DE / EN

Accord sur le traitement des données (DPA)

1 Introduction

Le présent accord sur le traitement des données ("accord sur le traitement des données") est conclu à compter du contrat principal et pour la durée de celui-ci, par et entre les parties.

Sous réserve des dispositions du contrat principal, le Responsable de traitement et le Sous-traitant ont conclu le présent DPA pour le traitement des données à caractère personnel.

- Une description du traitement, des finalités et des transferts figure à l'annexe 1.
- Les mesures organisationnelles et techniques prises par le Sous-traitant sont décrites dans l'annexe 2.
- L'annexe 3 présente une vue d'ensemble des Sous-traitants ultérieurs auxquels le Sous-traitant a recours.

La durée, le terme et la résiliation du présent DPA suivent la durée du contrat principal. Les termes qui ne sont pas définis dans le présent document ont la signification qui leur est donnée dans le contrat principal ou dans les lois sur la protection des données applicables.

Les parties cherchent à mettre en œuvre un accord de traitement des données qui soit conforme aux exigences du cadre juridique actuel en matière de protection des données, soit la loi fédérale suisse sur la protection des données (LPD) ainsi que, dans la mesure où celles-ci sont applicables au Responsable de traitement, les lois cantonales en matière de protection des données ou le règlement général sur la protection des données (RGPD).

En considération du contrat principal, les parties conviennent de ce qui suit.

2 Définitions et interprétation

Sauf définition contraire, les termes et expressions utilisés dans le présent DPA ont la signification suivante :

"Données à caractère personnel" : toutes les données personnelles traitées par le Sous-traitant pour le compte du Responsable du traitement en vertu du contrat principal ou en rapport avec celui-ci.

"Responsable de traitement" : aux fins du présent DPA, la partie qui détermine les finalités et les moyens du traitement des données à caractère personnel conformément aux lois suisses sur la protection des données ou aux lois de l'UE sur la protection des données.

"Sous-traitant", aux fins du présent DPA, la partie qui traite les données à caractère personnel pour le compte du Responsable du traitement conformément aux lois suisses sur la protection des données ou aux lois de l'UE sur la protection des données.

“Sous-traitant ultérieur" : toute personne désignée par le Sous-traitant ou en son nom pour traiter les données à caractère personnel pour le compte du Responsable de traitement dans le cadre du contrat principal.

Les termes utilisés mais non définis dans le présent DPA, tels que "violation de données à caractère personnel", "traitement", "transfert", "profilage" et "personne concernée" auront la même signification que celle énoncée à l'article 5 de la LPD, indépendamment du fait que la LPD s'applique ou non, et leurs termes apparentés seront interprétés en conséquence.

3 Traitement des données à caractère personnel

Le Sous-traitant doit:

- se conformer à toutes les lois applicables en matière de protection des données dans le cadre du traitement des données à caractère personnel ; et
- ne pas traiter les données personnelles autrement que selon les instructions documentées du Responsable de traitement.

Le Responsable du traitement donne instruction au Sous-traitant de traiter les données à caractère personnel dans le cadre de l'exécution du contrat principal. Le Sous-traitant informe immédiatement le Responsable du traitement s'il estime qu'une instruction émise par le Responsable du traitement enfreint les dispositions légales. Le Sous-traitant a le droit, sans reconnaître l'obligation de vérifier l'existence d'une instruction illégale, de rejeter ou de suspendre une instruction qu'il estime illégale jusqu'à ce qu'elle soit confirmée ou modifiée par le Responsable du traitement, ou de rejeter à tout moment des instructions manifestement illégales ou de suspendre le traitement qui s'y rapporte.

Le Sous-traitant s'engage à traiter les données à caractère personnel uniquement aux fins des activités visées dans le présent DPA ou dans le contrat principal. Le Sous-traitant garantit qu'il n'utilisera pas les données personnelles qu'il traite dans le cadre du présent DPA à ses propres fins ou à celles de tiers sans le consentement écrit exprès du Responsable du traitement, à moins qu'une disposition légale obligatoire ne l'y oblige. Dans ce cas, le Sous-traitant informe immédiatement le Responsable de traitement de cette exigence légale avant de traiter ces informations, à moins que la loi n'interdise explicitement une telle divulgation.

Le Sous-traitant peut utiliser et traiter les données personnelles dans le cadre de ses activités commerciales légitimes, comme indiqué dans l'annexe 1 et dans les limites fixées dans ladite annexe.

4 Confidentialité, divulgation des données personnelles

Le Responsable du traitement, le Sous-traitant et le Sous-traitant ultérieur doivent préserver la confidentialité de toutes les informations qu'ils reçoivent conformément aux dispositions pertinentes en matière de confidentialité énoncées dans le contrat principal et dans le présent DPA.

Le Sous-traitant ne divulgue pas les données à caractère personnel, sauf

- sur instructions du Responsable de traitement ;
- comme décrit dans le présent DPA ; ou
- comme l'imposent des dispositions légales impératives.

Le Sous-traitant ne divulguera pas de données personnelles à un organisme gouvernemental, sauf si la loi l'exige. S'il est contraint de divulguer des données à caractère personnel à un organisme gouvernemental, le Sous-traitant renverra, dans la mesure du possible, l'organisme gouvernemental demandeur au Responsable du traitement. Le Sous-traitant notifiera rapidement le Responsable de traitement d'une telle demande pour permettre au Responsable de traitement de chercher une solution appropriée, sauf si la loi l'interdit. Le Sous-traitant examinera toutes les demandes et contestera toute demande qu'il juge excessive ou inappropriée (par exemple, si une telle demande est contraire à la législation suisse. Si, après avoir épuisé les mesures décrites dans la présente section, le Sous-traitant reste contraint de divulguer des données à caractère personnel, il ne divulguera que la quantité minimale de données à caractère personnel nécessaire pour répondre à la demande.

Le Sous-traitant ne fournira à aucun tiers :

- un accès direct, indirect, généralisé ou sans entrave aux données personnelles ;
- les clés de cryptage utilisées pour sécuriser les données à caractère personnel ou la capacité de casser ce cryptage ; ou
- l'accès aux données à caractère personnel si le Responsable du traitement sait que ces données doivent être utilisées à des fins autres que celles indiquées dans la demande du tiers.

À l'appui de ce qui précède, le Sous-traitant peut fournir au tiers les coordonnées de base du Responsable de traitement.

Le Responsable du traitement est seul Responsable de la décision et de la procédure de divulgation des informations concernées aux autorités publiques/organismes gouvernementaux et doit être assisté par le Sous-traitant au mieux de ses capacités dans le cadre de cette divulgation.

5 Personnel du Sous-traitant

Le Sous-traitant prend des mesures raisonnables pour garantir la fiabilité de tout employé, agent, contractant ou Sous-traitant qui peut avoir accès aux données à caractère personnel, en veillant dans chaque cas à ce que l'accès soit strictement limité aux personnes qui ont besoin de connaître les données à caractère personnel pertinentes ou d'y accéder, dans la mesure où cela est strictement nécessaire aux fins de le contrat principal, et pour se conformer aux lois applicables dans le cadre des fonctions de cette personne auprès du Sous-traitant, en veillant à ce que toutes ces personnes soient soumises à des engagements de confidentialité ou à des obligations professionnelles ou légales de confidentialité.

6 Sécurité

Compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du risque de probabilité et de gravité variables pour les droits et libertés des personnes physiques, le Sous-traitant met en œuvre, en ce qui concerne les données à caractère personnel, les mesures techniques et organisationnelles mentionnées dans l'annexe 2 pour assurer un niveau de sécurité adapté à ce risque, y compris, le cas échéant, les mesures visées dans les lois sur la protection des données applicables.

Lors de l'évaluation du niveau de sécurité approprié, le Sous-traitant tient compte des risques présentés par le traitement, en particulier en cas de violation des données à caractère personnel.

7 Transfert de données

Le Sous-traitant ne peut transférer ou autoriser le transfert de données vers des pays situés en dehors de la Suisse ou de l'Espace économique européen sans l'accord écrit préalable du Responsable du traitement. Si les données personnelles traitées en vertu du présent DPA sont transférées de la Suisse ou d'un pays de l'Espace économique européen vers un pays situé en dehors de l'Espace économique européen, les Parties veilleront à ce que les données personnelles soient protégées de manière adéquate. Pour ce faire, les parties s'appuient, sauf accord contraire, sur une décision d'adéquation prise par les autorités suisses ou sur les clauses contractuelles types approuvées par l'UE ou la Suisse pour le transfert de données à caractère personnel.

8 Sous-traitance ultérieure

Le sous-traitant ne nomme pas (ou ne divulgue pas de données personnelles à) un sous-traitant ultérieur à moins que le responsable du traitement ne l'exige ou ne l'autorise préalablement.

Le Sous-traitant impose à chaque Sous-traitant secondaire de respecter les obligations de confidentialité, de notification, de transfert et les mesures de sécurité relatives au traitement des données à caractère personnel, ces obligations et mesures devant au moins être

conformes aux dispositions du présent DPA. Le Sous-traitant reconnaît être conjointement et solidairement responsable du respect des obligations imposées au Sous-traitant ultérieur en vertu du présent DPA.

