TRADUCTION FRANÇAISE A TITRE D'INFORMATION
SEULE LA VERSION ORIGINALE ALLEMANDE EST JURIDIQUEMENT VALABLE !

# Accord sur le traitement des données personnelles (ATD)

# ClubDesk pour les associations de l'Espace économique européen (EEE) ainsi que pour les associations basées en Suisse

Accord conclu entre

**l'association mandataire**

— responsable du traitement, ci-après « client » —

et

**reeweb ag (développeur de ClubDesk)**

Picassoplatz 8

4052 Bâle

Suisse

— sous-traite, ci-après « reeweb » –

# 1. Objet et durée du contrat, application de la loi sur la protection des données

## 1.1. Objet du contrat

L'objet du contrat est la fourniture du logiciel ClubDesk pour la gestion des données de l'association en tant que service Internet (Software-as-a-Service) conformément au contrat conclu en ligne entre le client et reeweb d'après les Conditions générales (CG).

La gestion du contenu des données d'association et la responsabilité de l'admissibilité du traitement des données, c'est-à-dire savoir si certaines données (par ex. les coordonnées des membres) peuvent être traitées, relèvent de la responsabilité du client ou du représentant autorisé. Dans le cadre des accords conclus, reeweb ne traite que les données saisies par le client pour son compte et conformément à ses instructions.

Le présent accord régit les droits et obligations du client et de reeweb dans le cadre d'un traitement des données personnelles sur mandat. Les dispositions s'appliquent à toutes les activités liées au contrat impliquant que reeweb et ses employés ou les agents mandatés par reeweb entrent en contact avec des données personnelles provenant du client ou collectées pour ce dernier.

## 1.2. Durée du contrat

La durée du présent contrat (durée) est déterminée par la durée du contrat principal. En cas de doute, la résiliation du contrat principal constitue également une résiliation du présent accord, et la résiliation du présent accord constitue également la résiliation de l'accord principal.

En cas de violation simple, c'est-à-dire ni intentionnelle ni liée à une négligence grave, le client doit d'abord fixer à reeweb un délai raisonnable pour y mettre fin. Le droit à la résiliation extraordinaire du présent accord pour motif grave n'est pas affecté.

## 1.3. Application du RGPD

Le règlement général sur la protection des données (ci-après "RGPD") s'applique au client en tant qu'association établie dans l'Espace économique européen (EEE) ou aux associations dont les membres sont établis dans l'EEE. Dans le cas contraire, la législation sur la protection des données applicable au client s'applique. reeweb, dont le siège est en Suisse, respecte les dispositions relatives à la protection des données qui lui sont respectivement applicables.

## 1.4. Lieu du traitement des données

Le traitement des données par reeweb a lieu en Suisse. La Commission européenne, par sa décision du 26 juillet 2000, qu'il existe en Suisse un niveau de protection des données adéquat.

reeweb est autorisé à déplacer le traitement et la conservation des données vers un État membre de l'Union européenne ou vers un autre État partie à l'accord sur l'Espace économique européen, ainsi que vers un pays disposant d'une décision d'adéquation.

L'éventuelle transmission ultérieure à des sous-traitants dans des États ne disposant pas d'un niveau de protection des données adéquat est garantie par la conclusion de clauses contractuelles types de

l'UE (module 3). Si, à l'avenir, reeweb devait transmettre des données en se basant sur d'autres mécanismes de transfert autorisés par la loi, elle en informera préalablement la cliente.

# 2. Concrétisation du contenu du contrat

## 2.1. Portée, nature et finalité du traitement des données envisagé

Le traitement des données vise à gérer des associations ou des groupes, comme convenu dans le contrat. Cela peut inclure par exemple la gestion des membres, des personnes intéressées, des participants à un événement, des fournisseurs et des rendez-vous. La portée, la nature et la finalité du traitement des données personnelles par reeweb pour le client sont décrites en termes plus spécifiques dans la politique de confidentialité.

