

## CONVENTION DE TRAITEMENT DE DONNÉES

### ENTRE

**1/** La société anonyme « **TEAMLEADER** », dont le siège est établi à 9000 Gand, Dok-Noord 3A bus 101, Belgique, TVA BE-0899.623.0.35, RPM Gand, division Gand, représentée ici valablement par l'administrateur délégué Jeroen De Wit;

### **2/ Le Client**

Ci-après dénommée « **Teamleader** »

Les Parties sub 1 et 2 sont dénommées ci-après ensemble les « **Parties** » ou séparément une « **Partie** ».

### CONSIDÉRANT QUE

Dans le cadre de l'exécution de certains travaux pour le Client, Teamleader, d'une part, aura accès à des données à caractère personnel et/ou, d'autre part, devra traiter des données à caractère personnel, dont le Client est responsable en tant que responsable du traitement au sens de la **(i)** loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, du **(ii)** Règlement européen de 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE et/ou la (future) législation belge relative à la mise en œuvre du Règlement susmentionné (ci-après la « **Législation Vie privée** »).

Au moyen de la présente convention, les Parties souhaitent établir par écrit leurs accords réciproques concernant **(i)** la gestion, la sécurisation et/ou le traitement de données à caractère personnel et **(ii)** le respect des obligations de la Législation Vie privée.

### IL EST CONVENU CE QUI SUIT

#### 1 DÉFINITIONS

Dans la présente convention, les notions suivantes signifient ce qui est mentionné ci-dessous (lorsqu'elles sont écrites avec une lettre majuscule) :

**Intéressé :** Celui à qui une Donnée à Caractère Personnel a trait ;

**Fuite de Données :** Sans autorisation, la publication, l'accès, l'abus, la perte, le vol ou la destruction accidentelle ou illicite de Données à Caractère Personnel, que Teamleader Traite pour le compte du Client ;

**Services :** Tous les services que Teamleader dispense au Client en ce qui concerne la Plateforme (comme, mais sans limitation, le support, les webinars, les e-books) ;

**Mission :** Toutes les activités que Teamleader exécute pour le compte du Client, et toute autre forme de collaboration par laquelle Teamleader traite des Données à Caractère Personnel pour le Client, indépendamment du caractère juridique de la convention dans le cadre de laquelle cela a lieu ;

#### **Donnée(s) à Caractère**

**Personnel :** Toute donnée concernant une personne physique identifiée ou identifiable ;

**Plateforme :** L'application en ligne de Teamleader sous le nom de marque « Teamleader® » (numéro d'enregistrement de la marque 012661963), qui offre une intégration de différents services en vue d'une administration plus efficace de l'entreprise de ses clients. Les services en ligne facilitent entre autres la gestion et la collaboration, et se composent entre autres d'un système CRM, d'un agenda, d'une gestion des offres, de l'IPA, du module de planification des projets, du module de la facturation, du ticketage et de la voix sur IP ('Voice-over-IP') ;

**Sous-traitant Ultérieur :** Tout Sous-traitant désigné par Teamleader ;

#### **Responsable du**

**Traitement :** L'entité qui, seule ou avec d'autres, constate le but du et les moyens pour le Traitement des Données à Caractère Personnel ;

**Sous-traitant :** L'entité qui Traite des Données à Caractère Personnel au profit du Responsable du Traitement ;

**Traitement/Traiter :** Tout acte ou tout ensemble d'actes en ce qui concerne des Données à Caractère Personnel, parmi lesquelles il convient en tout cas de comprendre, mais sans limitation : la collecte, l'établissement, la conservation, la mise à jour, la modification, la recherche, la consultation, l'utilisation, la fourniture au moyen d'un envoi, la diffusion ou une quelconque autre forme de mise à disposition, le rassemblement, la mise en liaison de Données à Caractère Personnel, ainsi que la protection, l'effacement, ou la destruction de Données à Caractère Personnel.