L'annexe 3 liste les Sous-traitants ultérieurs auxquels le Sous-traitant a recours. La modification des Sous-traitants désignés dans ladite annexe ou l'utilisation de Sous-traitants supplémentaires est autorisée si :

- le Sous-traitant indique à l'avance au Responsable de traitement cette externalisation vers des Sous-traitants ultérieurs par écrit ou sous une forme électronique appropriée dans un délai raisonnable, qui ne peut être inférieur à 14 jours ; et
- le Responsable du traitement ne s'oppose pas à l'externalisation prévue par écrit ou sous une forme électronique appropriée au Sous-traitant au moment de la divulgation ou de la transmission des données ; et
- la sous-traitance repose sur un contrat conforme à l'article 9 de l'OPDo ou à l'article 28 du RGPD, respectant ainsi le niveau de protection des données et de sécurité du traitement des données requis pour le traitement.

9 Droits de la personne concernée

Compte tenu de la nature du traitement, le Sous-traitant aide le Responsable du traitement en mettant en œuvre les mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour que le Responsable du traitement puisse s'acquitter de ses obligations, telles qu'il les conçoit raisonnablement, de répondre aux demandes d'exercice des droits des personnes concernées en vertu des lois sur la protection des données.

Le Sous-traitant:

- notifie rapidement le Responsable de traitement s'il reçoit une demande de la part d'une personne concernée en vertu de toute loi sur la protection des données en ce qui concerne les données personnelles ; et
- s'assure qu'il ne répond pas à cette demande, sauf sur instructions documentées du Responsable de traitement.

10 Violation de données à caractère personnel

En cas de violation de la sécurité des données à caractère personnel, le Sous-traitant coopère avec le Responsable de traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent.

En cas de violation de la sécurité en rapport avec des données **traitées par le Responsable de traitement**, le Sous-traitant prête assistance au Responsable de traitement aux fins de :

- notifier l'autorité de contrôle compétente, dans les meilleurs délais après que le Responsable de traitement a eu connaissance de la violation.
- obtenir les informations devant figurer dans la notification.

En cas de violation de la sécurité en rapport **avec des données traitées par le Sous-traitant**, celui-ci en informe le Responsable de traitement dans les meilleurs délais après en avoir pris connaissance. La notification au Responsable du traitement contient au moins les informations suivantes

- une description de l'incident de violation de données à caractère personnel ;
- des informations sur les données et les catégories de données concernés ainsi que l'estimation du nombre de personnes concernées ;
- une évaluation préliminaire des conséquences probables de la violation.
- une description des mesures et/ou des propositions de mesures déjà prises/à prendre par le Sous-traitant pour éviter ou atténuer les conséquences négatives pour les personnes concernées.

Les notifications d'incidents de sécurité sont adressées au délégué à la protection des données du Responsable du traitement ou à tout autre employé faisant office de point de contact, par tout moyen de communication approprié choisi par le Sous-traitant, y compris les courriels.

La notification ou la réponse du Sous-traitant à un incident de sécurité en vertu de la présente section ne constitue pas une reconnaissance par le Sous-traitant d'une faute ou d'une responsabilité à l'égard de l'incident de sécurité.

11 Analyse d'impact sur la protection des données

Le Sous-traitant assiste le Responsable de traitement dans les analyses d'impact sur la protection des données et les consultations avec les autorités compétentes en matière de confidentialité, lorsque le responsable de traitement le juge nécessaire. Cette assistance concerne uniquement le traitement des données personnelles effectué par le Sous-traitant et tient compte de la nature du traitement ainsi que des informations à sa disposition.

En cas de demandes fréquentes ou ayant un impact significatif sur ses ressources, le Sous-traitant peut demander une indemnisation raisonnable pour le travail fourni.

12 Restitution et suppression des données

Le Sous-traitant ne conserve pas les données à caractère personnel au-delà de la durée convenue avec le Responsable de traitement dans le contrat principal.

En cas de résiliation du contrat principal, le Responsable de traitement peut soit exporter ses données selon la procédure disponible en ligne, soit faire appel au service de support pour obtenir une copie de l'ensemble des données dans un format permettant leur ré-exploitation.

Le sous-traitant garantit que l'ensemble des données, y compris les sauvegardes, seront définitivement détruites dans un délai maximum de 3 (trois) mois suivant la fin de la relation contractuelle. Ce délai de rétention est rendu nécessaire d'un point de vue technique.

Compte tenu de l'automatisation de la procédure de suppression des données, la présente clause vaut pour attestation de confirmation de destruction.

13 Droits d'audit et inspections

Sous réserve de la présente section ou de toute autre disposition du contrat principal, le Sous-traitant autorise le responsable du traitement à effectuer des contrôles sur le respect des mesures techniques et organisationnelles.

Le Responsable de traitement peut faire appel à un tiers indépendant pour effectuer l'audit en son nom, à condition que le tiers soit accepté par le Responsable de traitement et le Sous-traitant. Les audits doivent être effectués pendant les heures normales d'ouverture, sous réserve des politiques du Sous-traitant, et ne doivent pas interférer de manière déraisonnable avec les activités commerciales et techniques du Sous-traitant. Ils doivent être notifiés au moins 14 jours à l'avance.

Le Sous-traitant fournira les ressources raisonnables et la documentation nécessaires pour soutenir les audits conformément à la LPD, en particulier pour prouver la mise en œuvre des mesures techniques et organisationnelles. La preuve des mesures techniques et organisationnelles visant à respecter les exigences particulières de la protection des données en général ainsi que celles relatives à la commande peut être apportée par:

- des attestations, des rapports ou des extraits de rapports actuels d'organismes indépendants ;
- une certification appropriée par un audit de sécurité informatique ou de protection des données.

Les Parties conviennent que les inspections sur place ne sont nécessaires que si le respect des obligations du Sous-traitant en vertu des articles 8 et 9 LPD ne peuvent pas déjà être prouvées par des éléments de preuve susmentionnés. En outre, les inspections sur place effectuées par le Responsable du traitement doivent être justifiées par une raison particulière et ne sont autorisées plus d'un jour d'audit par an et que dans des cas exceptionnels.

Aucune disposition de la présente section n'oblige le Sous-traitant à manquer à ses obligations de confidentialité vis-à-vis de ses clients ou de ses employés.

En cas d'inspection nécessaire (sur place) par le Responsable du traitement dans les locaux du Sous-traitant, chaque partie supporte ses coûts encourus pour l'inspection, tels que les frais d'inspection, de personnel et de déplacement. Si la coopération du Sous-traitant dans le cadre des inspections dépasse la mesure requise conformément à la présente section et si cela est associé à des frais d'inspection plus élevés ou au recours à des prestataires de services externes par le Sous-traitant, les coûts encourus à ce titre peuvent être facturés au Responsable du traitement selon les taux horaires et journaliers habituels dans l'industrie.

14 Conditions générales

Nonobstant ce qui précède, outre les dispositions applicables énoncées dans le contrat principal, tous les avis et communications donnés en vertu du présent DPA doivent être faits par écrit et envoyés par courrier électronique.

En ce qui concerne la résiliation du présent DPA, les dispositions spécifiques du contrat principal s'appliquent.

15 Droit applicable et juridiction compétente

Le choix de la loi et de la juridiction compétente est conforme aux dispositions applicables au contrat principal.

dsindip

Accord sur le traitement des données (DPA)

Annexe 1 : Description du traitement - application dsi indip

Catégories de personnes dont les données sont traitées	Personnes bénéficiaires de prestations d'institutions actives dans les domaines du social, de la santé et de l'éducation tels que les EMS, la réinsertion, le suivi de personnes en situation de handicap, la pédagogie spécialisée (liste non exhaustive).
Catégories de données personnelles	Données personnelles des bénéficiaires : nom, prénom, adresses email et postale, téléphone, no avs, copie de passeport ou carte d'identité, état civil, genre, date de naissance, lieu d'origine.
	Informations complémentaires telles que des données liées à la famille, aux relations personnelles ou la situation financière, à des événements personnels, au type de curatelle ou autres informations nécessaires à la prise en charge des bénéficiaires.
	Dossier administratif : assurances, contacts internes et externes, médecins traitants, séjours réalisés.
	Données d'utilisation de l'application: fichiers journaux, données d'authentification, historique de connexion, adresses IP, …
Catégories de données sensibles	Données de santé: dossiers de patients comprenant anamnèse, état de santé physique ou psychique, résultats de tests, groupe sanguin, caractéristiques physiques, observations, traitements, projets personnels, médication
	Données liées à des jugements, mesures administratives ou restrictives dont les personnes concernées peuvent faire l'objet.
	Autres données sensibles liées à la religion, l'ethnicité ou la sphère intime.
En sus dans indip	*Analyses graphiques, indicateurs avancés, tableaux de bord, questionnaires permettant le suivi objectif de l'évolution des bénéficiaires.*
Nature du traitement	Gestion des données du responsable de traitement saisies dans l'application dsi indip.
	Conseil et support informatique pour les utilisateurs désignés par le responsable de traitement.
Finalités du traitement	Fournir aux utilisateurs de dsi et indip une information centralisée, sécurisée et facilement accessible pour tous les intervenants.
Activités légitimes du Sous-traitant	Établissement de statistiques comparatives sur la base de données anonymisées exclusivement.
Lieux d'hébergement des données	Data centers en Suisse

dsindip

Accord sur le traitement des données (DPA)