## 2.2. Nature et catégories de données personnelles

L'objet de la collecte, du traitement ou de l'utilisation correspond à différents types/catégories de données, en fonction de la façon dont les fonctionnalités flexibles ClubDesk sont configurées et utilisées par l'association/le groupe, conformément au contrat principal. Les catégories de données suivantes doivent notamment être prises en considération :

- Données de base des personnes concernées, en particulier des membres de l'association, notamment
  - Adresse et numéro de téléphone
  - Adresse e-mail
  - Coordonnées bancaires
- Informations de règlement (telles que l'état du compte de cotisation, l'état des comptes client/fournisseur et les comptes salaire)
- Données de qualification (telles que la participation à des événements ainsi qu'à des concours et les résultats obtenus ou la formation des employés)

## 2.3. Cercle et catégories des personnes concernées

Le cercle ou les catégories de personnes concernées par ce traitement de données comprend différentes personnes, en fonction de la façon dont les fonctionnalités flexibles ClubDesk sont configurées et utilisées par l'association/le groupe, conformément au contrat principal. Les catégories de personnes suivantes doivent notamment être prises en considération :

- Membres de l'association/du groupe
- Personnes intéressées et invités
- Sponsors et mécènes
- Participants aux événements
- Collaborateurs
- Fournisseurs/prestataires de services

# 3. Description des mesures techniques et organisationnelles à prendre en matière de protection des données et de sécurité

(1) Les mesures techniques et organisationnelles nécessaires à la protection appropriée des données du client sont décrites par reeweb conformément à l'annexe. En cas d'acceptation par le client, les

mesures documentées constituent la base du contrat. Dans la mesure où un examen du client indique un besoin d'adaptation, celui-ci doit être mis en œuvre d'un commun accord.

(2) reeweb est tenu d'assurer la sécurité du traitement des données conformément à l'annexe du présent accord. Dans l'ensemble, les mesures à prendre sont des mesures de sécurité des données visant à assurer un niveau de protection adapté au risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes, en tenant compte notamment du contrôle organisationnel, des entrées, d'accès, des transferts, des contrats et de la disponibilité ainsi que de l'obligation de séparation. Il faut tenir compte de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée et des finalités du traitement, ainsi que des différentes probabilité d'occurrence et gravité du risque pour les droits et libertés des personnes physiques.

(3) Les mesures techniques et organisationnelles sont soumises au progrès et au développement techniques. À cet égard, reeweb est autorisé à mettre en œuvre des mesures alternatives adéquates. Toutefois, le niveau de sécurité minimum des mesures déterminées doit être respecté. Les modifications importantes doivent être communiquées immédiatement par écrit au client.

## 4. Rectification, blocage et suppression des données ; Droits des personnes concernées et responsabilité

(1) reeweb ne peut pas, de sa propre initiative, rectifier, supprimer ou bloquer les données traitées pour le compte du client, voire limiter leur traitement, mais uniquement après avoir reçu une directive documentée de la part de ce dernier. Le blocage de l'accès du client à ClubDesk par reeweb est autorisé dans la mesure où cela est autorisé par les CG de ClubDesk, par exemple en cas d'arriérés de paiement des frais ou de suspicion raisonnable d'utilisation abusive.

(2) Dans la mesure où une personne concernée (par ex. un membre de l'association) s'adresse directement à reeweb concernant ses droits à la protection des données, notamment en ce qui concerne l'information, la rectification, la suppression et le blocage conformément à la législation applicable en matière de protection des données , reeweb transmettra cette demande au client et/ou renverra la personne concernée au client tout en informant ce dernier de la demande de la personne concernée. reeweb ne prendra aucune décision sur la légitimité des demandes des personnes concernées ni ne répondra à leurs demandes d'informations.

(3) Si le client est incapable de satisfaire les exigences des personnes concernées sans son concours, reeweb l'aidera le client dans la mesure de ses capacités. Reeweb peut exiger du client une rémunération supplémentaire appropriée pour couvrir les coûts liés à la coopération.

