ADDENDA RELATIF AU TRAITEMENT DES DONNÉES - RGPD

Le présent Addenda relatif au traitement des données (ci-après désigné par « **ATD** » ou « Addenda ») est intégré à tous les contrats existants entre le Client et CA, et/ou à tout accord papier ou électronique établi entre CA et le Client dans le cadre de l'achat de Services fournis par CA (le « **Contrat** »), afin de valider le consentement des parties concernant le Traitement des Données à caractère personnel conformément aux exigences des Lois relatives à la protection des données. La Date d'effet du présent ATD est la dernière date de signature de l'une des parties indiquées ci-dessous. Tous les termes commençant par une majuscule et non définis précisément dans les présentes sont à interpréter dans le sens défini dans le Contrat.

1. CONDITIONS GÉNÉRALES

Cet ATD s'applique au Traitement des Données à caractère personnel par CA au nom du Client dans le cadre du Règlement général sur la protection des données de l'Union européenne n° 2016/679 (tel que défini dans la Section 11 et ci-après désigné par « RGPD »). À compter du 25 mai 2018, CA s'engage à traiter les Données à caractère personnel conformément aux exigences du RGPD directement applicables à la fourniture de ses Services. Le présent ATD ne limite ni ne réduit les engagements en matière de protection des Données à caractère personnel négociés précédemment avec le Client dans le cadre du Contrat (y compris tout addenda au Contrat éventuellement existant concernant le traitement des données).

En signant cet Addenda, le Client accepte de s'y conformer en son nom propre et, dans la mesure exigée par les Lois de protection des données en vigueur, au nom et pour le compte de ses Entités affiliées autorisées, si et dans la mesure où CA assure le Traitement de Données à caractère personnel pour lequel ces Entités affiliées autorisées sont qualifiées en tant que Responsable de traitement. Dans le cadre du présent ATD uniquement, le terme « Client » désigne à la fois le Client et ses Entités affiliées autorisées, excepté en cas de mention contraire spécifique.

Dans le cadre de la prestation de ses Services au Client, au titre du Contrat, CA peut être amené à Traiter des Données à caractère personnel pour le compte du Client. CA s'engage à se conformer aux dispositions suivantes concernant toutes Données à caractère personnel traitées au nom du Client en lien avec la prestation des Services. Sauf mention contraire expresse dans la section concernée, toutes les définitions appliquées dans le cadre du présent ATD ont été regroupées dans la Section 11, intitulée « Définitions ».

2. TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1 Les parties acceptent que, en ce qui concerne le Traitement des Données à caractère personnel, le Client soit le Responsable du traitement, que CA soit le Sous-traitant et que CA ou des membres du Groupe CA engagent des Sous-traitants secondaires au titre des obligations établies dans la Section 5, « Sous-traitants secondaires », ci-dessous.

2.2 Le Client est tenu, dans son utilisation ou sa réception des Services, de Traiter les Données à caractère personnel dans le respect des Lois sur la protection des données et doit s'assurer que ses instructions concernant ledit Traitement sont conformes auxdites Lois. Il est de la seule responsabilité du Client de s'assurer de l'exactitude, de la qualité et de la légalité des Données à caractère personnel et des moyens par lesquels il a acquis ces dernières.

2.3 CA s'engage à traiter les Données à caractère personnel conformément aux Lois en vigueur sur la protection des données et aux exigences du RGPD, directement applicables à la fourniture par CA de ses Services. CA doit traiter uniquement les Données à caractère personnel pour le compte du Client et conformément à ses instructions documentées, et traiter lesdites Données à caractère personnel en tant qu'Informations confidentielles. Le Client demande à CA de Traiter ses Données à caractère personnel aux fins suivantes : (i) Traitement des Données à

caractère personnel dans le cadre du Contrat et des commandes associées ; (ii) Traitement des Données à caractère personnel nécessaire pour le respect d'instructions autres fournies par le Client, dans la limite du raisonnable (ex., via un ticket de support), lorsque lesdites instructions sont conformes aux dispositions du Contrat ; et (iii) Traitement des Données à caractère personnel requis par la loi en vigueur à laquelle CA ou les Entités affiliées CA sont soumis, y compris, sans s'y limiter, les Lois de protection des données en vigueur, auquel cas CA ou les Entités affiliées CA concernées doivent, dans la mesure permise par la loi, informer le Client d'un tel Traitement des Données à caractère personnel imposé par la loi.