Annexe 2 : Mesures techniques et organisationnelles

Gouvernance & organisation	Tipee a mis en place et tient à jour un Système de Management de la Sécurité de l'Information (SMSI) conforme aux standards actuels. Les rôles et responsabilités en matière de sécurité sont définis et attribués. Le CTO et le DPO sont directement rattachés à la Direction générale. Les cyber risques et les politiques de sécurité sont revus périodiquement, au minimum une fois par an, et les ressources nécessaires adaptées en conséquence.
Audits, certifications	Des tests de pénétration sur les différentes applications sont réalisés à intervalle réguliers par un prestataire externe spécialisé.
Développement et hébergement en Suisse	Tipee développe ses applications avec ses propres développeurs en Suisse. Les solutions ainsi que les données personnelles qu'elles contiennent sont hébergées dans des datacenters de prestataires certifiés ISO 27001, tous basés en Suisse (cf. annexe 3)
Cycle de développement sécurisé	Nos équipes de développement appliquent des pratiques de sécurité intégrées à chaque étape du cycle de vie logiciel. Nous effectuons régulièrement des revues de code par les pairs, des tests de sécurité automatisés et des analyses de vulnérabilités. Des tests de pénétration sont régulièrement réalisés par une entreprise externe spécialisée en cybersécurité pour évaluer objectivement la robustesse de nos applications. Nos développeurs sont sensibilisés aux risques de sécurité courants (OWASP Top 10) et utilisent des bibliothèques fiables dont les dépendances sont systématiquement vérifiées. La séparation des environnements de développement, de test et de production, associée à un processus de validation progressive, nous permet de minimiser les risques d'introduction de failles de sécurité dans nos applications. Nous applique une approche de "sécurité par la conception" où les considérations de protection des données sont intégrées dès les premières phases de conception.
Sécurité des données	Les données en transit sont chiffrées au moyen du protocole TLS. Les données statiques, les identifiants des utilisateurs ainsi que les sauvegardes sont également chiffrés au moyen de technologies adaptées et constamment tenues à jour.
Confidentialité	Les données sont strictement compartimentées afin d'assurer un traitement confidentiel des informations de chaque client.

	L'architecture de l'application garantit l'étanchéité des données grâce à des bases de données dédiées et des périmètres spécifiques. Les employés de tipee sont contractuellement liés par des clauses de confidentialité et de respect du secret des affaires.
Disponibilité	Tous les éléments de notre infrastructure sont résilients aux pannes techniques grâce à la redondance des équipements. Les services sont monitorés 24h/7/365 par notre équipe de support. Les remontées d'alertes sont traitées immédiatement, de jour comme de nuit. Les sauvegardes régulières et nos procédures de reprise en cas d'incident permettent une restauration rapide des services.
Contrôle d'accès	Les accès des clients à tipee sont protégés par la combinaison du nom de l'utilisateur et de son mot de passe. Un second facteur d'authentification ou des clés d'accès sont des fonctionnalités disponibles pour permettre aux utilisateurs de sécuriser leur authentification. Au sein de l'application, des rôles utilisateurs permettent de définir précisément l'accès aux informations. Il est de la responsabilité de chaque client de définir et implémenter sa politique de gestion des droits d'accès et les méthodes d'authentification. En ce qui concerne les accès des collaborateurs de Tipee aux différents systèmes, ils sont limités selon les principes du privilège minimum et systématiquement protégés par une identification à double facteur.
Sauvegardes	Afin de minimiser le risque de perte de données, les bases de données de l'application sont intégralement sauvegardées chaque heure et la procédure de restauration régulièrement testée. Les sauvegardes sont chiffrées et entreposées sur des sites distincts. Elles sont conservées conformément à notre politique de rétention ainsi qu'aux engagements contractuels du présent DPA.
Mise à jour des systèmes	Les systèmes sont mis à jour en permanence. De manière générale, la redondance de l'infrastructure et les procédures en place permettent d'effectuer les opérations de maintenance sans interruption de service. Des notifications préalables sont adressées par email aux clients dans le cas où un arrêt des systèmes ne peut être évité.
Formation du personnel	Les politiques et procédures de sécurité sont communiquées à l'ensemble du personnel. Des formations relatives à la cybersécurité ainsi que des mesures du niveau de vigilance sont effectuées plusieurs fois par année.

Accord sur le traitement des données (DPA)

Incidents de sécurité et continuité d'activité	Tipee dispose d'un plan de reprise en cas d'incident, régulièrement testé et amélioré conformément aux exigences de son système de management de la sécurité de l'information.
Protection dès la conception et par défaut	Les principes de protection dès la conception et par défaut sont intégrés pour tout nouveau développement. Des analyses d'impact sont réalisées si les circonstances ou les lois l'exigent.
Journalisation / traçabilité	Notre infrastructure technique intègre un système complet de journalisation et de traçabilité qui capture les événements significatifs liés à la sécurité. Les journaux d'activité sont centralisés et conservés pour une durée conforme aux bonnes pratiques du secteur, permettant une analyse efficace en cas d'incident. Nous surveillons en continu les accès aux systèmes critiques, les modifications de configuration et les comportements anormaux grâce à des outils de détection. Les informations sensibles sont exclues des journaux pour respecter la confidentialité des données.

dsindip

Accord sur le traitement des données (DPA)

Annexe 3 : Liste des sous-traitants application dsi indip

Pour fournir ses prestations, tipee SA sélectionne soigneusement ses sous-traitants, lesquels sont retenus pour la qualité et la fiabilité de leurs services ainsi que leurs bonnes pratiques en matière de sécurité. Leur conformité par rapport aux exigences légales est régulièrement évaluée afin que les engagements pris par tipee SA envers ses clients puissent être assurés de bout en bout.

Par souci de transparence ainsi qu'en réponse à certaines obligations légales, tipee SA publie la liste de ses sous-traitants en indiquant la finalité du traitement externalisé ainsi que le lieu d'hébergement des données.

Sous-traitant	**Finalité**	**Localisation des données**
Infrastructure		
Infomaniak	Hébergement et backups	CH
Google Cloud Platform	Hébergement *(Indip uniquement)* et backups	CH
Services		
Datadog	Monitoring et gestion des logs techniques	EU
Google Analytics	Analyse des moyens techniques utilisés sur les applications (OS, navigateur, résolution, etc.)	Global
Support administratif et service client		
Zoho	Support client et marketing	EU
Outils internes		
Google Workspace	Messagerie & suite bureautique	EU
Atlassian (Cloud)	Développement, gestion des bugs	CH
Slack	Communication interne	USA

Abkommen über die Datenverarbeitung (ADV)

1 Einführung

Diese Vereinbarung zur Datenverarbeitung ("Vereinbarung zur Datenverarbeitung") wird ab dem Hauptvertrag und für die Dauer desselben von und zwischen den Parteien geschlossen.

Vorbehaltlich der Bestimmungen des Hauptvertrags haben der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter dieses ADV für die Verarbeitung personenbezogener Daten geschlossen.

- Eine Beschreibung der Verarbeitung, des Zwecks und der Übermittlungen findet sich in Anhang 1.
- Die organisatorischen und technischen Maßnahmen, die der Auftragsverarbeiter ergreift, sind in Anhang 2 beschrieben.
- Anhang 3 gibt einen Überblick über die nachfolgenden Auftragsverarbeiter, die der Auftragsverarbeiter einsetzt.

Die Dauer, die Laufzeit und die Kündigung dieses ADV folgen der Laufzeit des Hauptvertrags. Begriffe, die hier nicht definiert sind, haben die Bedeutung, die ihnen im Hauptvertrag oder in den geltenden Datenschutzgesetzen zugewiesen wird.

Die Parteien streben mit diesem ADV an, den Anforderungen des geltenden Datenschutzrechts zu entsprechen, namentlich dem Schweizer Bundesgesetz über den Datenschutz (DSG) sowie – sofern auf den Verantwortlichen anwendbar – kantonalen Datenschutzgesetzen oder der **Datenschutz-Grundverordnung der EU (DSGVO)**.

In Anbetracht des Hauptvertrags vereinbaren die Parteien Folgendes.

2 Definitionen und Auslegung

Sofern nicht anders definiert, haben die in diesem ADV verwendeten Begriffe und Ausdrücke folgende Bedeutung:

"Personenbezogene Daten": alle personenbezogenen Daten, die der Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen des Hauptvertrags oder in Verbindung mit diesem verarbeitet.

"Verantwortlicher": Im Sinne dieses ADV die Partei, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten gemäß den schweizerischen oder europäischen Datenschutzgesetzen entscheidet.

"Auftragsverarbeiter" im Sinne dieses ADV die Partei, die personenbezogene Daten im Auftrag des Verantwortlichen gemäß den schweizerischen Datenschutzgesetzen oder den Datenschutzgesetzen der EU verarbeitet.