(4) Si une personne concernée contacte directement reeweb pour une violation présumée de la protection des données et obtient des dommages-intérêts de sa part, le client remboursera reeweb pour les dommages en résultant dans la mesure où reeweb n'était pas responsable envers le client de cette violation de la protection des données en vertu des dispositions du présent accord et du contrat principal, notamment si elle a respecté l'accord et les instructions du client. Cela s'applique également en cas d'amende imposée à reeweb.

## 5. Contrôles et autres obligations de reeweb

En plus des dispositions de la présente ordonnance, reeweb est tenue de se conformer aux dispositions légales en matière de protection des données en vigueur en Suisse, où elle a son siège social. Cette interaction entre les réglementations contractuelles et légales donne naissance aux obligations particulières suivantes de reeweb :

1. reeweb n'est pas tenue de nommer un délégué à la protection des données. Les questions concernant la protection des données peuvent être adressées à datenschutz@clubdesk.com.
2. Pour l'exécution des travaux, reeweb emploie uniquement des collaborateurs s'étant engagés par écrit à préserver la confidentialité et ayant déjà été familiarisés avec les dispositions pertinentes en matière de protection des données ou étant soumis à une obligation légale de confidentialité. En outre, reeweb prendra les précautions voulues pour assurer le respect de cette obligation. reeweb et tout subordonné de reeweb ayant accès aux données personnelles ne peuvent traiter ces données que conformément aux instructions du client, comprenant les autorisations conférées par le présent accord, à moins d'être soumis à une obligation légale de traitement. Dans un tel cas, reeweb communique ces exigences légales au client avant le traitement, à moins que le droit concerné n'interdise une telle communication pour un motif d'intérêt public important.
3. reeweb contrôle régulièrement les mesures techniques et organisationnelles en matière de sécurité des données afin de s'assurer que le traitement est effectué dans le champ de ses responsabilités conformément aux exigences de protection des données en vigueur pendant la durée du traitement des données du client.
4. reeweb tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du client.

## 6. Contrats de sous-traitance

(1) Au sens du présent règlement, les contrats de sous-traitance sont définis comme des services qui se rapportent directement à la prestation du service principal. Cela ne comprend pas les services auxiliaires utilisés par reeweb, tels que les services de télécommunications, les services de poste et de transport, la maintenance et le service à l'utilisateur ou l'élimination des supports de données, ni d'autres mesures visant à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des installations de traitement des données. reeweb est toutefois tenue de recourir à des accords contractuels et à des mesures de contrôle légaux et appropriés pour assurer la protection des données et la sécurité des données du client, même dans le cas de services auxiliaires externalisés.

(2) Par la présente, le client accepte, de façon général, le recours à des sous-traitants avec lesquels reeweb a conclu un accord conformément au présent accord. Vous trouverez la liste des fournisseurs de services actuels sur le site web de reeweb à l'adresse www.clubdesk.com/unterauftragnehmer.

(3) La sous-traitance ou le changement de sous-traitant existant est autorisé à condition que :

- un accord contractuel avec le sous-traitant est pris comme basse comparable au présent accord,
- reeweb informe à l'avance (en règle générale, deux (2) mois) par écrit le client du recours à la sous-traitance, en indiquant la date de transfert des données et
- le client ne fait pas parvenir à reeweb, par écrit ou sous forme de texte, une objection motivée à l'externalisation prévue avant la date de transmission des données.

Une opposition du client est considérée comme une résiliation extraordinaire du contrat principal juste avant le transfert. Après cette date, le client ne peut plus utiliser les services de reeweb. Avant le transfert au sous-traitant, reeweb supprime les données du client. Il est de la responsabilité du client de sauvegarder les données dans son propre système avant cette date.

(4) Le transfert des données personnelles du client au sous-traitant et la première intervention de ce dernier ne sont autorisés que si toutes les conditions de sous-traitance sont réunies. Si un sous-traitant ne respecte pas ses obligations en matière de protection des données, reeweb est responsable vis-à-vis du client du respect des obligations de ce sous-traitant.