2.4. Tel que stipulé dans l'Article 28, § 3 du RGPD, « l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées » sont définis dans l'Annexe I du présent Addenda (intitulée « Annexe 1 : Détails relatifs au traitement des données à caractère personnel du Client »). L'objet du Traitement des Données à caractère personnel par CA est la prestation des Services fournis dans le cadre du Contrat. Par une demande écrite préalable, le Client peut requérir une modification raisonnable de l'Annexe 1, s'il la considère raisonnablement nécessaire pour satisfaire aux dispositions de l'Article 28, § 3 du RGPD ; CA examinera les modifications demandées. Rien dans l'Annexe 1 ne confère de droit ni n'impose d'obligation aux parties concernées par le présent Addenda.

3. DROITS DES PERSONNES CONCERNÉES

3.1. CA est tenu, dans les limites autorisées par la loi, d'informer rapidement le Client lorsqu'il reçoit une demande de la part d'une Personne concernée pour exercer ses droits d'accès, de rectification, de limitation du Traitement, d'effacement (« droit à l'oubli »), de portabilité des données, d'opposition au Traitement ou son droit à refuser d'être soumise à une prise de décision individuelle automatisée (« **Demande de la Personne concernée**"). En tenant compte de la nature du Traitement, CA se doit d'assister le Client par toutes les mesures techniques et organisationnelles appropriées, dans la mesure du possible, afin que le Client puisse respecter son obligation de réponse à une Demande de la Personne concernée, au titre du Chapitre III du RGPD. Excepté lorsque la loi en vigueur l'y oblige, CA ne doit jamais répondre à ce type de Demande de la Personne concernée sans l'accord écrit préalable du Client, sauf pour confirmer que la demande concerne le Client.

3.2 D'autre part, dans la mesure où le Client, dans son utilisation des Services, n'a pas la capacité à prendre en charge la Demande de la Personne concernée, CA se doit, à la demande du Client, de fournir tous les efforts commercialement raisonnables pour aider ce dernier à répondre à la Demande de la Personne concernée, dans la mesure où CA est légalement autorisé à le faire et dans la mesure où ladite Demande de la Personne concernée est requise conformément aux Lois sur la protection des données en vigueur. Tous les frais découlant de cette prestation d'assistance seront à la charge du Client, dans les limites autorisées par la loi.

4. PERSONNEL

4.1 CA doit s'assurer que son personnel chargé du Traitement des Données à caractère personnel est informé de la nature confidentielle des Données à caractère personnel, a reçu une formation appropriée sur ses responsabilités, est soumis aux obligations de confidentialité, et comprend que ces obligations de confidentialité se poursuivront même après la fin de ses engagements auprès de CA.

4.2 CA doit prendre toutes les mesures commercialement raisonnables pour s'assurer de la fiabilité du personnel qu'il affecte au Traitement des Données à caractère personnel.

4.3 CA doit s'assurer que l'accès aux Données à caractère personnel par le Groupe CA est limité au personnel pour lequel un tel accès est nécessaire pour l'exécution du Contrat.

4.4 Délégué à la protection des données. Les membres du Groupe CA ont nommé un délégué à la protection des données lorsque cela était imposé par les Lois sur la protection des données. La personne nommée à ce poste est joignable à l'adresse datatransfers@ca.com.

5. SOUS-TRAITANTS SECONDAIRES

5.1 Le Client reconnaît et accepte que (a) des Entités affiliées CA puissent être désignées comme Sous-traitants secondaires ; et que (b) CA et des Entités affiliées CA, respectivement, puissent faire appel à des Sous-traitants secondaires tiers dans le cadre de la prestation des Services. Lesdits Sous-traitants secondaires sont autorisés à recueillir des Données à caractère personnel dans l'exécution des Services pour lesquels CA a fait appel à eux, mais il leur est interdit d'utiliser lesdites Données à caractère personnel à d'autres fins.

5.2 CA est responsable des actes et omissions de ses Sous-traitants secondaires, de la même manière que CA serait responsable si l'exécution des Services par chaque Sous-traitant secondaire s'effectuait selon les dispositions du présent ATD, sauf disposition contraire dans le Contrat.