Les annexes suivantes font partie de la présente convention :

**Annexe I :** Aperçu **(i)** des Données à Caractère Personnel que les Parties prévoient de traiter, **(ii)** les catégories des Intéressés dont les Parties prévoient de traiter des Données à Caractère Personnel, **(iii)** de l'utilisation (c.-à-d. le(s) mode(s) de Traitement) des Données à Caractère Personnel, **(iv)** des fins et des moyens du (des) Traitement(s) et **(v)** du (des) délai(s) d'utilisation et de conservation des (différents types de) Données à Caractère Personnel ;

**Annexe II :** Aperçu et description des mesures de sécurité prises par Teamleader.

#### 2 QUALITÉ DES PARTIES

Les Parties reconnaissent et acceptent, dans le cadre du Traitement des Données à Caractère Personnel, que le Client sera considéré comme le 'Responsable du Traitement' et Teamleader comme le 'Sous-traitant'. En outre, Teamleader sera habilitée à faire appel à des Sous-traitants Ultérieurs conformément aux dispositions de l'**Article 6**.

#### 3 UTILISATION DE LA PLATEFORME ET/OU DES SERVICES

##### 3.1 Le Client reconnaît expressément que :

- ✓ Teamleader intervient uniquement en tant que facilitateur de la Plateforme et/ou des Services, de sorte que le Client supporte seul la responsabilité de la manière dont il utilise la Plateforme et/ou les Services ;

- ✓ En conséquence de l'utilisation qu'il fait de la Plateforme, un certain nombre d'intégrations seront automatiquement faites par le biais de l'interface de programmation de l'application (IPA). Toutes les autres intégrations offertes par Teamleader sont optionnelles et ne seront exécutées qu'à la demande expresse du Client ;
- ✓ Il est le seul responsable du respect de toutes les législations et réglementations (notamment en ce qui concerne le délai de conservation), qui s'appliquent à lui en conséquence de l'utilisation qu'il fait de la Plateforme et/ou des Services.

**3.2** En cas d'abus par le Client de la Plateforme et/ou des Services, le Client accepte que Teamleader ne pourra en aucun cas être tenue pour responsable à cet égard, ni de quelconques dommages qui découlent de l'abus précité.

**3.3** Le Client s'engage donc à garantir Teamleader contre un tel abus, ainsi que contre toute réclamation d'un Intéressé et/ou d'une quelconque tierce partie en conséquence de l'abus commis par le Client.

#### **4 OBJET**

**4.1** Le Client reconnaît qu'en conséquence de l'utilisation qu'il fait de la Plateforme et/ou des Services de Teamleader, la dernière citée Traitera les Données à Caractère Personnel - telles que collectées par le Client.

**4.2** Teamleader Traitera les Données à Caractère Personnel de façon convenable et minutieuse, et ce en conformité avec la Législation Vie privée et avec une autre réglementation applicable relative au Traitement de Données à Caractère Personnel.

Plus précisément, Teamleader mettra tout son savoir-faire à disposition, dans l'exécution de la Mission, pour exécuter la Mission selon les règles de l'art, comme il sied à un « bon » Sous-traitant spécialisé.

**4.3** Teamleader ne Traitera toutefois les Données à Caractère Personnel que pour le compte du Client et suivra toutes les instructions du Client, telles que décrites à l'**Annexe I**, à ce sujet, sauf obligations légales dérogatoires.

**4.4** Le Client, en tant que Responsable du Traitement, a et conserve le contrôle total concernant entre autres (i) le Traitement des Données à Caractère Personnel, (ii) quelles Données à Caractère Personnel sont collectées, (iii) le but du Traitement et (iv) la question de savoir si le Traitement est proportionnel.

En outre, le Client est le seul responsable du respect de toutes les obligations (légales) qui reposent sur lui en tant que Responsable du traitement (notamment concernant le délai de conservation), ainsi que de l'exactitude, de la qualité et de la légitimité des Données à caractère personnel, encodées dans la Plateforme, et de la manière dont il a acquis les Données à caractère personnel.

Le contrôle des Données à Caractère Personnel dispensé dans le cadre de la présente convention ne repose dès lors jamais sur Teamleader.

#### **5 MESURES DE SÉCURITÉ**

Compte tenu de l'état de la technique, Teamleader prendra toutes les mesures techniques et organisationnelles appropriées pour sécuriser les Données à Caractère Personnel et pour maintenir leur sécurité de façon adéquate – y compris la sécurisation contre toute forme d'utilisation et/ou de Traitement et de sécurisation imprudent(e), non expert(e), non compétent(e) ou illicite contre la perte, la destruction ou les dommages – ainsi que pour la protection de la confidentialité et de l'intégrité des Données à Caractère Personnel, telles que décrites à l'**Annexe II**.