(5) Si le sous-traitant fournit le service convenu en dehors de l'UE/EEE/Suisse, reeweb prend les mesures appropriées pour garantir les conditions spécifiques de délocalisation vers un pays tiers. Il en va de même si des prestataires de services doivent être utilisés pour des prestations accessoires au sens de l'art. 1, par. 2 ci-dessus de l'UE/EEE/Suisse.

## 7. Droits de contrôle du client

(1) reeweb s'assure que le client est en mesure de vérifier le respect des obligations de reeweb en vertu du présent contrat. reeweb s'engage à fournir au client les informations nécessaires sur demande et, en particulier, à prouver la mise en œuvre des mesures techniques et organisationnelles.

(2) reeweb a le droit, à sa propre discrétion et en tenant compte des obligations légales du client, de ne pas divulguer des informations sensibles pour l'activité de reeweb ou dont la divulgation violerait les dispositions légales ou d'autres dispositions contractuelles. Le client n'a pas le droit d'accéder aux données ou informations concernant d'autres clients de reeweb, à des informations relatives aux coûts ni à toutes les autres données confidentielles de reeweb qui ne sont pas directement pertinentes aux fins de contrôle convenues.

(3) Le client a le droit, en accord avec reeweb, d'effectuer des inspections (contrôle des commandes) durant les heures normales d'ouverture, à ses frais, sans perturber les opérations et dans le strict respect de la confidentialité des secrets commerciaux et industriels de reeweb, ou de les faire effectuer par un auditeur nommé ponctuellement, dans la mesure où ce dernier n'est pas dans une relation de concurrence avec reeweb. Le client doit informer reeweb en temps utile (généralement au moins quatre semaines à l'avance) de toutes les circonstances liées au déroulement du contrôle.

(4) eeweb peut choisir que la preuve du respect des mesures techniques et organisationnelles ne soit pas apportée par un contrôle sur place, mais plutôt par un test approprié et à jour, des rapports ou des extraits de rapports d'organismes indépendants (par ex. commissaires aux comptes, auditeurs, délégués à la protection des données, département de sécurité informatique, auditeurs

en matière de protection des données ou auditeurs qualité) ou par une certification appropriée au moyen d'audits de sécurité informatique ou de protection des données — par exemple conformément à la norme ISO 27001 ou conformément à l'art. 42 RGPD — (« Certification »), si la certification permet au client de vérifier de façon adéquate le respect des mesures techniques et organisationnelles. Le respect des codes de conduite approuvés est aussi considéré comme une preuve.

(5) Si le client engage un tiers pour effectuer le contrôle, il doit l'obliger à la confidentialité. reeweb a également le droit de demander au tiers une obligation de confidentialité avant le contrôle, qui interdit que le client soit informé des circonstances non pertinentes à la protection des données en vertu du contrat et que des tiers aient connaissance de circonstances mises à jour dans le cadre du mandat et du contrôle. Le client ne peut pas confier l'exécution du contrôle à un concurrent de reeweb.

(6) reeweb peut exiger une rémunération supplémentaire appropriée pour l'aide consentie dans le cadre des contrôles du client.

## 8. Notification en cas de violation par reeweb et soutien apporté au client

(1) Dans tous les cas, reeweb informera immédiatement le client si l'entreprise, les personnes qu'elle emploie ou les sous-traitants attribués au client n'ont pas respecté les dispositions relatives à la protection des données personnelles du client ou d'autres dispositions contractuelles et que reeweb en a eu connaissance. Le contenu des notifications est basé sur la législation applicable en matière de protection des données.

(2) Le client est tenu d'informer reeweb immédiatement et en détail s'il constate, lors du contrôle des résultats, des erreurs ou des irrégularités par rapport à la réglementation en matière de protection des données ou à ses instructions.

