le prestataire de services en tant que sous-traitant pour le compte du responsable du traitement.

Alternativement, le prestataire de services peut agir en tant que sous-traitant de la responsable du traitement, laquelle agit elle-même comme sous-traitante d'un tiers.

Dans la mesure où la responsable du traitement agit elle-même comme sous-traitante (par exemple pour un client), elle est, dans les limites autorisées, l'unique interlocutrice du responsable de traitement, et ses instructions sont réputées émaner de ce dernier.

Les données personnelles désignent toutes les données reçues par le prestataire de services dans le cadre du traitement, que ce soit de la part du responsable du traitement, d'une entreprise affiliée ou d'un tiers.

L'objet, la durée, la nature et la finalité du traitement, ainsi que les catégories de données personnelles traitées et les catégories de personnes concernées, sont définis conformément à la lettre c, chiffre 5 du présent Accord.

2. Traitement de données personnelles

Obligations de la responsable du traitement

La responsable du traitement confirme au prestataire que :

elle a effectué ou obtenu toutes les notifications, enregistrements, autorisations administratives et consentements nécessaires des personnes concernées pour permettre un traitement licite des données personnelles par le prestataire en tant que sous-traitant conformément au DSG et, le cas échéant, à la DSGVO ; et

elle répond à toutes les demandes des personnes concernées exerçant leurs droits en vertu des dispositions applicables en matière de protection des données.

Obligations du prestataire de services

Le prestataire s'engage et garantit à la responsable du traitement :

a) de ne traiter les données personnelles que pour le compte de la responsable du traitement et uniquement aux fins de l'exécution du contrat principal, conformément aux instructions documentées de cette dernière ;
b) de ne traiter les données personnelles que dans les lieux convenus ou autorisés par la responsable du traitement ;
c) keine Personendaten ins Ausland bekanntzugeben oder zu übermitteln, ausser der de ne pas divulguer ni transférer les données personnelles à l'étranger, sauf si cela est requis par le client dans le cadre du service commandé ;
d) de mettre en place et de maintenir des mesures techniques et organisationnelles appropriées (TOM conformément à l'annexe du présent Accord) pour garantir en tout temps la confidentialité, l'intégrité et la disponibilité des données personnelles et les protéger contre tout traitement, accès ou divulgation non autorisés, ainsi que contre toute altération, destruction ou perte accidentelle ou illicite, en particulier – et au minimum – les mesures prévues par le DSG et, le cas échéant, par l'article 32 de la DSGVO et par d'autres dispositions applicables en matière de protection des données. Le prestataire vérifiera régulièrement le respect et l'efficacité de ces mesures et

proposera à la responsable du traitement les améliorations ou ajustements nécessaires;

de ne recourir, pour le traitement de données personnelles, qu'à des employés ou autres auxiliaires (y compris tous les sous-traitants agissant sur instruction du prestataire) qui sont contractuellement ou légalement tenus à la confidentialité et à ne traiter les données personnelles que dans la mesure nécessaire à l'exécution des tâches qui leur sont confiées par le prestataire conformément au contrat principal et au présent Accord. Il est en outre convenu entre les parties que le prestataire reste responsable du comportement de ses employés et auxiliaires comme de son propre comportement ;

de ne déléguer le traitement de données personnelles à des sous-traitants que si la responsable du traitement ne s'y est pas opposée. Le prestataire doit informer la responsable du traitement soixante (60) jours avant le recours à un sous-traitant. L'absence d'opposition dans un délai de trente (30) jours vaut approbation. Iomarket est autorisée à recourir aux sous-traitants mentionnés dans la section « Sous-traitants de io market AG » pour les prestations indiquées. Le prestataire s'engage à imposer à tout sous-traitant des obligations de confidentialité et de protection des données au moins aussi strictes que celles du contrat principal et du présent Accord. Il est également convenu que le prestataire reste responsable du comportement de ses sous-traitants comme de son propre comportement et qu'il informe immédiatement et de manière appropriée la responsable du traitement de tout changement concernant les coordonnées, l'emplacement ou d'autres aspects essentiels des sous-traitants. Toute modification d'éléments ayant une portée sur la protection des données nécessite une nouvelle approbation. Aucun sous-traitement ultérieur par un sous-traitant n'est autorisé ;

de notifier immédiatement à la responsable du traitement, en tout cas dans un délai de 24 heures à l'adresse indiquée par cette dernière (et à défaut à l'adresse de contact figurant sur la page de signature):