"Unter Auftragsverarbeiter": jede Person, Auftragsverarbeiter beauftragt wird oder in dessen Namen personenbezogene Daten im Rahmen des Hauptvertrags für den Verantwortlichen verarbeitet.

Die in diesem ADV verwendeten, aber nicht definierten Begriffe wie "Verletzung des Schutzes personenbezogener Daten", "Verarbeitung", "Übermittlung", "Profiling" und "betroffene Person" haben unabhängig davon, ob das DSG Anwendung findet, dieselbe Bedeutung wie in Artikel 5 DSG, und ihre verwandten Begriffe werden entsprechend ausgelegt.

3 Verarbeitung von personenbezogenen Daten

Der Auftragsverarbeiter muss:

- bei der Verarbeitung personenbezogener Daten alle geltenden Datenschutzgesetze einhalten; und
- personenbezogene Daten nicht anders als gemäß den dokumentierten Anweisungen des Verantwortlichen zu verarbeiten.

Der Verantwortliche weist den Auftragsverarbeiter an, die personenbezogenen Daten im Rahmen der Erfüllung des Hauptvertrags zu verarbeiten. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Ansicht ist, dass eine vom Verantwortlichen erteilte Weisung gegen gesetzliche Bestimmungen verstößt. Der Auftragsverarbeiter hat das Recht, ohne Anerkennung der Verpflichtung, das Vorliegen einer rechtswidrigen Weisung zu prüfen, eine Weisung, die er für rechtswidrig hält, abzulehnen oder auszusetzen, bis sie vom Verantwortliche bestätigt oder geändert wird, oder er hat das Recht, offensichtlich rechtswidrige Weisungen jederzeit abzulehnen oder die damit verbundene Verarbeitung auszusetzen.

Der Verantwortliche erteilt dem Auftragsverarbeiter die Weisung, personenbezogene Daten im Rahmen der Erfüllung des Hauptvertrags zu verarbeiten. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Ansicht ist, dass eine Weisung des Verantwortlichen gegen geltendes Recht verstößt. Der Auftragsverarbeiter ist berechtigt, ohne Anerkennung einer Prüfungspflicht eine offensichtlich rechtswidrige Weisung abzulehnen oder auszusetzen, bis sie vom Verantwortlichen bestätigt oder angepasst wurde, oder diese jederzeit zurückzuweisen.

Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten ausschließlich zu den im AVV oder Hauptvertrag genannten Zwecken zu verarbeiten. Der Auftragsverarbeiter gewährleistet, dass er die im Rahmen dieses AVV verarbeiteten personenbezogenen Daten nicht zu eigenen oder fremden Zwecken nutzt, es sei denn, eine zwingende gesetzliche Vorschrift schreibt dies vor. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über die gesetzliche Verpflichtung, sofern das Gesetz eine solche Mitteilung nicht ausdrücklich untersagt.

Der Auftragsverarbeiter darf personenbezogene Daten im Rahmen seiner legitimen Geschäftstätigkeit nur in dem in Anhang 1 beschriebenen Umfang und unter den dort genannten Bedingungen verwenden und verarbeiten.

4 Vertraulichkeit, Offenlegung persönlicher Daten

Der Verantwortliche, der Auftragsverarbeiter und der nachfolgende Auftragsverarbeiter müssen alle Informationen, die sie erhalten, gemäß den relevanten Vertraulichkeit Bestimmungen, die im Hauptvertrag und in diesem ADV festgelegt sind, vertraulich behandeln.

Der Auftragsverarbeiter legt die personenbezogenen Daten nicht offen, es sei denn

- auf Anweisung des Verantwortliche ;
- wie in diesem ADV beschrieben; oder
- wie es durch zwingende gesetzliche Bestimmungen vorgeschrieben ist.

Der Auftragsverarbeiter wird keine personenbezogenen Daten an eine Regierungsbehörde weitergeben, es sei denn, dies ist gesetzlich vorgeschrieben. Wenn er gezwungen wird, personenbezogene Daten gegenüber einer Regierungsbehörde offenzulegen, wird der Auftragsverarbeiter, soweit möglich, die anfragende Regierungsbehörde an den Verantwortlichen verweisen. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen für die Datenverarbeitung umgehend über eine solche Anfrage, damit der Verantwortliche für die Datenverarbeitung nach einer geeigneten Lösung suchen kann, sofern dies nicht gesetzlich verboten ist. Der Auftragsverarbeiter wird alle Anträge prüfen und jeden Antrag bestreiten, den er für übertrieben oder unangemessen hält (z. B. wenn ein solcher Antrag gegen das Schweizer Recht verstößt. Wenn der Auftragsverarbeiter nach Ausschöpfung der in diesem Abschnitt beschriebenen Maßnahmen weiterhin gezwungen ist, personenbezogene Daten offenzulegen, wird er nur die Mindestmenge an personenbezogenen Daten offenlegen, die zur Beantwortung der Anfrage erforderlich sind.

Der Auftragsverarbeiter wird keine Dritten beliefern :

- einen direkten, indirekten, allgemeinen oder ungehinderten Zugang zu personenbezogenen Daten ;
- die Verschlüsselungsschlüssel, die zur Sicherung der personenbezogenen Daten verwendet werden, oder die Fähigkeit, diese Verschlüsselung zu brechen; oder
- Zugang zu personenbezogenen Daten, wenn dem Verantwortlichen bekannt ist, dass diese Daten für andere als die im Antrag des Dritten angegebenen Zwecke verwendet werden sollen.

Zur Unterstützung des Vorstehenden kann der Auftragsverarbeiter dem Dritten die grundlegenden Kontaktdaten des Verantwortlichen zur Verfügung stellen.

Der Verantwortliche ist allein verantwortlich für die Entscheidung und das Verfahren zur Offenlegung personenbezogener Daten gegenüber Behörden und wird dabei vom Auftragsverarbeiter bestmöglich unterstützt.

5 Personal des Auftragsverarbeiters

Der Auftragsverarbeiter ergreift angemessene Maßnahmen, um die Zuverlässigkeit jedes Mitarbeiters, Beauftragten, Unter Auftragsverarbeiter oder Dritten sicherzustellen, der Zugang zu personenbezogenen Daten erhalten kann. Er stellt dabei sicher, dass der Zugang auf diejenigen Personen beschränkt ist, die diese Daten kennen oder verarbeiten müssen, soweit dies für die Erfüllung des Hauptvertrags erforderlich ist und um die geltenden Datenschutzvorschriften zu erfüllen. Der Auftragsverarbeiter gewährleistet, dass alle betroffenen Personen einer Vertraulichkeitspflicht unterliegen, sei es durch arbeitsrechtliche, vertragliche oder gesetzliche Verpflichtungen.

6 Sicherheit

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie des Risikos unterschiedlicher Eintrittswahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen, implementiert der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen im Hinblick auf personenbezogene Daten, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, einschließlich – soweit anwendbar – der in den geltenden Datenschutzgesetzen genannten Maßnahmen.

Bei der Bewertung des geeigneten Sicherheitsniveaus berücksichtigt der Auftragsverarbeiter insbesondere die Risiken, die mit der Verarbeitung verbunden sind, insbesondere im Falle einer Verletzung des Schutzes personenbezogener Daten.

7 Übertragung von Daten

Der Auftragsverarbeiter darf ohne die vorherige schriftliche Zustimmung des Verantwortlichen keine Daten in Länder außerhalb der Schweiz oder des Europäischen Wirtschaftsraums übertragen oder die Übertragung von Daten in solche Länder genehmigen. Wenn personenbezogene Daten, die gemäß diesem ADV verarbeitet werden, aus der Schweiz oder einem Land des Europäischen Wirtschaftsraums in ein Land außerhalb des Europäischen Wirtschaftsraums übermittelt werden, stellen die Parteien sicher, dass die personenbezogenen Daten angemessen geschützt werden. Hierzu stützen sich die Parteien, sofern nichts anderes vereinbart wurde, auf einen Angemessenheitsbeschluss der Schweizer Behörden oder auf die von der EU oder der Schweiz genehmigten Standardvertragsklauseln für die Übermittlung personenbezogener Daten.

8 Nachträgliche Vergabe von Unteraufträgen

Der Auftragsverarbeiter ernennt keinen nachfolgenden Unter Auftragsverarbeiter (oder gibt personenbezogene Daten an ihn weiter), es sei denn, der für die Verarbeitung Verantwortliche verlangt dies oder genehmigt es vorab.

Der Auftragsverarbeiter verpflichtet jeden nachfolgenden Unter Auftragsverarbeiter zur Einhaltung der Vertraulichkeits-, Benachrichtigungs-, Übertragung Pflichten und

Sicherheitsmaßnahmen in Bezug auf die Verarbeitung personenbezogener Daten, wobei diese Pflichten und Maßnahmen zumindest den Bestimmungen dieses ADV entsprechen müssen. Der Auftragsverarbeiter bestätigt, dass er gesamtschuldnerisch für die Einhaltung der Verpflichtungen, die dem nachfolgenden Auftragsverarbeiter gemäß diesem ADV auferlegt werden, verantwortlich ist.