#### **6 SOUS-TRAITANTS ULTÉRIEURS**

**6.1** Le Client reconnaît et accepte que Teamleader soit habilitée à faire appel à des Sous-traitants Ultérieurs pour l'exécution de la Mission. Dans un tel cas, Teamleader veille à ce que les Sous-traitants Ultérieurs soient au moins liés par les mêmes obligations que celles

par lesquelles Teamleader est liée sur la base de la présente convention.

**6.2** Teamleader s'engage à mettre à la disposition de la Plateforme deux (2) listes concernant l'appel qu'elle fait à des Sous-traitants Ultérieurs pour l'exécution de la Mission, à savoir :

- ✓ Une liste des Sous-traitants Ultérieurs auxquels Teamleader fait toujours appel, vu que ces intégrations sont prévues de façon standard (cf. **Article 3.1**) ; et
- ✓ Une liste des Sous-traitants Ultérieurs optionnels, auxquels Teamleader fait seulement appel lorsque le Client a opté pour cette (ces) intégration(s) (cf. **Article 3.1**).

De telles listes contiennent l'identité des Sous-traitants Ultérieurs, ainsi que leur pays d'établissement.

**6.3** Teamleader s'engage à informer le Client par écrit lorsqu'elle modifiera la liste des Sous-traitants Ultérieurs (comme, mais sans limitation, l'ajout et/ou le remplacement d'un Sous-traitant Ultérieur).

**6.4** Sans préjudice de l'**Article 6.3**, le Client a le droit de s'opposer à un nouveau Sous-traitant Ultérieur engagé par Teamleader lorsqu'il s'agit d'un Sous-traitant Ultérieur d'une intégration standard.

Lorsque le Client souhaite exercer son droit d'opposition, il doit en informer Teamleader par écrit et de façon motivée, et ce au plus tard dans les dix (10) jours suivant la réception de la notification précitée par le Client (cf. **Article 6.3**)

**6.5** Au cas où le Client formulerait une objection contre un nouveau Sous-traitant Ultérieur et où cette objection ne serait pas considérée comme déraisonnable, Teamleader mettra à la disposition du client, au mieux de sa capacité, (i) une modification apportée dans la Plateforme et/ou dans les Services, ou (ii) recommandera au Client d'effectuer une modification commerciale et raisonnable de sa configuration ou de l'utilisation de la Plateforme et/ou des Services, de manière à éviter que des Données à Caractère Personnel ne soient Traitées par le Sous-traitant Ultérieur auquel il s'est opposé, sans que cela ne puisse toutefois entraîner des conséquences déraisonnables pour le Client.

Si Teamleader n'est pas en mesure de mettre une telle modification à disposition du Client dans un délai raisonnable (lequel ne dépassera pas trente (30) jours calendrier suivant la contestation du Client), le Client sera habilité à résilier la convention conclue avec Teamleader à condition que :

- ✓ La Plateforme ne puisse être utilisée par le Client sans qu'il ne soit fait appel à un Sous-traitant Ultérieur auquel le Client s'est opposé ; et/ou que
- ✓ La résiliation ait uniquement trait aux Services qui ne peuvent être livrés par Teamleader sans faire appel à un Sous-traitant Ultérieur auquel le Client s'est opposé ;

et ce en informant Teamleader dans un délai raisonnable, au moyen d'un courrier recommandé.

#### **7 DÉLÉGUÉ À LA PROTECTION DES DONNÉES**

**7.1** Teamleader a désigné un délégué à la protection des données ('DPO').

**7.2** Ce délégué à la protection des données est joignable au moyen de l'adresse e-mail suivante : [dpo@teamleader.eu](mailto:dpo@teamleader.eu).

#### **8 TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL EN DEHORS DE L'EEE**

Tout transfert de Données à Caractère Personnel en dehors de l'Espace économique européen (EEE) à un destinataire qui a son domicile ou son siège dans un pays qui ne tombe pas sous une décision d'adéquation, promulguée par la Commission européenne, sera régi par les dispositions d'une convention de transfert de données, laquelle contiendra (i) les clauses contractuelles standards telles que définies dans la 'Décision de la Commission européenne du

5 février 2010 (Décision 2010/87/CE)', ou (ii) un quelconque autre mécanisme sur la base de la Législation Vie privée et/ou d'une autre réglementation applicable relative au Traitement de Données à Caractère Personnel.