5.3 CA ou une Entité affiliée CA a signé un accord écrit avec chaque Sous-traitant secondaire, stipulant des obligations de protection des données ne pouvant être moins strictes que les dispositions établies dans le présent Addenda au regard de la protection des Données à caractère personnel et qui satisfont aux exigences de l'Article 28, § 3 du RGPD ou aux dispositions équivalentes de toute autre Loi sur la protection des données, dans la mesure applicable à la nature des Services fournis par les Sous-traitants secondaires.

5.4 Le Client autorise CA et chaque Entité affiliée CA à engager des Sous-traitants secondaires, dans le respect du présent Article 5. La liste des Sous-traitants secondaires auxquels CA fait appel dans le cadre de la prestation des Services est indiquée dans l'Annexe 2 ; ladite liste inclut l'identité et le pays de chaque Sous-traitant secondaire (« **Liste des Sous-traitants secondaires** »). En cas de changement ou d'ajout par CA à cette liste, la Liste des Sous-traitants secondaires à jour sera mise à disposition du Client à l'adresse suivante : https://support.ca.com/us/product-content/admin-content/subprocessor-list.html.. Le Client a alors l'opportunité de s'opposer aux modifications apportées (tel qu'indiqué dans l'Article 5.5 ci-dessous).

5.5. Le Client peut s'opposer à l'emploi par CA d'un nouveau Sous-traitant secondaire, en notifiant au plus vite CA par écrit de sa décision, dans un délai de dix (10) jours ouvrés après la mise à jour par CA de la Liste des Sous-traitants secondaires. En cas d'objections soulevées par le Client, CA est tenue de prendre toutes les mesures commercialement raisonnables pour répondre à ces objections et fournir au Client une explication raisonnable, par écrit, desdites mesures.

5.6. Transferts de données. Il est interdit à CA de transférer les Données à caractère personnel du Client, excepté lorsque la loi l'y autorise et en conformité avec les Lois sur la protection des données en vigueur. Les Données à caractère personnel devront être transférées conformément à la déclaration de CA et aux dispositions établies dans le document https://www.ca.com/fr/legal/privacy/data-transfers.html. Uniquement dans le cadre de la prestation des Services au Client, au titre du Contrat, et conformément aux dispositions du présent Article 5.6, le Client autorise par les présentes CA à effectuer des transferts de routine des Données à caractère personnel à destination d'une entité locale du Groupe CA et/ou de Sous-traitants secondaires agréés par CA. Néanmoins, si les Données à caractère personnel du Client devaient être transférées depuis l'Union européenne, l'Espace économique européen et/ou ses États membres, la Suisse et le Royaume-Uni, vers des pays ne garantissant pas un niveau de protection des données adéquat, au sens entendu par les Lois sur la protection des données des territoires susmentionnés

(« **Transferts interdits »**), CA s'engage à se conformer aux dispositions de l'Article 5.6(a) en ce qui concerne lesdits Transferts interdits.

(a) **Mécanismes de transfert pour les Transferts interdits.** CA propose les mécanismes de transfert suivants qui doivent être appliqués à tous les Transferts interdits au titre du présent ATD, dans la mesure où lesdits transferts sont soumis aux Lois sur la protection des données concernées :

(1) **Autocertifications dans le cadre du Bouclier de protection des données**. CA a certifié sa conformité au programme de Bouclier de protection des données UE-États-Unis. CA doit garantir sa certification au titre du Bouclier de protection des données tant qu'il conserve des Données à caractère personnel de l'EEE. Si des autorités ou des tribunaux de l'UE venaient à déterminer que le Bouclier de protection des données n'est pas une base appropriée pour les transferts, les parties devront exécuter rapidement les clauses contractuelles types approuvées par l'UE (Sous-traitants), qui devront alors être intégrées aux présentes dès leur exécution.

(2) **Clauses contractuelles types de l'UE**. CA et les Entités affiliées CA jouant le rôle de Sous-traitant secondaire (tels que répertoriés dans l'Annexe 2) ont au préalable accepté les Clauses contractuelles types de l'UE pour une relation Responsable de traitement-Sous-traitant et pour le bénéfice du Client.

Dans l'éventualité où les Services seraient couverts par plus d'un mécanisme de transfert, le transfert des Données à caractère personnel du Client sera soumis à un mécanisme de transfert unique conformément à l'ordre de préséance ci-dessous : (i) autocertifications dans le cadre du Bouclier de protection des données ; (ii) clauses contractuelles types de l'UE.