(i) toute violation avérée ou suspectée de la sécurité des données personnelles (y compris toute violation de la présente clause 2.0 et toute autre violation au sens de la DSGVO, du DSG ou d'autres dispositions applicables en matière de protection des données), accompagnée de toutes les informations visées à l'article 33, alinéa 3 de la DSGVO, ainsi que les informations pertinentes selon le DSG et autres législations applicables en la matière, et sur simple demande, toute autre information, y compris celle prévue au chiffre 2 (v) (par exemple Root Cause Analysis);

(ii) toute déficience réelle ou imminente du prestataire à se conformer à l'une quelconque des dispositions du présent Accord, ainsi que toutes les informations raisonnablement demandées à ce sujet ;

(iii) toute demande ou tout accès effectif aux données personnelles par une autorité ou autre entité, sauf si la loi applicable interdit expressément une telle notification pour des raisons impérieuses d'intérêt public. En cas d'accès tel que décrit en (iii), le prestataire s'efforcera en outre, dans la mesure du raisonnable et sauf instruction contraire de la responsable du traitement, de contester et de limiter cet accès ;

d'assister la responsable du traitement, à sa demande et de la manière souhaitée par cette dernière, dans le respect de la DSGVO, du DSG et des autres lois applicables en matière de protection des données, en tenant compte de la nature du traitement et des informations disponibles au prestataire, notamment dans l'exécution de ses obligations (i) envers les personnes concernées exerçant leurs droits au titre de la législation applicable (y compris le chapitre III de la DSGVO et les dispositions correspondantes du DSG et d'autres textes légaux) et (ii) selon les articles 32 à 36 de la DSGVO, ainsi que les dispositions équivalentes du DSG et autres réglementations applicables;

d’informer immédiatement la responsable du traitement si, selon lui, une instruction donnée viole les lois applicables en matière de protection des données ou toute autre législation. Dans la mesure du possible, il poursuivra le traitement en l’absence d’autre instruction ;

de fournir à la responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations, d’autoriser les audits et inspections (y compris sur site) par la responsable du traitement ou les auditeurs mandatés par elle, et d’y coopérer pleinement. Le prestataire fournira à la responsable du traitement, de manière proactive ou sur simple demande, les rapports d’audit établis par ses auditeurs attestant de la conformité aux obligations du présent Accord ou documentant toute violation, sans frais supplémentaires. Il veillera à ce que ces droits d’audit s’appliquent également aux sous-traitants. Il corrigera sans délai fautif et à ses frais toute non-conformité constatée et en apportera la preuve. Si des lacunes significatives sont constatées lors d’un audit ou si le comportement du prestataire justifie un audit, ce dernier en assumera les coûts ;

selon le choix de la responsable du traitement et sous réserve des obligations légales de conservation applicables, à la fin du contrat principal ou sur demande de la responsable du traitement, de restituer ou de supprimer toutes ou certaines données personnelles sans en conserver de copie, et d’attester par écrit cette suppression.

Indemnisation

Le prestataire s’engage à indemniser et à dégager de toute responsabilité la responsable du traitement à l’égard de toute réclamation de tiers résultant d’une violation du présent Accord ou des dispositions applicables en matière de protection des données. Cette obligation d’indemnisation couvre notamment tous les dommages, frais, sanctions administratives, réclamations ou dépenses encourus par la responsable du traitement en raison de telles violations.

Sauf disposition expresse contraire spécifiquement applicable à la présente clause, cette obligation d’indemnisation, de même que toute éventuelle demande de dommages-intérêts de la part de la responsable du traitement ou de ses sociétés affiliées, est limitée au double du plafond de responsabilité éventuellement convenu dans le contrat principal.

Toute exclusion de responsabilité pour négligence légère ne s’applique pas.

3) Dispositions complémentaires:

Les parties conviennent en outre de ce qui suit :

Le présent Accord s’applique également au bénéfice des sociétés affiliées de la responsable du traitement, pour lesquelles le prestataire traite des données personnelles conformément au contrat principal. En conséquence, les sociétés affiliées de la responsable du traitement peuvent faire valoir les mêmes droits que la responsable du traitement à l’encontre du prestataire, et celui-ci est tenu envers elles des mêmes obligations prévues par le présent Accord que celles qui lui incombent vis-à-vis de la responsable du traitement.

