# Accordrelatif au traitement des mandats en vertu de l‘art. 28 RGPD

entre

................................................................................................

- Responsable – ci-après dénommé le « mandant » –

et

Tandberg Data GmbH

................................................................................................

- Responsable du traitement – ci-après dénommé le « mandataire » –

[Représentant selon l'art. 27 RGPD *si nécessaire* :

................................................................................................]

## 1. Objet et durée du contrat

(1) Objet

L’objet du contrat relatif à la gestion des données est l’exécution des tâches suivantes par le mandataire : Accès à distance avec TeamViewer et par téléphone pour un assistance technique

(2) Durée

Le contrat est établi pour une exécution unique. Cliquez ici pour saisir du texte.

## 2. Concrétisation du contenu du contrat

(1) Type et objectif du traitement prévu des données

Description plus précise de l'objet du contrat en matière de type et d’objectif des tâches du mandataire : Le client permet le support technique de se connecter sur son ordinateur en en transmettant une identification du TeamViewer.  Le client peut suivre tous les activités pendant la session TeamViewer et peut également interrompre la session a tout moment.

L'exécution du traitement des données fixé dans le contrat a lieu exclusivement dans un État membre de l'Union européenne ou dans un autre État contractuel de l'accord dans l'Espace économique européen. Tout transfert dans un pays tiers requiert l'accord préalable du mandant et ne doit être effectué que si les conditions spéciales de l'art. 44 ff. RGPD sont respectées. Le niveau de protection approprié dans le pays tiers concerné (………………………) est garanti d’apporte la garantie de clauses contractuelles type de l'Union europeenne (article 46, paragraphe 2) du RGPD auquel il se refere ici, à qui il est fait référence ici : Les clauses contractuelles pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers conformément a la directive 95/46/CE du conseil et Parlement européen

(2) Type de données

L'objet du traitement des données personnelles relève des types ou catégories de données indiqué(e)s à l'[Annexe 1](#_Anlage_1_–).

(3) Catégories de personnes concernées

Les catégories de personnes concernées par le traitement sont mentionnées à l'[Annexe 1](#_1.2_Kategorien_betroffener) :

## 3. Mesures techniques et organisationnelles

(1) Le mandataire doit documenter la mise en œuvre des mesures techniques et organisationnelles qui sont présentées avant l'attribution du mandat et requises avant le début du traitement, notamment en ce qui concerne l'exécution concrète du contrat, et remettre cette documentation au mandant pour vérification. En cas d'acceptation par le mandant, les mesures documentées constituent la base du contrat. Dans la mesure où la vérification ou un audit du mandant indique la nécessité d’une adaptation, celle-ci doit être effectuée de manière consensuelle.

(2) Le mandataire doit assurer la sécurité selon l'art. 28 al. 3 let. c, 32 RGPD, en particulier en lien avec l'art. 5 al. 1, let. 2 RGPD. Globalement, les mesures à prendre sont des mesures relatives à la sécurité des données, ainsi que la garantie d'un niveau de protection adapté au risque affectant la confidentialité, l'intégrité, la disponibilité et la capacité de charge des systèmes. Pour cela, l'état de la technique, les coûts de mise en œuvre ainsi que le type, l'étendue et les objectifs du traitement, tout comme les différentes probabilités et gravités du risque pour les droits et libertés des personnes, sont à prendre en compte, au sens de l'art. 32 al. 1 RGPD ([Annexe 3](#_Anlage_2–_Technisch-organisatorisch)).

(3) Les mesures techniques et organisationnelles sont soumises aux progrès techniques et aux développements futurs. À cet égard, le mandataire peut appliquer des mesures alternatives appropriées. Dans ce contexte, le niveau de sécurité des mesures définies doit être respecté. Les modifications importantes doivent être documentées.

## 4. Rectification, limitation et suppression de données

(1) Le mandataire ne peut pas rectifier, supprimer ou limiter le traitement des données traitées dans le cadre du contrat de son propre chef, mais uniquement après consigne documentée du mandant. Si une personne concernée contacte directement le mandataire à ce sujet, ce dernier transmettra immédiatement cette demande au mandant.

(2) Dans la mesure où ces concepts sont inclus dans l'étendue des prestations, le mandataire doit garantir la suppression, le droit à l'oubli, la rectification, la portabilité des données et le renseignement après consigne documentée du mandant.

## 5. Assurance qualité et autres obligations du mandataire

Outre les préconisations du présent contrat, le mandataire est assujetti à des obligations légales selon l'art. 28 à 33 RGPD ; dans cette mesure, il garantit notamment le respect des prescriptions suivantes :

1. Désignation écrite d'un responsable de la protection des données exerçant son activité selon l'art. 38 et 39 RGPD*. Si le mandataire n'a pas l'obligation de désigner un responsable de la protection des données, il nomme un interlocuteur pour les questions relatives à la protection des données*.