6. SÉCURITÉ

6.1. Compte tenu de l'état de la technique, des coûts d'implémentation et de la nature, de la portée, du contexte et de la finalité du Traitement, ainsi que du degré de probabilité et de gravité variable des droits et des libertés des personnes, le Client et CA s'engagent à mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer que le degré de sécurité appliqué est adapté aux risques. CA assure l'application de mesures techniques et organisationnelles appropriées pour la protection de la sécurité, de la confidentialité et de l'intégrité des Données à caractère personnel, conformes aux exigences relatives aux Responsable du traitement au titre du RGPD, telles qu'indiquées dans l'Annexe 2, « Sécurité du traitement – RGPD Art. 32 ». CA s'engage à contrôler régulièrement le respect de ces garanties de protection. CA ne devra pas matériellement réduire le niveau de sécurité global des Services sur la période de prestation, conformément au Contrat ou au bon de commande associé.

6.2 Sur demande écrite du Client, et à une fréquence raisonnable, CA se doit de fournir une copie de ses certifications et audits tiers les plus récents, le cas échéant, ou toute synthèse desdits audits et certifications, concernant le Traitement des Données à caractère personnel du Client. Sur demande écrite raisonnable du Client, CA doit mettre à sa disposition toutes les informations nécessaires démontrant son respect du présent Addenda ; il doit permettre, pour toutes les demandes d'audit écrites de la part du Client ou d'un auditeur indépendant en rapport avec le Traitement des Données à caractère personnel, de vérifier qu'il applique des procédures raisonnables et adéquates au titre du présent Addenda, dans la mesure où le Client n'exerce pas ce droit plus d'une fois par an. Lesdites informations et les droits d'audit sont octroyés au titre du présent Article 6., dans la mesure où le Contrat n'octroie pas déjà de tels droits d'audit répondant aux exigences des Lois sur la protection des données en vigueur (y compris, le cas échéant, l'Article 28, § 3, point h) du RGPD). Toute information fournie par CA et/ou tout audit réalisé au titre de la présente section sont soumis aux obligations de confidentialité établies dans le Contrat.

6.3 CA doit apporter au Client une assistance raisonnable, le cas échéant, pour aider le Client à respecter son obligation de réalisation d'une analyse d'impact de la protection des données, au titre de l'Article 35 ou 36 du RGPD,

dans le cadre de l'utilisation des Services par le Client. CA fournira cette assistance au Client à sa demande raisonnable et dans la mesure où le Client n'accède pas aux informations pertinentes par un autre moyen et dans la mesure où lesdites informations sont à la disposition de CA. En outre, CA s'engage à offrir une assistance raisonnable au Client en coopération avec ou sur la base d'une consultation préalable avec l'Autorité de contrôle, dans l'exécution de ses tâches au titre du présent Article 6.3, dans la mesure exigée par le RGPD.

7. GESTION ET NOTIFICATION DES VIOLATIONS DE SÉCURITÉ

7.1 CA s'engage à informer rapidement le Client, sans retard injustifié, lorsqu'il a connaissance de toute destruction, perte, altération, divulgation non autorisée ou accès accidentel(le) ou illégal(e) relatif/ve aux Données à caractère personnel du Client qui sont transmises, conservées ou Traitées de quelque autre manière que ce soit par CA ou ses Sous-traitants secondaires (« **Violation de sécurité** »). CA fera tous les efforts raisonnablement nécessaires pour identifier la cause de ladite Violation de sécurité et engagera les actions suivantes rapidement et sans délai injustifié : (a) enquêter sur la Violation de sécurité et fournir au Client toutes les informations la concernant y compris, le cas échéant, les informations que le Sous-traitant est tenu de fournir au Responsable du traitement au titre de l'Article 33, § 3 du RGPD, dans la mesure où lesdites informations sont raisonnablement disponibles ; et (b) prendre des mesures raisonnables pour limiter l'impact et les dommages découlant de la Violation de sécurité, dans la mesure où une telle remédiation est sous le contrôle raisonnable de CA. Les obligations établies dans les présentes ne s'appliquent pas aux violations de sécurité causées par le Client ou ses Utilisateurs autorisés. Une notification est envoyée au Client conformément aux dispositions de l'Article 7.3 ci-dessous.

7.2 L'obligation de CA de signaler toute Violation de sécurité ou d'y répondre, au titre du présente article, n'est et ne sera pas considérée comme une reconnaissance par CA d'une éventuelle faute ou responsabilité concernant ladite Violation de sécurité.