## 9 CONFIDENTIALITÉ

**9.1** Teamleader observe la confidentialité des Données à Caractère Personnel. Teamleader ne mettra donc pas les Données à Caractère Personnel à la disposition de tiers, ni ne transférera celles-ci sans l'approbation écrite préalable du Client, sauf lorsque :

- ✓ La présente convention déroge à cette règle ;
- ✓ La publication/communication est requise par la loi ou par une décision judiciaire ou émanant d'une autre autorité (de quelque nature que ce soit). Dans un tel cas, Teamleader discutera avec le client, préalablement à la publication et/ou à la communication, de l'ampleur et du mode de la publication/communication.

**9.2** Teamleader s'engage à ce que son personnel, chargé de l'exécution de la Mission et qui a connaissance de la nature confidentielle des Données à Caractère Personnel, ait reçu une formation adéquate concernant ses responsabilités et qu'il soit lié par une convention de confidentialité. Teamleader s'engage en outre à ce que de telles obligations de confidentialité subsistent après la fin du contrat de travail.

**9.3** Teamleader garantit que l'accès aux Données à Caractère Personnel est limité au personnel qui est chargé de l'exécution de la Mission en conformité avec la présente convention.

## 10 NOTIFICATION

**10.1** Teamleader essaie, au mieux de ses capacités, d'informer le Client dans un délai raisonnable lorsqu'elle :

- ✓ Reçoit une demande d'information, une citation ou une requête en inspection ou en audit d'une instance publique compétente, en rapport avec le Traitement des Données à Caractère Personnel ;
- ✓ A l'intention de mettre les Données à Caractère Personnel à la disposition d'une instance publique compétente ;
- ✓ Constate ou présume raisonnablement qu'une Fuite de Données s'est produite en ce qui concerne les Données à Caractère Personnel.

**10.2** Dans le cas d'une Fuite de Données, Teamleader s'engage à :

- ✓ En informer le Client, sans retard inutile suivant la constatation d'une Fuite de Données, ainsi que, dans la mesure du possible, à accorder son assistance au Client dans le cadre de son obligation de faire rapport sur la base de la Législation Vie privée ;
- ✓ Aussi vite que cela est raisonnablement possible, prendre les mesures appropriées et correctrices pour mettre fin à la Fuite de Données et pour prévenir et/ou limiter une éventuelle Fuite de Données à l'avenir.

## 11 DROITS DE L'INTÉRESSÉ

**11.1** Dans la mesure où le Client - dans le cadre de l'utilisation qu'il fait de la Plateforme et/ou des Services - n'est pas en mesure de corriger, de modifier, de bloquer ou de supprimer les Données à Caractère Personnel, tel que requis par la Législation Vie privée, Teamleader satisfera - pour autant qu'elle y est légalement tenue - à une demande commerciale raisonnable du Client visant à permettre de tels actes.

Dans la mesure permise par la loi, le Client sera responsable de tous les frais que Teamleader doit supporter en conséquence d'une telle assistance.

**11.2** Teamleader informera le Client sans délai, dans la mesure permise par la loi, lorsqu'elle reçoit une demande d'un Intéressé concernant l'accès aux, la correction, la modification ou la suppression des Données à Caractère Personnel de l'Intéressé. Teamleader ne réagira

toutefois pas à une telle demande d'un Intéressé sans l'autorisation écrite préalable du Client, sauf pour confirmer que la demande a trait au Client pour lequel le Client a donc donné son accord.

Teamleader accordera au Client une collaboration et assistance commerciale et raisonnable dans le cadre du traitement d'une demande d'un Intéressé concernant l'accès aux, la correction, la modification ou la suppression des Données à Caractère Personnel de cet Intéressé, dans la mesure permise par la loi et pour autant que le Client n'ait lui-même pas accès à de telles Données à Caractère Personnel au moyen de l'utilisation qu'il fait de la Plateforme et/ou des Services.

Dans la mesure permise par la loi, le Client sera responsable de tous les frais que Teamleader doit supporter en conséquence d'une telle assistance.

**11.3** Si Teamleader doit effacer les Données à Caractère Personnel d'un Intéressé - dans le cadre de l'assistance précitée -, le Client reconnaît que Teamleader ne peut être tenue pour responsable lorsqu'elle doit de nouveau Traiter, après la suppression, les Données à Caractère Personnel de cet Intéressé dans le cadre d'une convention qu'elle a conclue avec un client.