Les coordonnées du responsable de la protection des données ou de l'interlocuteur doivent être communiquées au mandant [[Annexe 1](#_1.3_Datenschutzbeauftragter_/)], et tout changement doit être immédiatement communiqué au mandant.

1. Si le siège social du mandataire se situe en dehors de l'Union européenne, il nomme le représentant suivant selon l'art. 27 al. 1 RGPD dans l'Union européenne [Annexe 1]
2. Garantie de la confidentialité selon l'art. 28 al. 3 n. 2 let. b, 29, 32 al. 4 RGPD. Pour l'exécution des tâches, le mandataire n'emploie que des personnes soumises à l'obligation de confidentialité et qui ont préalablement pris connaissance des conditions pertinentes relatives à la protection des données. Le mandataire et toute personne subordonnée au mandataire ayant accès aux données personnelles peuvent traiter ces données exclusivement selon les consignes du mandant, y compris les compétences attribuées dans le présent contrat, sauf en cas d'obligation légale de traitement.
3. Mise en œuvre et le respect de toutes les mesures techniques et organisationnelles requises pour le présent contrat selon l'art. 28 al. 3 c. 2 let. c, 32 RGPD ; ([Annexe 3](#_Anlage_3_–)).
4. Sur demande, le mandant et le mandataire doivent collaborer avec les autorités de surveillance lors de l'exécution de leurs tâches.
5. Information immédiate du mandant à propos des contrôles et mesures des autorités de surveillance, dans la mesure où ils se rapportent au présent contrat. Cette disposition s'applique également dans la mesure où une autorité responsable enquête auprès du mandataire dans le cadre d'une procédure pour infraction ou procédure pénale relative au traitement des données personnelles en lien avec le mandat.
6. Dans la mesure où le mandant est soumis de son côté à un contrôle des autorités de surveillance, une procédure pour infraction ou procédure pénale, une plainte d'une personne concernée ou d'un tiers, ou une autre plainte en lien avec l'exécution du mandat par le mandataire, ce dernier doit le soutenir au mieux de ses capacités.
7. Le mandataire contrôle régulièrement les processus internes et les mesures techniques et organisationnelles afin de garantir que le traitement dans son domaine de responsabilité correspond aux exigences du droit sur la protection des données en vigueur et que la protection des droits des personnes concernées est assurée.
8. Capacité à démontrer les mesures techniques et organisationnelles prises vis-à-vis du mandant dans le cadre de ses compétences de contrôle selon l'alinéa 7 du présent contrat.

## 6. Contrats de sous-traitance

(1) Les contrats de sous-traitance au sens du présent règlement désignent les services qui concernent immédiatement l'exécution du service principal. Cette disposition n'inclut pas les prestations annexes auxquelles le mandataire a recours, par exemple les services de télécommunications, services postaux ou de transport, la maintenance et le service utilisateur, ou l'élimination des supports de données, ainsi que les autres mesures visant à assurer la confidentialité, la disponibilité, l'intégrité et la capacité de charge du matériel et des logiciels des installations de traitement des données. Toutefois, le mandataire a l'obligation de prendre des mesures de contrôle et de conclure des accords contractuels juridiquement conformes et appropriés pour assurer la protection et la sécurité des données du mandant, y compris en cas de prestations annexes externalisées.

(2) Le mandataire peut engager des sous-traitants (autres responsables du traitement) uniquement après accord écrit explicite préalable et documenté du mandant.

1. Le mandant accepte l'engagement des sous-traitants mentionnés à l'[Annexe 2](#_Anlage_2_–_1) à la condition d'un accord contractuel selon l'art. 28 al. 2-4 RGPD.
2. L'externalisation auprès de sous-traitants ou le changement du sous-traitant existant sont autorisés, dans la mesure où :

* le mandataire présente une telle externalisation ou un tel transfert à des sous-traitants au mandant dans un format écrit ou textuel moyennant un préavis adéquat ;
* le mandant ne s’oppose pas à l'externalisation planifiée au format écrit ou textuel vis-à-vis du mandataire avant le moment du transfert des données et
* un accord contractuel selon l'art. 28 al. 2 – 4 RGPD est présenté.

(3) La transmission de données personnelles du mandant au sous-traitant et son entrée en vigueur sont autorisées uniquement si toutes les conditions d'un contrat de sous-traitance sont réunies.

(4) Si le sous-traitant réalise la prestation convenue en dehors de l'UE ou de l'EEE, le mandataire assure l'admissibilité au titre du droit sur la protection des données par le biais de mesures appropriées. Il en va de même lorsque des prestataires de services doivent être sollicités au sens de l'al. 1 phrase 2.