Chaque partie respecte les obligations qui lui incombent en vertu des dispositions légales applicables en matière de protection des données, en particulier celles du DSG et, dans la mesure où elles s’appliquent, du DSGVO.

La version en vigueur est publiée en ligne sur le site internet. En cas de divergences entre différentes versions linguistiques résultant de traductions, la version allemande fait foi.

Le présent Accord est considéré comme un accord autonome en complément du contrat principal. En cas de contradiction entre les dispositions du présent Accord et celles du contrat principal, les dispositions du présent Accord prévalent, dans la mesure où elles concernent le traitement de données personnelles par le prestataire dans le cadre du contrat principal.

Les dispositions du présent Accord restent en vigueur après la fin du contrat principal et aussi longtemps que le prestataire détient ou a accès aux données personnelles couvertes par le présent Accord.

Les dispositions du présent Accord sont régies par le droit suisse. Le for juridique est défini dans le contrat principal.

La version en vigueur est publiée en ligne sur le site internet. En cas de divergences entre différentes versions linguistiques résultant de traductions, la version allemande fait foi.

Annexe:
Mesures techniques et organisationnelles (TOM)

Dans le monde numérique actuel, la protection des données et la sécurité de l'information revêtent une importance capitale. Cela s'applique tout particulièrement aux services de communication et EDI comme ceux d'iomarket. Afin de garantir la sécurité et la confidentialité des données des utilisateurs, l'application de mesures techniques et organisationnelles efficaces (TOM) est indispensable.

Les sections suivantes présentent les mesures spécifiques de protection des données mises en œuvre chez iomarket et sur la plateforme « gate2b », afin d'assurer le respect des normes en matière de protection des données et de sécurité de l'information.

Ces mesures sont fondées sur la loi fédérale suisse sur la protection des données (DSG), qui constitue une base solide pour la sécurité des données. Conformément au DSG, iomarket s'engage à mettre en œuvre des mesures techniques et organisationnelles étendues afin de garantir la confidentialité, l'intégrité et la disponibilité de vos données.

De plus, iomarket se réfère à l'Ordonnance sur la protection des données (DSV) pour couvrir de manière détaillée des domaines de sécurité spécifiques. Ces prescriptions légales servent de guide pour assurer la protection et la sécurité des données.

1. Mesures générales de sécurité

Contrôle d'accès physique

Régule les autorisations d'accès de l'organisation :

- Klingelanlage mit Gegensprechanlage / Empfang
- Système d'interphone / réception
- Accès par serrures électroniques de sécurité et deux portes de sécurité
- Gestion des autorisations d'accès par l'administration, avec journalisation
- Gestion des droits des utilisateurs par les administrateurs, avec journalisation
- Les visiteurs ne peuvent entrer que sous la supervision d'un collaborateur
- Sélection rigoureuse du service de nettoyage

- Gestion des clés
- Enregistrement des visiteurs

Contrôle d’accès aux systèmes

Garantit que seules les personnes autorisées peuvent accéder aux systèmes :

- Coffre-fort de donnéesPasswortvergabe
- Attribution de mots de passe
- Attribution de droits d’utilisateur
- Concepts de droits et d’authentification limités au strict nécessaire (« Need to know »)
- Verrouillage automatique des postes de travail
- Authentification à deux facteurs
- Utilisation de pare-feu matériels
- Utilisation de pare-feu logiciels
- Utilisation de profils utilisateurs

Contrôle d’accès aux données

Assure que le traitement des données est conforme aux autorisations :

- Droits des utilisateurs
- Richtline Clean Desk
- Politique de bureau propre (« Clean Desk »)
- Chiffrement du matériel
- Gestion des droits par les administrateurs système
- Désactivation des droits d’accès en cas de changement de personnel
- Politiques de mots de passe
- Sensibilisation à la prévention du phishing

2. Mesures spécifiques

Contrôle de la transmission

Mesures pour s'assurer que les données personnelles ne peuvent pas être lues, copiées, modifiées ou supprimées sans autorisation lors de la transmission :

- Chiffrement (p. ex. TLS)
- Sécurisation des canaux de communication
- Chiffrement matériel

Contrôle des sous-traitants

Assure que les données sont traitées uniquement selon les instructions du responsable :.