Anhang 3 listet die nachfolgenden Auftragsverarbeiter auf, die der Auftragsverarbeiter einsetzt. Die Änderung der in diesem Anhang aufgeführten Auftragsverarbeiter oder die Verwendung zusätzlicher Auftragsverarbeiter ist erlaubt, wenn :

- der Auftragsverarbeiter dem Verantwortliche diese Auslagerung an nachfolgende Auftragsverarbeiter im Voraus schriftlich oder in geeigneter elektronischer Form innerhalb einer angemessenen Frist, die nicht weniger als 14 Tage betragen darf, anzeigt; und
- der Verantwortliche zum Zeitpunkt der Offenlegung oder Übermittlung der Daten keine Einwände gegen die geplante Auslagerung schriftlich oder in einer geeigneten elektronischen Form an den Auftragsverarbeiter erhebt; und
- die Unterauftragsvergabe auf einem Vertrag gemäß Artikel 9 DSV oder Artikel 28 DSGVO beruht und somit das für die Verarbeitung erforderliche Datenschutzniveau und die Sicherheit der Datenverarbeitung eingehalten wird.

9 Rechte der betroffenen Person

Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortliche durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen, soweit dies möglich ist, damit der Verantwortliche seinen Verpflichtungen, wie sie ihm vernünftigerweise erscheinen, nachkommen kann, auf Anträge auf Ausübung der Rechte der betroffenen Personen nach den Datenschutzgesetzen zu reagieren.

Der Auftragsverarbeiter:

- den Verantwortliche umgehend benachrichtigt, wenn er einen Antrag von einer betroffenen Person nach einem beliebigen Datenschutzgesetz in Bezug auf personenbezogene Daten erhält; und
- beantwortet diese Anfrage nur auf dokumentierte Weisung des Verantwortlichen hin.

10 Verletzung von personenbezogenen Daten

Im Falle einer Verletzung der Sicherheit der personenbezogenen Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn bei der Einhaltung seiner Verpflichtungen.

Im Falle einer Sicherheitsverletzung in Bezug auf Daten, die **von dem Verantwortliche verarbeitet** werden, unterstützt der Auftragsverarbeiter den Verantwortliche bei folgenden Aufgaben:

- die zuständige Aufsichtsbehörde so bald wie möglich, nachdem der Verantwortliche von der Verletzung Kenntnis erlangt hat, zu benachrichtigen.
- die Informationen erhalten, die in der Benachrichtigung enthalten sein müssen.

Im Falle einer Sicherheitsverletzung im Zusammenhang **mit Daten, die vom Auftragsverarbeiter verarbeitet** werden, benachrichtigt der **Auftragsverarbeiter** den Verantwortlichen so schnell wie möglich, nachdem er davon Kenntnis erlangt hat. Die Mitteilung an den Verantwortliche enthält mindestens die folgenden Informationen

- eine Beschreibung des Vorfalls der Verletzung des Schutzes personenbezogener Daten ;
- Informationen über die betroffenen Daten und Datenkategorien sowie eine Schätzung der Anzahl der betroffenen Personen ;
- eine vorläufige Bewertung der wahrscheinlichen Folgen des Verstoßes.
- eine Beschreibung der Maßnahmen und/oder Vorschläge für Maßnahmen, die der Auftragsverarbeiter bereits ergriffen hat/ergreifen wird, um die negativen Folgen für die betroffenen Personen zu vermeiden oder abzuschwächen.

Meldungen von Sicherheitsvorfällen sind an den Datenschutzbeauftragten des Verantwortlichen oder an einen anderen Mitarbeiter, der als Kontaktstelle fungiert, über jedes geeignete, vom Auftragsverarbeiter gewählte Kommunikationsmittel, einschließlich E-Mail, zu richten.

Eine solche Meldung oder Reaktion stellt kein Schuldanerkenntnis oder eine Haftungsübernahme des Auftragsverarbeiters dar.

11 Datenschutz-Folgenabschätzung

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei Datenschutz-Folgenabschätzungen und Konsultationen mit den zuständigen Datenschutzbehörden, wenn der für die Verarbeitung Verantwortliche dies für erforderlich hält. Diese Unterstützung bezieht sich nur auf die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter und berücksichtigt die Art der Verarbeitung sowie die dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

Im Falle von Anfragen, die häufig gestellt werden oder sich erheblich auf seine Ressourcen auswirken, kann der Auftragsverarbeiter eine angemessene Entschädigung für die geleistete Arbeit verlangen.

12 Rückgabe und Löschung von Daten

Der Auftragsverarbeiter speichert personenbezogene Daten nicht länger als den Zeitraum, der mit dem Verantwortlichen im Hauptvertrag vereinbart wurde.

Im Falle der Kündigung des Hauptvertrags kann der für die Verarbeitung Verantwortliche entweder seine Daten nach dem online verfügbaren Verfahren exportieren oder den Support-Service in Anspruch nehmen, um eine Kopie aller Daten in einem Format zu erhalten, das ihre Wiederverwendung ermöglicht.

Der Auftragsverarbeiter garantiert, dass alle Daten, einschließlich der Backups, innerhalb einer Frist von maximal 3 (drei) Monaten nach Beendigung des Vertragsverhältnisses

Angesichts des automatisierten Löschprozesses gilt diese Klausel als Bestätigung der Datenvernichtung.

13 Audit-Rechte und Inspektionen

Vorbehaltlich dieses Abschnitts oder einer anderen Bestimmung des Hauptvertrags gestattet der Auftragsverarbeiter dem Verantwortlichen, Kontrollen über die Einhaltung der technischen und organisatorischen Maßnahmen durchzuführen.

Der Verantwortliche kann einen unabhängigen Dritten beauftragen, das Audit in seinem Namen durchzuführen, vorausgesetzt, der Dritte wird vom Verantwortlichen und vom Auftragsverarbeiter akzeptiert. Audits müssen vorbehaltlich der Richtlinien des Auftragsverarbeiters während der normalen Geschäftszeiten durchgeführt werden und dürfen die geschäftlichen und technischen Aktivitäten des Auftragsverarbeiters nicht unangemessen beeinträchtigen. Sie müssen mindestens 14 Tage im Voraus angekündigt werden.

Der Auftragsverarbeiter stellt angemessene Ressourcen und Unterlagen zur Verfügung, um Audits gemäß dem DSG zu unterstützen, insbesondere um die Umsetzung der technischen und organisatorischen Maßnahmen zu belegen. Der Nachweis der technischen und organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes im Allgemeinen sowie der Anforderungen im Zusammenhang mit dem Auftrag kann erbracht werden durch:

- aktuelle Bescheinigungen, Berichte oder Auszüge aus Berichten unabhängiger Einrichtungen ;
- eine angemessene Zertifizierung durch ein Audit der Computersicherheit oder des Datenschutzes.

Die Parteien vereinbaren, dass Vor-Ort-Inspektionen nur dann erforderlich sind, wenn die Einhaltung der Verpflichtungen des Auftragsverarbeiters gemäß Artikel 8 und 9 DSG nicht bereits durch die oben genannten Beweismittel nachgewiesen werden kann. Darüber hinaus müssen Vor-Ort-Inspektionen durch den Verantwortlichen durch einen besonderen Grund gerechtfertigt sein und sind nur an mehr als einem Prüfungstag pro Jahr und nur in Ausnahmefällen zulässig.

Keine Bestimmung dieses Abschnitts verpflichtet den Auftragsverarbeiter, seine Geheimhaltungspflichten gegenüber seinen Kunden oder Mitarbeitern zu verletzen.

Im Falle einer notwendigen Inspektion (vor Ort) durch den Verantwortlichen in den Räumlichkeiten des Auftragsverarbeiters trägt jede Partei ihre für die Inspektion entstandenen Kosten, wie Inspektions-, Personal- und Reisekosten. Wenn die Kooperation des Auftragsverarbeiters bei Inspektionen über das nach diesem Abschnitt erforderliche Maß hinausgeht und dies mit höheren Inspektionskosten oder der Inanspruchnahme externer Dienstleister durch den Auftragsverarbeiter verbunden ist, können die dadurch entstandenen

Kosten dem Verantwortliche nach den branchenüblichen Stunden- und Tagessätzen in Rechnung gestellt werden.

14 Allgemeine Bedingungen

Ungeachtet des Vorstehenden müssen zusätzlich zu den anwendbaren Bestimmungen, die im Hauptvertrag festgelegt sind, alle Mitteilungen und Kommunikationen, die im Rahmen dieses ADV gegeben werden, schriftlich erfolgen und per E-Mail versandt werden.

In Bezug auf die Kündigung dieses ADV gelten die besonderen Bestimmungen des Hauptvertrags.