## 12 BIFFURE OU RESTITUTION DE DONNÉES À CARACTÈRE PERSONNEL

**12.1** Après la fin de la Mission et/ou en cas de résiliation de la convention, Teamleader informera le client du fait qu'il a la possibilité, pendant la période telle que communiquée dans la notification précitée, d'exporter les Données à Caractère Personnel de la Plateforme au moyen des outils d'exportation disponibles.

**12.2** Une fois que le délai d'exportation précité a expiré, Teamleader effacera d'abord les Données à caractère personnel via une « suppression réversible ('soft deletion') » et après un certain délai de six (6) mois anonymiser les Données à Caractère Personnel.

## 13 CONTRÔLE

**13.1** Teamleader essaie de mettre à disposition toutes les informations qui sont nécessaires pour permettre au Client de vérifier si Teamleader respecte les dispositions de la convention.

**13.2** Dans ce cadre, Teamleader doit également permettre au Client (ou à un tiers auquel le dernier cité fait appel) d'exécuter des inspections - comme, mais sans limitation, les audits - et d'accorder la collaboration nécessaire à cette fin.

## 14 DISPOSITIONS FINALES

**14.1** La présente convention dure aussi longtemps que la Mission dure. Les dispositions de la présente convention continuent de s'appliquer pour autant que nécessaire pour le déroulement de la présente convention et pour autant que celles-ci soient destinées à survivre la fin de la présente convention (comme, mais sans limitation, les **Articles 9 et 15**).

**14.2** L'éventuelle nullité d'une ou de plusieurs clauses de la présente convention ou d'une partie de celle-ci ne fait pas préjudice à la validité et à l'applicabilité des autres clauses et/ou du reste de la disposition en question. En cas de nullité d'une ou de plusieurs clauses, les Parties négocieront pour remplacer la disposition nulle par une disposition équivalente qui répond à l'esprit de cette disposition. Si les Parties ne parviennent pas à un accord, le juge compétent pourra atténuer la disposition nulle jusqu'à ce qui est (légalement) permis.

**14.3** Les dérogations, les modifications et/ou les additions à la convention ne sont valables et impératives pour autant qu'elles aient été acceptées par les deux Parties.

**14.4** La présente convention, ainsi que les droits et obligations qui en découlent pour les Parties, ne sont pas cessibles, directement ou indirectement, sans l'accord écrit préalable de l'autre Partie.

**14.5** La non-application éventuelle ou même répétée d'un quelconque droit par les Parties ne peut être considérée que comme de la

tolérance à l'égard d'une certaine situation, et n'entraîne pas de forclusion.

**14.6** La présente convention a la primauté sur toutes autres conventions conclues entre le Client et Teamleader.

**15 DROIT & JURIDICTION APPLICABLES**

**15.1** La présente convention et son exécution seront exclusivement régies par le et interprétées conformément au droit belge.

**15.2** Tous les éventuels litiges et difficultés qui se seraient produits concernant l'exécution et/ou l'explication de la présente convention, relèvent de la compétence exclusive des tribunaux de l'arrondissement où Teamleader a son siège social.

\*\*\*\*\*

**Annexes :**

- Annexe I – Aperçu de Données à Caractère Personnel
- Annexe II – Description des mesures de sécurité

## Annexe I – Aperçu de Données à Caractère Personnel <sup>1</sup>

### I. Voici les Données à Caractère Personnel que les Parties prévoient de Traiter :

- Nom
- Prénom
- Nom du compte
- Mot de passe
- Adresse e-mail
- Numéro de téléphone (fixe/gsm)
- Adresse de domicile
- N° de compte
- Code bancaire
- Autres Données à Caractère Personnel dépendant des champs libres que le Client a lui-même ajoutés

### II. Les catégories des Intéressés dont les Parties prévoient de traiter des Données à Caractère Personnel :

- Travailleurs
- Prospects
- Clients
- Fournisseurs
- Partenaires commerciaux
- Autre(s)

### III. L'utilisation (= mode(s) de Traitement) des Données à Caractère Personnel et les moyens pour et les buts du Traitement :