- Conclusion de contrats de sous-traitance (ADV)
- Audits réguliers des sous-traitants

3. Intégrité des données

Contrôle d'intégrité

Protection contre les modifications accidentelles ou non autorisées :

- Mise en œuvre d'un ISMS garantissant l'intégrité des données et mis régulièrement à jour
- Réaction rapide et documentée aux incidents de sécurité via notre CSIRT
- Surveillance continue des modifications de données via un système de monitoring
- Gestion complète des identités et des accès
- Tests de pénétration réguliers et programme de Bug Bounty actif
- Formations conformes à l'OWASP Top 10 sur le développement sécurisé de logiciels
- Plans d'urgence efficaces en cas d'atteinte à l'intégrité des données

Contrôle de la disponibilité

Assure l'accessibilité et la fonctionnalité continues des systèmes et des données :

- Utilisation d'outils de sécurité, tels que des scanners de logiciels malveillants
- Opérations en cloud redondantes pour les applications iomarket
- Sauvegardes régulières garantissant la disponibilité et la restauration des données
- Systèmes de détection incendie et fumée
- Concepts de sauvegarde et de restauration
- Plan de réponse aux situations d'urgence
- Salle serveur climatisée

4. Mesures organisationnelles (Art. 26 DSG)

Englobent la structure et les processus internes :

- Structure organisationnelle adaptée pour la sécurité de l'information et intégration dans les processus globaux
- Implication cohérente du responsable de la sécurité de l'information (ISO)
- Formation de tout le personnel à la sécurité de l'information et à la protection des données
- Communication régulière sur les nouveautés relatives à la sécurité et à la protection des données
- Les principes de sécurité de l'information sont intégrés dans les processus métier et renforcés par des formations continues et des contrôles des compétences

5. Type et finalité du traitement

Dans le cadre de l’exécution du contrat de prestation :

Catégories de données personnelles traitées

- Données de base clients : nom, prénom, date de naissance, adresse, nationalité, etc.
- Données des clients du clien
- Données des personnes concernées du client
- Données de base des collaborateurs
- Données d’adresses : rue, numéro, NPA, ville, pays
- Métadonnées et données de communication (ex. téléphone, e-mail)
- Données de livraison : biens, quantités, lieux et dates de livraison, destinataires
- Données de facturation : factures clients, factures fournisseurs
- Données de contenu du client

Catégories de personnes concernées

Les données personnelles des catégories de personnes suivantes sont concernées :

- Kundendaten
- Lieferantendaten
- Mitarbeiter des Kunden
- Externe Mitarbeiter des Kunden
- Endkunden des Kunden
- Betroffene des Kunden
- Dienstleister des Kunden
- Données clients
- Données fournisseurs
- Collaborateurs du client
- Collaborateurs externes du client
- Clients finaux du client
- Personnes concernées du client
- Prestataires de services du client

But du traitement des données

Le type de traitement comprend toutes les formes de traitement au sens de la DSG. Les « buts » sont les mesures nécessaires à la fourniture de la prestation convenue.

Le traitement des données comprend le stockage des données, l'accès aux données, l'enregistrement et l'analyse des journaux d'activité. Le traitement des données a lieu exclusivement dans un environnement applicatif sécurisé avec des droits d'accès appropriés. Le sous-traitant est autorisé à traiter, sur ses systèmes, les données personnelles dans la

mesure nécessaire à l'accomplissement de ses tâches.
Le traitement des données personnelles a pour but :

● l'automatisation des processus débiteurs et créditeurs du responsable du traitement.

L'étendue et le but du traitement des données résultent également du contrat de prestations.

Les parties conviennent expressément que les obligations définies dans le présent accord en matière de traitement des données personnelles s'appliquent à tout moment, dès lors et tant que le sous-traitant traite des données personnelles du responsable du traitement.

Lieu du traitement des données

Le traitement a lieu exclusivement en Suisse. Il est interdit au sous-traitant de traiter des données personnelles en dehors de la Suisse.

Restitution et suppression

Après la fin de la prestation convenue, le prestataire s'engage à supprimer ou à restituer toutes les données personnelles, selon le choix du responsable du traitement, sauf obligation légale de conservation des données personnelles en vertu du droit applicable à la protection des données ou d'autres dispositions légales applicables. La suppression des données a lieu 30 jours après la fin de la prestation.

6. Sensibilisation et formation

Formations du personnel

Mesures régulières de sensibilisation à la protection des données :

- Programmes d’apprentissage en ligne
- Formations en présentiel sur des thèmes liés au DSG

7. Amélioration continue

Audit et révision

Vérification régulière de l'efficacité des mesures mises en œuvre :

- Audits internes et externes
- Analyse d'impact relative à la protection des données (DPIA)