(3) Dans le cadre de ses capacités et du présent contrat, reeweb apporte son soutien au client pour ce qui concerne le respect des obligations légales relatives à la sécurité des données personnelles, les obligations de déclaration en cas de violation des données, l'analyse d'impact relative à la protection des données et la consultation préalable auprès de l'autorité de contrôle. Il s'agit notamment d'assurer un niveau de protection approprié grâce à des mesures techniques et organisationnelles tenant compte des circonstances et des objectifs du traitement ainsi que de la probabilité et de la gravité anticipées d'une éventuelle infraction liée à des atteintes à la sécurité, et fournissant une identification immédiate des violations pertinentes.

(4) Pour les services de soutien pour des actions non incluses dans la description du service du contrat principal ou dont la faute ne peut être imputée à reeweb, cette dernière peut réclamer une rémunération supplémentaire appropriée pour les charges justifiées.

## 9. Autorisation du client à donner des instructions

(1) Le traitement des données s'effectue exclusivement dans le cadre des accords conclus et conformément aux instructions du client, à moins que les dispositions légales ne contredisent lesdites instructions. reeweb communiquera ces exigences légales au client, à moins que la notification ne soit empêchée par un intérêt public important. Le client donnera automatiquement ses instructions générales via les fonctions du logiciel ClubDesk fournies en vertu du contrat principal ainsi que par ses entrées client et ses configurations.

(2) reeweb n'est pas tenue d'exécuter les instructions individuelles différentes. Cela ne s'applique pas aux instructions individuelles de suppression de toutes les données traitées pour le compte du client, que reeweb est tenue d'exécuter dans la mesure où il est établi qu'elles proviennent du client ou d'une personne habilitée à le représenter. Le client doit confirmer immédiatement par écrit les instructions verbales individuelles. Pour une suppression, l'instruction doit toujours être donnée par écrit. reeweb doit informer immédiatement le client si elle estime qu'une instruction individuelle conforme au présent paragraphe enfreint la réglementation relative à la protection des données. reeweb est en droit de suspendre la mise en œuvre de l'instruction en question jusqu'à ce qu'elle soit confirmée ou modifiée par le client. Si reeweb exécute une instruction individuelle conformément au présent paragraphe, elle a le droit d'exiger une rémunération supplémentaire appropriée pour les charges justifiées.

(3) Sont considérées personnes autorisées celles pouvant représenter efficacement le client.

## 10. Suppression des données personnelles

(1) Les données ne sont ni copiées ni dupliquées à l'insu du client. Cela ne s'applique pas aux copies de sauvegarde, dans la mesure où elles sont nécessaires pour assurer un traitement adéquat des données. En outre, reeweb peut utiliser des copies des données du client pour tester des logiciels (par ex. migration des données lors de nouvelles versions) et pour l'assistance (par ex. débogage sur les systèmes de test).

(2) Sur demande du clien,t et au plus tôt après l'achèvement des travaux convenus par le contrat (c'est-à-dire à la fin du contrat conformément aux CG applicables), reeweb est tenue de supprimer toutes les données personnelles du domaine de responsabilité du client en sa possession et faisant partie de la relation contractuelle. Cela s'applique également à la reproduction des données client chez reeweb, telles que les sauvegardes de données. Il est de la responsabilité du client de sécuriser lui-même ses données dans son propre système avant la fin du contrat ou avant de transmettre une instruction de suppression. reeweb confirmera la suppression au client par écrit.

(3) Les documents utilisés pour prouver que le traitement des données est conforme au contrat et correct doivent être conservés après la fin du contrat par reeweb, conformément aux délais de conservation respectifs. reeweb peut s'en décharger en les remettant au client à la fin du contrat.

## 11. Divers

Dans la mesure où aucune disposition particulière ne figure dans le présent contrat, les dispositions du contrat s'appliquent conformément aux CG applicables, notamment les limitations de responsabilité prévues au point 14 des CGV.