#### Utilisation des Données à Caractère Personnel :

- Stockage sur la Plateforme et/ou dans l'Appli
- Traitement

#### Moyen de Traitement :

- Logiciel développé par Teamleader
- Intégrations
  - Les intégrations standards
  - Les intégrations pour lesquelles le Client a lui-même opté

#### But du Traitement :

- Intégrations standards
  - Gestion des tâches, des réunions et des appels
  - Ajout de Données à Caractère Personnel à l'outil CRM en vue du suivi des e-mails envoyés et de la gestion de contacts et d'entreprises
  - Suivi d'un projet de vente (y compris la gestion des offres)
  - Planification des projets (y compris les projets internes)
  - Facturation
  - Gestion des utilisateurs / des équipes d'utilisateurs de la Plateforme
  - Enregistrement du temps
  - Élaboration et gestion de tickets de support (y compris les statistiques de ceux-ci)
  - Élaboration et gestion de buts
  - Voix sur IP
  - Gestion de mailings (ciblés)
  - Élaboration et gestion de formulaires d'envoi
  - Élaboration et gestion de commandes

<sup>1</sup> Le Client reconnaît que l'énumération ci-dessus donne un aperçu général des Données à caractère personnel que Teamleader peut traiter par le biais de sa Plateforme. Au cas où la Plateforme serait customisée sur demande du Client (via des intégrations disponibles sur Marketplace), un aperçu customisé/actualisé pourra, à la demande expresse du Client, être transmis ou mis à disposition par le biais de la Plateforme.

- Élaboration, planification et gestion d'événements
- Enregistrement et conservation de documents
- Création de comptes de Teamleader par le Client
- Gestion des stocks
- Les intégrations pour lesquelles le Client a lui-même opté (les buts du Traitement de ces intégrations dépendent des intégrations choisies)

**IV. Les délais d'utilisation et de conservation des (différents types de) Données à Caractère Personnel :**

Teamleader conservera les Données à caractère personnel tant que la Mission et/ou le contrat est en cours. Une fois la Mission et/ou le contrat terminé et que la période d'exportation par le client a expiré, Teamleader effacera d'abord les Données à caractère personnel via une « suppression réversible ('soft deletion') » et ensuite, après un certain délai de six (6) mois anonymiser les Données à Caractère Personnel.

Une fois que le délai d'exportation précité a expiré, Teamleader effacera d'abord les Données à caractère personnel via une « suppression réversible ('soft deletion') » et après un certain délai de six (6) mois.

En dérogation à cette règle générale, le cas échéant, Teamleader appliquera un délai de conservation plus court sur base duquel Teamleader effacera déjà les Données à caractère personnel via une « suppression réversible ». Dans tous les cas, cette « suppression réversible » sera suivie d'une anonymisation à la fin de la Mission et/ou du contrat (conformément à ce qui est exposé ci-dessus).

Teamleader opte pour une « suppression réversible » notamment afin de rattraper des erreurs dans le chef du Client et réactiver le compte Teamleader après la fermeture de celui-ci.

Finalement, Teamleader se réserve le droit de conserver les Données à Caractère Personnel anonymes (ou une partie de celles-ci) après la fin de la Mission / du contrat, à des fins statistiques et analytiques.

## Annexe II – Description des mesures de sécurité

*Le présent document reprend les mesures de sécurité techniques et organisationnelles mises en place par Teamleader afin de soutenir ses activités (de Traitement) conformément à la Législation relative à la protection de la vie privée.*

### I. Contrôle des accès aux zones de traitement (physique)

Les applications Web, ainsi que les serveurs de communications et de bases de données de Teamleader sont situés en Irlande dans des centres de données sécurisés, lesquels sont gérés par Amazon Web Services, Inc. (AWS). Teamleader a signé avec AWS le « AWS Data Processing Addendum » (l'addendum d'AWS relatif au Traitement des Données) afin de se conformer aux normes et aux obligations fixées par la Législation relative à la protection de la vie privée.

### II. Contrôle des accès aux systèmes de Traitement des Données à Caractère Personnel (logique)

Teamleader a mis en place des mesures adaptées pour empêcher que des personnes non autorisées utilisent ses systèmes de Traitement des Données à Caractère Personnel.