15 Anwendbares Recht und zuständige Gerichtsbarkeit

Die Wahl des Rechts und des zuständigen Gerichts richtet sich nach den Bestimmungen, die für den Hauptvertrag gelten.

dsindip

Abkommen über die Datenverarbeitung (ADV)

Anhang 1: Beschreibung der Behandlung - dsi indip

Kategorien betroffener Personen	Leistungsempfänger von Institutionen in den Bereichen Soziales, Gesundheit und Bildung, wie z. B. Alters- und Pflegeheime, berufliche oder soziale Wiedereingliederung, Betreuung von Menschen mit Behinderungen sowie Sonderpädagogik (nicht abschließende Aufzählung).
Kategorien personenbezogenen Daten	Personenbezogene Daten der Leistungsempfänger: Name, Vorname, E-Mail-Adresse, Postanschrift, Telefonnummer, AHV-Nummer, Kopie des Passes oder Identitätskarte, Zivilstand, Geschlecht, Geburtsdatum, Heimatort.
	Zusätzliche Informationen, z. B. Angaben zur Familie, zu persönlichen Beziehungen oder zur finanziellen Situation, zu persönlichen Ereignissen, zur Art der Beistandschaft oder andere für die Betreuung der Leistungsempfänger notwendigen Informationen.
	Administratives Dossier: Versicherungen, interne und externe Kontaktpersonen, behandelnde Ärzte, durchgeführte Aufenthalte.
	Nutzungsdaten der Anwendung: Logdateien, Authentifizierungsdaten, Meldehistorie, IP-Adressen usw.
Kategorien sensibler Daten	Gesundheitsdaten: Patientendossiers mit Anamnese, körperlichem oder psychischem Gesundheitszustand, Testergebnissen, Blutgruppe, körperlichen Merkmalen, Beobachtungen, Behandlungsplänen, persönlichen Entwicklungszielen sowie Medikation.
	Daten im Zusammenhang mit gerichtlichen Entscheiden, administrativen oder einschränkenden Massnahmen, denen betroffene Personen unterliegen können.
	Weitere besonders schützenswerte Daten, wie solche zur Religion, ethnischen Zugehörigkeit oder zum Intimbereich.
Zusätzlich im Rahmen von indip	*Grafische Auswertungen, Frühindikatoren, Dashboards und Fragebögen zur objektiven Verlaufskontrolle der betreuten Personen.*
Art der Behandlung	Verwaltung der Daten des Verantwortliche, die in der Anwendung tipee eingegeben wurden.
	IT-Beratung und -Unterstützung für die vom Verantwortlichen benannten Nutzer.
Zweck der Verarbeitung	Den Nutzern von dsi indipen zentralisierte, sichere und für alle Beteiligten leicht zugängliche Informationen zur Verfügung stellen.
Legitime Aktivitäten des Auftragsverarbeiters	Erstellung vergleichender Statistiken ausschließlich auf der Grundlage anonymisierter Daten.
Orte, an denen die Daten gehostet werden	Rechenzentren in der Schweiz

dsindip

Abkommen über die Datenverarbeitung (ADV)

Anhang 2: Technische und organisatorische Maßnahmen

Governance & Organisation	Tipee betreibt ein Informationssicherheits-Managementsystem (ISMS) gemäss aktuellem Standard. Rollen und Verantwortlichkeiten sind definiert. CTO und DPO berichten direkt an die Geschäftsleitung. Risiken und Sicherheitsrichtlinien werden mindestens jährlich überprüft..
Audits, Zertifizierungen	Penetrationstests für die verschiedenen Anwendungen werden in regelmäßigen Abständen von einem spezialisierten externen Dienstleister durchgeführt.
Entwicklung und Hosting in der Schweiz	Tipee entwickelt seine Anwendungen mit eigenen Entwicklern in der Schweiz. Die Lösungen sowie die darin enthaltenen persönlichen Daten werden in Rechenzentren von ISO 27001-zertifizierten Anbietern gehostet, die alle in der Schweiz ansässig sind (siehe Anhang 3).
Sicherer Entwicklungszyklus	Unsere Entwicklungsteams wenden in jeder Phase des Software-Lebenszyklus integrierte Sicherheitspraktiken an. Wir führen regelmäßig Peer-Reviews des Codes, automatisierte Sicherheitstests und Schwachstellenanalysen durch. Penetrationstests werden regelmäßig von einem externen, auf Cybersicherheit spezialisierten Unternehmen durchgeführt, um die Robustheit unserer Anwendungen objektiv zu bewerten. Unsere Entwickler sind für die gängigen Sicherheitsrisiken (OWASP Top 10) sensibilisiert und verwenden zuverlässige Bibliotheken, deren Abhängigkeiten systematisch überprüft werden. Durch die Trennung von Entwicklungs-, Test- und Produktionsumgebung in Verbindung mit einem schrittweisen Validierungsprozess können wir das Risiko minimieren, dass Sicherheitslücken in unsere Anwendungen eingeschleust werden. Wir wenden einen "Security by Design"-Ansatz an, bei dem Datenschutzüberlegungen bereits in den frühen Entwurfsphasen einbezogen werden.
Sicherheit der Daten	Daten auf der Durchreise werden mithilfe des TLS-Protokolls verschlüsselt. Statische Daten, Benutzerkennungen sowie Datensicherungen werden ebenfalls mithilfe geeigneter Technologien verschlüsselt und ständig auf dem neuesten Stand gehalten.
Datenschutz	Die Daten sind streng unterteilt, um eine vertrauliche Behandlung der Informationen jedes einzelnen Klienten zu gewährleisten. Die Architektur der Anwendung gewährleistet durch dedizierte Datenbanken und spezifische Perimeter die Wasserdichtigkeit der Daten.

Abkommen über die Datenverarbeitung (ADV)

	Die Mitarbeiter von Tipee sind vertraglich an Vertraulichkeits- und Geheimhaltungsklauseln gebunden.
Verfügbarkeit	Alle Elemente unserer Infrastruktur sind dank redundanter Geräte ausfallsicher gegen technische Störungen. Die Dienste werden rund um die Uhr von unserem Supportteam überwacht. Warnmeldungen werden sofort bearbeitet, Tag und Nacht. Regelmäßige Datensicherungen und unsere Wiederherstellungsverfahren im Falle eines Vorfalls ermöglichen eine schnelle Wiederherstellung der Dienste.
Zugangskontrolle	Der Zugriff von Kunden auf tipee wird durch die Kombination von Benutzername und Passwort geschützt. Ein zweiter Authentifizierungsfaktor oder Zugangsschlüssel sind verfügbare Funktionen, mit denen die Nutzer ihre Authentifizierung absichern können. Innerhalb der Anwendung kann der Zugriff auf Informationen durch Benutzerrollen genau definiert werden. Es liegt in der Verantwortung jedes Kunden, seine Richtlinien für die Verwaltung der Zugriffsrechte und die Authentifizierungsmethoden zu definieren und zu implementieren. Was den Zugang von Tipee-Mitarbeitern zu den verschiedenen Systemen betrifft, so wird dieser nach den Grundsätzen des minimalen Privilegs beschränkt und systematisch durch eine Zwei-Faktor-Identifikation geschützt.
Backups	Um das Risiko eines Datenverlustes zu minimieren, werden die Anwendungsdatenbanken jede Stunde vollständig gesichert und das Wiederherstellungsverfahren regelmäßig getestet. Die Backups werden verschlüsselt und an getrennten Standorten aufbewahrt. Sie werden in Übereinstimmung mit unserer Aufbewahrungsrichtlinie und den vertraglichen Verpflichtungen in diesem ADV aufbewahrt.
Aktualisieren von Systemen	Die Systeme werden ständig aktualisiert. Generell ermöglichen die redundante Infrastruktur und die vorhandenen Verfahren die Durchführung von Wartungsarbeiten ohne Betriebsunterbrechung. Die Kunden werden vorab per E-Mail benachrichtigt, falls sich eine Abschaltung der Systeme nicht vermeiden lässt.
Ausbildung des Personals	Die Sicherheitsrichtlinien und -verfahren werden allen Mitarbeitern mitgeteilt. Mehrmals im Jahr werden Schulungen zur Cybersicherheit und Wachsamkeitsmessungen durchgeführt.
Sicherheitsvorfälle und Geschäftskontinuität	Tipee verfügt über einen Notfallplan, der regelmäßig getestet und gemäß den Anforderungen seines Managementsystems für Informationssicherheit verbessert wird.

Abkommen über die Datenverarbeitung (ADV)

Schutz von Anfang an und standardmäßig	Die Grundsätze des Schutzes durch Technik (Protection by Design) und des Schutzes durch Voreinstellungen (Protection by Default) werden bei jeder neuen Entwicklung integriert. Folgenabschätzungen werden durchgeführt, wenn die Umstände oder Gesetze dies erfordern.
Protokollierung / Rückverfolgbarkeit	Unsere technische Infrastruktur umfasst ein umfassendes Protokollierungs- und Rückverfolgungssystem, das wichtige sicherheitsrelevante Ereignisse erfasst. Die Aktivitätsprotokolle werden zentralisiert und für einen Zeitraum aufbewahrt, der den bewährten Praktiken der Branche entspricht und eine effektive Analyse im Falle eines Vorfalls ermöglicht. Wir überwachen mithilfe von Erkennungstools kontinuierlich den Zugriff auf kritische Systeme, Konfigurationsänderungen und anormales Verhalten. Sensible Informationen werden aus den Protokollen ausgeschlossen, um die Vertraulichkeit der Daten zu wahren.