Bâle, 15.09.2023

# 12. Annexe — Mesures techniques et organisationnelles

## 1. Confidentialité )

- Contrôle d'accès (pas d'accès non autorisé à l'installation de traitement des données) :

  *reeweb ag* : Pas de stockage de données chez reeweb ag, les logiciels et les données sont entièrement hébergés dans un centre de données externe (production et systèmes de test) ;

  *Centre de données :* Aucun accès non autorisé aux installations de traitement des données ; la vidéosurveillance et le principe de contrôle d'accès à plusieurs niveaux garantissent la sécurité physique ;

- Contrôle d'accès (pas d'utilisation non autorisée du système) :

  Mots de passe forts (longueur minimale de 8 caractères requis pour les mots de passe administrateur pour ClubDesk, nombre et caractères spéciaux, etc.), mécanismes de verrouillage automatique (les comptes utilisateur sont automatiquement bloqués au bout de 10 échecs de connexion), seule la valeur de hachage des mots de passe est stockée ;

- Contrôle d'entrée (pas de lecture, de copie, de modification ni de suppression non autorisées dans le système) :

  ClubDesk offre un système de rôles complet pour les droits d'accès ponctuels de différents utilisateurs d'une association, l'enregistrement des connexions et l'accès en écriture (les modifications apportées aux données sont classées par date, et comprennent l'horodatage et l'utilisateur) ;

- Contrôle de la séparation (traitement séparé des données collectées à des fins différentes) :

  les données sont stockées par association dans une base de données à part avec un identifiant séparé pour la base de données.

## 2. Intégrité

- Contrôle des transferts (pas de lecture, de copie, de modification ni de suppression non autorisées en cas de transmission électronique ou de transport) :

  Connexion web sécurisée aux serveurs d'applications via HTTPS — également pour les sites web des associations créés dans le logiciel ClubDesk.

  Envoi et réception sécurisés d'e-mails au moyen de TLS (si le serveur d'envoi ou de réception le supporte). En outre, ClubDesk utilise différentes technologies pour assurer l'intégrité et l'authenticité des e-mails et de leurs expéditeurs : Domain-based Message Authentication (DMARC), Domain Keys Identified Mail (DKIM) et Sender Policy Framework (SPF). Le client est lui-même responsable de l'envoi non crypté d'e-mails (si un serveur d'e-mail récepteur ou émetteur ne supporte pas TLS) par le client au moyen de la fonctionnalité correspondante de ClubDesk.

- Contrôle de la saisie (détermine si des données personnelles sont saisies ou modifiées dans les systèmes de traitement des données, ou supprimées de ces derniers, et par qui) :

  Journalisation des connexions et des accès en écriture : Les modifications apportées aux données sont stockées par date, et comprennent l'horodatage et l'utilisateur ;

## 3. Disponibilité et résilience

- Contrôle de la disponibilité (protection contre la destruction accidentelle ou intentionnelle et contre la perte) :

  *reeweb* ag : y compris duplication des disques durs (RAID), sauvegardes quotidiennes dans le centre de données, pare-feu, protection antivirus des fichiers téléversés, surveillance externe des composants logiciels et matériels importants avec alerte SMS au niveau 3 d'assistance ;

  *Centre de données :* Détecteurs d'incendie ; lignes d'alimentation et de données redondantes et entièrement séparées ; internet ultra-fiable, composants réseau redondants ; alimentation sans interruption (ASI) ; protection des données à la pointe de la technologie : sécurité multiple, réparties dans différentes zones protégées contre les incendies ;

- Rétablissement rapide

  Les sauvegardes et la configuration standardisée du serveur permettent de rétablir rapidement le service en cas d'urgence.

## 4. Procédures visant à tester, à analyser et à évaluer régulièrement

- Gestion de la protection des données :
  dispositions relatives à la protection des données dans tous les contrats de travail et lignes directrices sur le wiki interne ; la direction est sensibilisée au sujet de la protection des données ;

- Gestion de réponse aux incidents :
  outil externe d'assistance en cas d'incident qui gère et surveille toutes les demandes d'assistance ;

- Protection des données par défaut :
  par ex. des rôles par défaut pour les fonctions typiques au sein d'une association ;

- Contrôle des mandats (aucun traitement des données pour le compte du client sans des instructions correspondantes de sa part) :
  élaboration claire du contrat, sélection rigoureuse et contrôle du centre de données.