(5) Une externalisation supplémentaire par le sous-traitant nécessite l’accord explicite du mandant principal au format texte ; toutes les réglementations contractuelles dans la chaîne contractuelle doivent également être imposées au mandataire.

## 7. Droits de contrôle du mandant

(1) Le mandant a le droit d'effectuer des contrôles en consultation avec le mandataire ou de les faire réaliser par des contrôleurs à nommer dans les cas particuliers. Il a le droit de vérifier le respect de cet accord par le mandataire dans ses activités professionnelles par le biais de contrôles d'échantillons qui doivent généralement être annoncés en temps opportun.

(2) Le mandataire garantit que le mandant peut vérifier le respect des obligations du mandataire selon l'art. 28 RGPD. Le mandataire s'engage à donner au mandant les informations requises, et plus particulièrement de démontrer la mise en œuvre des mesures techniques et organisationnelles.

(3) La démonstration de ces mesures, qui ne concernent pas uniquement le contrat concret, peut se faire à travers :

* le respect des règles comportementales approuvées en vertu de l'art. 40 RGPD ;
* la certification selon une procédure de certification approuvée en vertu de l'art. 42 RGPD ;
* des attestations, rapports ou extraits de rapports actuels d'instances indépendantes (audit, révision, responsable de la protection des données, département de sécurité informatique, auditeurs de protection des données, auditeurs de qualité, etc.) ou
* un certificat approprié à travers un audit de sécurité informatique ou de protection des données (ISO 27001 ou protection de base BSI).

(4) Afin de permettre les contrôles par le mandant, le mandataire peut faite valoir un droit d'indemnisation.

## 8. Information en cas de non-respect de la part du mandataire

(1) Le mandataire aide le mandant à respecter les obligations citées dans les articles 32 à 36 du RGPD sur la sécurité des données personnelles, l'obligation d'information en cas de problèmes affectant les données, les études d'impact sur la protection des données et les consultations préalables. Cette disposition inclut entre autres

1. la garantie d'un niveau de protection adéquat par le biais de mesures techniques et organisationnelles qui tiennent compte des circonstances et objectifs du traitement, ainsi que de la probabilité et de la gravité envisagées d'une éventuelle violation des droits due à des failles de sécurité, et qui permettent de constater immédiatement des violations pertinentes ;
2. l'obligation de signaler immédiatement au mandant les violations des données personnelles ;
3. l'obligation d'aider le mandant dans le cadre de son obligation d'information vis-à-vis de la personne concernée et de mettre immédiatement à sa disposition toutes les informations pertinentes dans ce contexte ;
4. le soutien du mandant pour l'étude d'impact sur la protection des données ;
5. le soutien du mandant dans le cadre de consultations préalables avec les autorités de surveillance.

(2) Le mandataire peut demander une indemnisation pour les prestations de soutien non comprises dans la description des prestations ou qui ne sont pas dues à une faute du mandataire.

## 9. Compétence de consigne du mandant

(1) Le mandant confirme immédiatement les consignes orales (au format textuel).

(2) Le mandataire doit informer immédiatement le mandant s'il estime qu'une consigne est contraire aux dispositions relatives à la protection des données. Le mandataire a le droit de suspendre l'exécution de la consigne concernée jusqu'à ce que le mandant la confirme ou la modifie.

## 10. Suppression et restitution des données personnelles

(1) Aucune copie ni aucun double des données n'est créé sans la connaissance du mandant. Cette disposition ne concerne pas les copies de sécurité, dans la mesure où elles sont nécessaires à l'assurance d'un traitement des données conforme, ainsi que les données requises pour le respect des obligations légales de conservation.

(2) Après la fin des tâches contractuelles ou plus tôt sur demande du mandant (au plus tard à la fin du contrat de prestation), le mandataire doit remettre au mandant tous les documents entrés en sa possession, les résultats obtenus via le traitement et l'utilisation, ainsi que les stocks de données en lien avec la relation contractuelle, ou il doit les détruire de manière conforme à la protection des données après accord préalable. Il en va de même pour les supports de test et les contenus résiduels. Le protocole de suppression doit être présenté sur demande.

(3) Le mandataire doit conserver les documents servant à démontrer que le traitement des données est correct et conforme au contrat au-delà de la fin du contrat, conformément aux délais de conservation pertinents. Pour se décharger de cette tâche, il peut transmettre ces documents au mandant à la fin du contrat.

## 11. Dispositions finales

(1) Les accords complémentaires à cet accord-cadre requièrent une forme écrite.

(2) Les parties impliquées dans le présent contrat conviennent que les éventuelles « conditions générales » du mandataire ne s'appliquent pas au présent contrat.