Abkommen über die Datenverarbeitung (ADV)

Anhang 3: Liste der Unter Auftragsverarbeiter dsi indip

Die tipee AG wählt ihre Unter Auftragsverarbeiter sorgfältig nach Dienstleistungsqualität, Zuverlässigkeit und Sicherheitsstandards aus. Ihre gesetzliche Konformität wird regelmäßig überprüft, um die Einhaltung der Verpflichtungen gegenüber den Kunden sicherzustellen. Zur Transparenz und in Erfüllung gesetzlicher Vorgaben veröffentlicht tipee AG die Liste ihrer Unterauftragsverarbeiter mit Angabe des Verarbeitung Zwecks und des Datenstandorts.

Unter Auftragsverarbeiter	**Zweck**	**Lokalisierung von Daten**
Infrastruktur		
Infomaniak	Hosting, backups, managed services	CH
Google Cloud Platform	Hosting, backups, managed services	CH
Dienstleistungen		
Datadog	Monitoring und Verwaltung technischer Logs	EU
Google Analytics	Analyse technischer Zugriffsdaten (OS, Browser, etc.	Global
Verwaltung und Kundensupport		
Zoho	Kundensupport und Marketing	EU
Interne Tools		
Google Workspace	Messaging & office suite	EU
Atlassian (Cloud)	Entwicklung, Fehlermanagement	CH
Slack	Interne Kommunikation	USA

Data Processing Agreement (DPA)

1 Introduction

This data processing agreement ("Data Processing Agreement") is concluded from and for the duration of the main contract, by and between the parties.

Subject to the provisions of the main contract, the Controller and the Processor have entered into this DPA for the processing of personal data.

- A description of processing, purposes and transfers is given in Appendix 1.
- The organizational and technical measures taken by the Processor are described in Appendix 2.
- Appendix 3 provides an overview of subsequent subcontractors used by the Processor.

The duration, term and termination of this DPA follow the duration of the main contract. Terms not defined herein shall have the meaning given to them in the main contract or in applicable data protection laws.

The parties seek to implement a data processing agreement that complies with the requirements of the current legal framework for data protection, i.e. the Swiss Federal Data Protection Act (FADP) as well as, insofar as these are applicable to the Controller, cantonal data protection laws or the General Data Protection Regulation (GDPR).

In consideration of the principal contract, the parties agree as follows.

2 Definitions and interpretation

Unless otherwise defined, the terms and expressions used in this PAD have the following meanings:

"Personal Data" all personal data processed by the Processor on behalf of the Controller under or in connection with the main contract.

"Controller": for the purposes of this DPA, the party who determines the purposes and means of processing personal data in accordance with Swiss data protection laws or EU data protection laws.

"Processor", for the purposes of this DPA, the party that processes personal data on behalf of the Controller in accordance with Swiss data protection laws or EU data protection laws.

"Subsequent Processor": any person appointed by or on behalf of the Processor to process personal data on behalf of the Controller under the main contract.

Terms used but not defined in this DPA, such as "personal data breach", "processing", "transfer", "profiling" and "data subject" will have the same meaning as set out in Article 5 of

the FADP, regardless of whether the FADP applies, and their related terms will be interpreted accordingly.

3 Processing of personal data

The Processor must:

- comply with all applicable data protection laws when processing personal data; and
- not to process personal data other than in accordance with the Controller's documented instructions.

The Controller instructs the Processor to process personal data in the context of the performance of the main contract. The Processor shall immediately inform the Data Controller if it believes that an instruction issued by the Data Controller is in breach of the law. The Processor has the right, without recognizing the obligation to verify the existence of an unlawful instruction, to reject or suspend an instruction that it considers unlawful until it is confirmed or modified by the Data Controller, or to reject manifestly unlawful instructions at any time or to suspend the related processing.

The Processor undertakes to process personal data solely for the purposes of the activities referred to in this DPA or in the main contract. The Processor guarantees that it will not use the personal data it processes under this DPA for its own purposes or for those of third parties without the express written consent of the Controller, unless a mandatory legal provision obliges it to do so. In this case, the Contractor shall immediately inform the Controller of this legal requirement before processing such information, unless the law explicitly prohibits such disclosure.

The Processor may use and process personal data in connection with its legitimate business activities, as indicated in Appendix 1 and within the limits set forth in said Appendix.

4 Confidentiality, disclosure of personal data

The Processor, Processor and Subsequent Processor shall maintain the confidentiality of all information they receive in accordance with the relevant confidentiality provisions set forth in the main contract and this DPA.

The Processor does not disclose personal data, except

- on instructions from the Data Controller ;
- as described in this PAD; or
- as required by mandatory legal provisions.

The Processor will not disclose personal data to any government agency, except as required by law. If compelled to disclose personal data to a government agency, the Processor will, where possible, refer the requesting government agency to the Controller. The Processor will promptly notify the Controller of any such request to enable the Controller to seek an

appropriate solution, unless prohibited by law. The Processor will examine all requests and will contest any request that it considers excessive or inappropriate (for example, if such a request is contrary to Swiss law. If, after exhausting the measures described in this section, the Processor is still obliged to disclose personal data, it will disclose only the minimum amount of personal data necessary to meet the request.

The Processor will not provide any third party with :

- direct, indirect, widespread or unhindered access to personal data;
- the encryption keys used to secure personal data or the ability to break such encryption; or
- access to personal data if the Controller is aware that the data is to be used for purposes other than those indicated in the third party's request.

In support of the above, the Processor may provide the third party with the basic contact details of the Controller.

The Controller shall be solely responsible for the decision and procedure for disclosure of the relevant information to public authorities/governmental bodies and shall be assisted by the Processor to the best of its ability in connection with such disclosure.

5 Processor's personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent, contractor or subprocessor who may have access to personal data, ensuring in each case that access is strictly limited to those persons who have a need to know or access the relevant personal data, to the extent strictly necessary for the purposes of the main contract, and to comply with the laws applicable to that person's duties to the Processor, ensuring that all such persons are subject to confidentiality undertakings or professional or legal obligations of confidentiality.

6 Security

Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, as well as the risk of varying probability and severity to the rights and freedoms of natural persons, the Processor implements, with respect to personal data, the technical and organizational measures listed in Appendix 2 to ensure a level of security appropriate to this risk, including, where applicable, the measures referred to in applicable data protection laws.

When assessing the appropriate level of security, the Processor takes into account the risks presented by the processing, in particular in the event of a breach of personal data.

7 Data transfer

The Data Processor may not transfer or authorize the transfer of data to countries outside Switzerland or the European Economic Area without the prior written consent of the Controller. If personal data processed under this DPA is transferred from Switzerland or a

European Economic Area country to a country outside the European Economic Area, the Parties will ensure that the personal data is adequately protected. For this purpose, the Parties shall rely, unless otherwise agreed, on an adequacy decision issued by the Swiss authorities or on the standard contractual clauses approved by the EU or Switzerland for the transfer of personal data.

8 Sub Processing

The Processor does not appoint (or disclose personal data to) a Subsquent Processor unless required or authorized in advance by the Controller.

The Processor requires each Subsequent Processor to comply with confidentiality obligations, notification obligations, transfer obligations and security measures relating to the processing of personal data, which obligations and measures shall at least comply with the provisions of this DPA. The Processor acknowledges that it is jointly and severally responsible for compliance with the obligations imposed on the Subsequent Processor under this DPA.

Appendix 3 lists the Subsequent Processors used by the Processor. The modification of the Processors designated in the said appendix or the use of additional Processors is authorized if :

- the Processor notifies the Controller in advance of such outsourcing to Subsequent Processors in writing or in an appropriate electronic form within a reasonable period of time, which may not be less than 14 days; and
- the Controller does not object to the planned outsourcing in writing or in an appropriate electronic form to the Processor at the time of disclosure or transmission of the data; and
- subcontracting is based on a contract that complies with Article 9 of the Swiss Data Protection Ordinance or Article 28 of the GDPR, thus respecting the level of data protection and data processing security required for the processing.

9 Rights of the person concerned

Given the nature of the processing, the Processor assists the Controller by implementing appropriate technical and organizational measures, as far as possible, so that the Controller can fulfil its obligations, as it reasonably understands them, to respond to requests to exercise data subjects' rights under data protection laws.

The Processor:

- promptly notifies the Controller if it receives a request from a data subject under any data protection law with respect to personal data; and
- ensures that it does not respond to this request, except on documented instructions from the Controller.

10 Violation of personal data

In the event of a breach of personal data security, the Processor shall cooperate with and assist the Controller in complying with its obligations.

In the event of a security breach in relation to data **processed by the Controller**, the Processor shall assist the Controller for the purposes of:

- notify the competent supervisory authority as soon as possible after the Controller becomes aware of the breach.
- obtain the information to be included in the notification.

In the event of a breach of security in relation **to data processed by the Processor**, the Processor shall notify the Controller as soon as possible after becoming aware of the breach. The notification to the Controller shall contain at least the following information:

- a description of the personal data breach incident;
- information on the data and data categories concerned and an estimate of the number of people concerned;
- a preliminary assessment of the likely consequences of the violation.
- a description of the measures and/or proposals for measures already taken/to be taken by the Processor to avoid or mitigate the negative consequences for the persons concerned.