Cela est rendu possible par :

- L'établissement de l'identification du terminal et/ou de l'utilisateur du terminal des systèmes de Teamleader ;
- La déconnexion automatique du terminal utilisateur en cas d'inactivité. L'obligation de s'identifier et d'entrer un mot de passe pour rouvrir une session ;
- Le verrouillage automatique de l'identifiant de l'utilisateur après un certain nombre de mots de passe erronés. L'enregistrement de l'activité, ainsi que des examens réguliers des registres d'activité ;
- L'utilisation de pare-feu, de routeurs et de contrôles des accès basés sur un réseau VPN afin de protéger les réseaux de service privés et les serveurs dorsaux ;
- La sécurité ad hoc de l'infrastructure de contrôle ;
- Des examens réguliers des risques relatifs à la sécurité réalisés par des employés internes et des auditeurs tiers ;
- La délivrance et la sauvegarde de codes d'identification ;
- Le contrôle des accès en fonction des rôles mis en place de manière à appliquer le principe de séparation des privilèges ;
- L'enregistrement des accès aux serveurs hôtes, aux applications, aux bases de données, aux routeurs, aux commandes, etc.
- L'utilisation d'outils disponibles sur le marché et d'outils sur mesure afin d'établir et d'examiner les registres système de sa Plateforme pour déceler toute anomalie.

### III. Contrôle des disponibilités

Teamleader a mis en place des mesures adaptées pour garantir la protection des Données à Caractère Personnel contre la perte ou la destruction accidentelles.

Cela est rendu possible par :

- une infrastructure de services redondante ;
- l'évaluation continue des centres de données et des fournisseurs de services Internet (FSI) afin de maximiser pour ses clients les performances en matière de bande passante, de latence et d'isolement pour le recouvrement après un désastre ;
- le placement des centres de données dans des installations de colocalisation sécurisées qui sont neutres vis-à-vis des FSI et garantissent une sécurité physique, une alimentation redondante et une infrastructure redondante ;
- des accords de niveau de service des FSI permettant de garantir un temps de disponibilité optimal ;
- une capacité rapide de basculement.

### IV. Contrôle de transmission

Teamleader a mis en place des mesures adaptées pour empêcher la lecture, la reproduction, la modification ou la suppression par des parties non autorisées des Données à Caractère Personnel pendant la transmission desdites données ou le transport des supports de données.

Cela est rendu possible par :

- l'utilisation de technologies de pare-feu et de cryptage adéquates afin de protéger les passerelles et les pipelines par lesquels passent les données ;
- le cryptage des Données sensibles à Caractère Personnel pendant leur transmission au moyen de versions à jour du protocole TLS ou d'autres protocoles de sécurisation utilisant de puissants algorithmes et clés de cryptages ;
- la protection des accès Web aux interfaces de gestion des comptes par les employés au moyen d'un cryptage TLS ;
- le cryptage de bout en bout du partage d'écran aux fins de l'accès à distance, de l'assistance et de la communication en temps réel.

### V. Contrôle d'entrée

Teamleader a mis en place des mesures adaptées pour permettre de contrôler et d'établir si les Données à Caractère Personnel ont été entrées dans les systèmes de Traitement des Données à Caractère Personnel ou supprimées, et par qui.

Cela est rendu possible par :

- l'identification du personnel autorisé ;
- des mesures de protection pour l'entrée de Données à Caractère Personnel dans la mémoire, ainsi que pour la lecture, la modification et la suppression des Données à Caractère Personnel enregistrées, y compris en documentant ou en enregistrant les changements matériels effectués sur les données ou les paramètres des comptes ;
- la séparation et la protection de toutes les Données à Caractère Personnel enregistrées au moyen de schémas de bases de données, de contrôles logiques d'accès et/ou de cryptage ;

- l'utilisation d'identifiants utilisateur ;
- la sécurité physique des installations de traitement des données ;
- la fermeture automatique de session après un délai prédéfini.

## **VI. Surveillance**

Teamleader ne consulte pas les Données à Caractère Personnel du Client, excepté :

- lorsque cela s'avère nécessaire à la fourniture des Services fixés par l'accord passé avec le Client ;
- lorsque ladite consultation favorise une meilleure expérience client ;
- lorsque la loi l'exige ; ou
- lorsque le Client en fait la demande.

Cela est rendu possible par :

- la nomination individuelle d'administrateurs système ;
- l'adoption de mesures adéquates pour la tenue de registres reprenant les accès à l'infrastructure par les administrateurs système.