(3) La résiliation requiert une forme écrite.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Lieu, date |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Mandant |  | Mandant |
| Signature, nom, poste |  | Signature, nom, poste |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Lieu, date |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| ppp Andrea Spengler Mandataire |  | Mandataire |
| Signature, nom, poste |  | Signature, nom, poste |

## Types de données

Données personnelles

Données de communication (ex : téléphone, e-mail)

Données contractuelles de base (relation contractuelle, intérêts du produit ou du contrat)

Historique des clients et fournisseurs

Données de paiement et règlement contractuel

Informations (de tiers, par exemple agences de renseignement ou de dossiers publics)

Images

Catégories spéciales de données personnelles (art. 9 RGPD)

Données personnelles sur les jugements pénaux et délictuels (art. 10 RGPD)

L'adresse IP du client.

## 1.2 Catégories des personnes concernées

Clients

Personnes intéressées

Abonnés

Employés

Employés d'entreprises liées au mandant

Employés d'entreprises dans lesquelles le mandant détient des participations

Fournisseurs

Représentants commerciaux

Interlocuteurs

…

## 1.3 Responsable de la protection des données ou interlocuteur auprès du mandataire

Prénom et nom : Arnd Fackeldey

Poste ou fonction : Datenschutzbeauftragter

Lieu, adresse : Digital Compliance Consulting GmbH / Heinrich-Dauer-Straße 10, 52351 Düren

Numéro de téléphone : +49 (0)2421/555933

Adresse e-mail : fackeldey@digital-compliance-consulting.com

## 1.4 Représentant du responsable du traitement (*si nécessaire selon l'art. 27 RGPD*)

Prénom et nom : Andrea Spengler

Unité organisationnelle : Customer Service

Lieu, adresse : Nikolaus-Groß-Strasse 13, 44329 Dortmund

Numéro de téléphone : +49 231/5436-0

Adresse e-mail : privacy@tandbergdata.com

|  |  |  |
| --- | --- | --- |
| Sous-traitant | Adresse | Prestation |
| Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. |
| Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. |
| Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. |
| Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. | Cliquez ici pour saisir du texte. |

# 1. Confidentialité (art. 32 al. 1 let. b RGPD)

* Contrôle d'entrée  
  Pas d'entrée non autorisée dans les installations de traitement des données, par ex. cartes magnétiques ou à puce, clés, dispositifs électriques d'ouverture de porte, sécurité du bâtiment ou concierge, alarmes, installations vidéo ;
* Contrôle d'accès  
  Pas d'utilisation non autorisée du système, par ex. mots de passe (sûrs), mécanismes de verrouillage automatiques, authentification bifactorielle, chiffrement des supports de données ;
* Contrôle de manipulation  
  Pas de lecture, copie, modification ou suppression non autorisée dans le système, par ex. concepts d'autorisation et droits d'accès conformes aux besoins, protocoles d'accès ;
* Contrôle de séparation  
  Traitement séparé des données collectées à des fins différentes, par ex. capacité des mandants, système de « bac à sable » ;
* Pseudonymisation (art. 32 al. 1 let. a RGPD ; art. 25 al. 1 RGPD). Traitement des données personnelles visant à ce que les données ne puissent plus être affectées à une personne spécifiques sans l'ajout d'informations complémentaires, dans la mesure où ces informations complémentaires sont conservées séparément et soumises à des mesures techniques et organisationnelles appropriées.

## 2. Confidentialité (art. 32 al. 1 let. b RGPD)

* Contrôle de transmission  
  Pas de lecture, copie, modification ou suppression non autorisée dans le système, par ex. chiffrement, réseaux privés virtuels (VPN), signature électronique ;
* Contrôle de saisie  
  Vérifier si et pour qui des données personnelles ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données, par ex. journalisation, gestion des documents ;

## 3. Disponibilité et durabilité (art. 32 al. 1 let. b RGPD)

* Contrôle de disponibilité  
  Protection contre la destruction ou la perte accidentelle ou délibérée, par ex. stratégie de sauvegarde (en/hors ligne, sur/hors site), alimentation électrique ininterrompue, protection antivirus, pare-feu, voies de signalement et plans d'urgence ;
* Capacité de restauration rapide (art. 32 al. 1 let. c RGPD)

## 4. Procédure de contrôle et d'évaluation régulière (art. 32 al. 1 let. d RGPD ; art. 25 al. 1 RGPD)

* Gestion de la protection des données ;
* Gestion de la réponse aux incidents ;
* Préconfigurations conformes à la protection des données (art. 25 al. 2 RGPD) ;
* Contrôle contractuel  
  Pas de traitement des données contractuelles au sens de l'art. 28 RGPD sans consigne du mandant en ce sens, par ex. structure claire du contrat, gestion formalisée du contrat, sélection stricte du prestataire de services, obligation de contrôle préalable, contrôles ultérieurs.

Tandberg Data GmbH

Amtsgericht Dortmund HRB 5589

Geschäftsführer Kurt Kalbfleisch