Notifications of security incidents shall be sent to the Data Protection Officer of the Data Controller or to any other employee acting as a point of contact, by any appropriate means of communication chosen by the Processor, including e-mail.

Processor's notification or response to a Security Incident under this section shall not constitute an admission by Processor of fault or liability with respect to the security Incident.

11 Data protection impact assessment

The Processor assists the Controller with data protection impact assessments and consultations with the relevant privacy authorities, where the Controller deems this necessary. This assistance relates solely to the processing of personal data carried out by the Processor, and takes into account the nature of the processing and the information available to the Processor.

In the event of frequent requests or requests which have a significant impact on the Processor's resources, the Processor may request reasonable compensation for the work performed.

12 Restitution and deletion of data

The Processor does not retain personal data beyond the period agreed with the Controller in the main contract.

In the event of termination of the main contract, the Controller may either export his data using the procedure available online, or call on the support service to obtain a copy of the entire data set in a format enabling it to be re-used.

The Processor guarantees that all data, including backups, will be definitively destroyed within a maximum period of 3 (three) months following the end of the contractual relationship. This retention period is necessary for technical reasons.

In view of the automation of the data deletion procedure, the present clause serves as a confirmation of deletion.

13 Audit rights and inspections

Subject to this section or any other provision of the main contract, the Processor authorizes the Controller to carry out checks on compliance with technical and organizational measures.

The Controller may engage an independent third party to carry out the audit on its behalf, provided that the third party is accepted by the Controller and the Processor. Audits must be carried out during normal business hours, subject to the Processor's policies, and must not unreasonably interfere with the Processor's commercial and technical activities. They must be notified at least 14 days in advance.

The Processor will provide reasonable resources and documentation to support audits in accordance with the FADP, in particular to prove the implementation of technical and organizational measures. Proof of technical and organizational measures to comply with specific data protection requirements in general as well as those relating to the order may be provided by:

- certificates, reports or extracts from current reports by independent bodies;
- appropriate certification by an IT security or data protection audit.

The Parties agree that on-site inspections are only necessary if compliance with the Processor's obligations under Articles 8 and 9 FADP cannot already be proven by the aforementioned evidence. In addition, on-site inspections carried out by the Controller must be justified by a specific reason and are permitted for no more than one audit day per year and only in exceptional cases.

Nothing in this section shall require Processor to breach its confidentiality obligations to its customers or employees.

In the event of a necessary (on-site) inspection by the Controller at the Processor's premises, each party shall bear its costs incurred for the inspection, such as inspection, personnel and

travel expenses. If the Processor's cooperation in inspections exceeds the extent required in accordance with this section and if this is associated with higher inspection costs or the use of external service providers by the Processor, the costs incurred in this respect may be charged to the Controller at the hourly and daily rates customary in the industry.

14 General terms and conditions

Notwithstanding the foregoing, in addition to the applicable provisions set forth in the main contract, all notices and communications given under this DPA shall be in writing and sent by electronic mail.

With regard to the termination of this DPA, the specific provisions of the main contract apply.

15 Applicable law and jurisdiction

The choice of law and jurisdiction is in accordance with the provisions applicable to the main contract.

dsindip

Data Processing Agreement (DPA)

Appendix 1 : Processing description - application dsi indip

Categories of data subjects	Recipients of services provided by institutions active in the fields of social care, healthcare, and education, such as nursing homes, reintegration programs, support for persons with disabilities, and special education (non-exhaustive list).
Categories of personal data	Personal data of beneficiaries: first and last name, email and postal address, telephone number, social security number (AVS), copy of passport or identity card, marital status, gender, date of birth, place of origin.
	Additional information such as data relating to family, personal relationships or financial situation, personal life events, type of guardianship, or other information necessary for the care and support of beneficiaries.
	Administrative records: insurance details, internal and external contacts, attending physicians, records of stays.
	Application usage data: log files, authentication data, connection history, IP addresses, etc.
Categories of sensitive data	Health data: patient records including medical history, physical or mental health status, test results, blood type, physical characteristics, clinical notes, treatment plans, personal development projects, and medication.
	Data related to legal decisions, administrative or restrictive measures affecting the data subjects.
	Other sensitive data relating to religion, ethnicity, or intimate life
Additionally, in the context of indip	*Graphical analyses, advanced indicators, dashboards, and questionnaires enabling the objective monitoring of beneficiaries' progress.*
Type of treatment	Processing of data entered by the data controller in the dsi indip application.
	IT consulting and support for users designated by the data controller.
Purpose of processing	Provide dsi indip users with centralized, secure and easily accessible information for all stakeholders.
Processor's legitimate activities	Preparation of comparative statistics based exclusively on anonymized data.
Data hosting locations	Data centers in Switzerland

dsindip

Data Processing Agreement (DPA)

Appendix 2: Technical and organizational measures

Governance & organization	Tipee has implemented and maintains an Information Security Management System (ISMS) that complies with current standards. Security roles and responsibilities are defined and assigned. The CTO and DPO report directly to General Management. Cyber risks and security policies are reviewed periodically, at least once a year, and the necessary resources adapted accordingly.
Audits, certifications	Penetration tests on the various applications are carried out at regular intervals by a specialized external service provider.
Development and hosting in Switzerland	Tipee develops its applications with its own developers in Switzerland. The solutions and the personal data they contain are hosted in data centers operated by ISO 27001-certified service providers, all based in Switzerland (see Appendix 3).
Secure development cycle	Our development teams apply integrated security practices at every stage of the software lifecycle. We regularly carry out peer code reviews, automated security tests and vulnerability scans. Penetration tests are regularly carried out by an external firm specialized in cybersecurity to objectively assess the robustness of our applications. Our developers are aware of current security risks (OWASP Top 10) and use reliable libraries whose dependencies are systematically checked. The separation of development, test and production environments, combined with a progressive validation process, enables us to minimize the risk of introducing security flaws into our applications. We apply a "security by design" approach where data protection considerations are integrated from the earliest design phases.
Data security	Data in transit is encrypted using the TLS protocol. Static data, user IDs and backups are also encrypted using appropriate technologies that are constantly kept up to date.
Privacy	Data is strictly compartmentalized to ensure confidential treatment of each customer's information. The application's architecture guarantees data watertightness, thanks to dedicated databases and specific perimeters. Tipee employees are contractually bound by confidentiality and trade secret protections clauses.
Availability	All elements of our infrastructure are resilient to technical breakdowns thanks to redundant equipment. Services are monitored 24/7/365 by our support team. Alerts are dealt with immediately, day or night. Regular backups and our disaster recovery procedures ensure rapid restoration of services.

Data Processing Agreement (DPA)

Access control	Customer access to tipee is protected by a combination of user name and password. A second authentication factor or access keys are available to enable users to secure their authentication. Within the application, user roles are used to precisely define access to information. It is the responsibility of each customer to define and implement their own access rights management policy and authentication methods. Tipee employees' access to the various systems is limited according to the principles of minimum privilege and systematically protected by two-factor identification.
Backups	To minimize the risk of data loss, application databases are fully backed up every hour, and the restoration procedure is regularly tested. Backups are encrypted and stored on separate sites. They are stored in accordance with our retention policy and the contractual commitments of this DPA.
System updates	Systems are constantly updated. Generally speaking, the redundancy of the infrastructure and the procedures in place mean that maintenance operations can be carried out without interrupting service. Advance notification is sent by e-mail to customers in the event of unavoidable downtime.
Staff training	Security policies and procedures are communicated to all staff. Cybersecurity training and vigilance measurements are carried out several times a year.
Security incidents and business continuity	Tipee has a disaster recovery plan that is regularly tested and improved in line with the requirements of its information security management system.
Protection by design and default	The principles of protection by design and by default are integrated into all new developments. Impact analyses are carried out if circumstances or legislation so require.
Logging / traceability	Our technical infrastructure incorporates a comprehensive logging and traceability system that captures significant security-related events. Activity logs are centralized and kept for a period in line with industry best practice, enabling effective analysis in the event of an incident. We continuously monitor access to critical systems, configuration changes and abnormal behavior using detection tools. Sensitive information is excluded from logs to respect data confidentiality.

dsindip

Data Processing Agreement (DPA)

Appendix 3: List of Subprocessors application dsi indip

To provide its services, tipee SA carefully selects its subprocessors, who are chosen for the quality and reliability of their services as well as their good safety practices. Their compliance with legal requirements is regularly assessed to ensure that tipee SA's commitments to its customers are met from start to finish.

For the sake of transparency and in response to certain legal obligations, tipee SA publishes the list of its subcontractors, indicating the purpose of the outsourced processing and the location where the data is hosted.

Subprocessor	**Purpose**	**Data localization**
Infrastructure		
Infomaniak	Hosting, backups, managed services	CH
Google Cloud Platform	Hosting, backups, managed services	CH
Services		
Datadog	Monitoring and management of technical logs	EU
Google Analytics	Analysis of technical resources used on applications (OS, browser, resolution, etc.)	Global
Admin and customer support		
Zoho	Customer support and marketing	EU
Internal tools		
Google Workspace	Messaging & office suite	EU
Atlassian (Cloud)	Development, bug management	CH
Slack	Internal communication	USA