7.3. Les notifications de Violation de sécurité, le cas échéant, seront transmises à un ou plusieurs interlocuteurs métier, techniques ou administratifs du Client, par tout moyen choisi par CA, y compris par courriel. Il est de la seule responsabilité du Client de s'assurer que les informations de contact dont disposent les services de support de CA sont à jour.

8. RENVOI ET SUPPRESSION DES DONNÉES CLIENT

8.1 CA est tenu de renvoyer et/ou de supprimer les Données à caractère personnel du Client conformément aux procédures CA, aux Lois sur la protection des données et/ou aux dispositions du Contrat.

8.2 À la demande du Client, CA est tenu de supprimer ou de renvoyer toutes les Données à caractère personnel du Client une fois la prestation des Services terminée en ce qui concerne le Traitement, et d'en supprimer toutes les copies existantes, conformément aux procédures établies dans l'Annexe 2 « Sécurité du traitement – RGPD Art. 32 », excepté lorsque les Lois sur la protection des données imposent de conserver ces Données à caractère personnel.

9. DISPOSITIONS COMPLÉMENTAIRES POUR LES DONNÉES À CARACTÈRE PERSONNEL DE L'UE

9.1 Les Clauses contractuelles types et les dispositions additionnelles établies dans le présent Article 9 s'appliquent au Traitement par CA des Données à caractère personnel dans le cadre de la prestation des Services.

9.1.1 Les Clauses contractuelles types s'appliquent uniquement aux Données à caractère personnel transférées depuis l'Espace économique européen (EEE) ou la Suisse vers une destination extérieure, que ce soit directement ou via un transfert ultérieur, à tout pays ou destinataire présentant les caractéristiques suivantes : (i) non reconnu par la Commission européenne comme offrant un niveau de protection adéquat

pour les Données à caractère personnel (tel que décrit dans les Lois sur la protection des données en vigueur) et (ii) non couvert par un cadre adéquat reconnu par les autorités ou les tribunaux compétents comme offrant un niveau de protection adéquat pour les Données à caractère personnel, y compris, sans s'y limiter, des règles d'entreprise contraignantes (REC) pour les Sous-traitants.

9.1.2 Les Clauses contractuelles types s'appliquent (i) à l'entité juridique ayant exécuté les Clauses contractuelles types en tant qu'Exportateur de données et (ii) à toutes les Entités affiliées (telles que définies dans le Contrat) du Client établies au sein de l'Espace économique européen (EEE) et en Suisse, et ayant acheté les Services par une commande au titre du Contrat. Dans le cadre des Clauses contractuelles types et du présent Article 9, le Client et ses Entités affiliées seront considérés comme étant les « Exportateurs de données ».

9.2 Le présent ATD et le Contrat constituent les instructions finales et exhaustives, fournies par l'Exportateur de données à l'Importateur de données, pour le Traitement des Données à caractère personnel. Toute instruction complémentaire ou alternative doit faire l'objet d'un accord séparé. Dans le cadre de la Clause 5, point a) des Clauses contractuelles types, les instructions suivantes sont fournies par l'Exportateur de données pour le Traitement des Données à caractère personnel : (a) respecter les dispositions du Contrat et les commandes réalisées au titre de celui-ci et (b) respecter toute autre instruction raisonnable fournie par le Client (ex., via un ticket d'assistance au Support), lorsque ladite instruction respecte les dispositions du Contrat.

9.3 Conformément à la Clause 5, point h) des Clauses contractuelles types, l'Exportateur de données reconnaît et accepte expressément que (a) des Entités affiliées CA puissent être désignées comme Sous-traitants secondaires ; et que (b) CA et des Entités affiliées CA, respectivement, puissent faire appel à des Sous-traitants secondaires tiers dans le cadre de la prestation des Services. L'Importateur de données doit mettre à disposition du Client une liste à jour des Sous-traitants secondaires pour les Services respectifs, indiquant l'identité desdits Sous-traitants secondaires, conformément à l'Article 5.5 du présent ATD, détaillant la Liste de sous-traitants secondaires fournie par CA.

9.4 Les parties acceptent que, dans les copies de contrats de Sous-traitants secondaires qui doivent être envoyées par l'Importateur de données à l'Exportateur de données, conformément à la Clause 5, point j) des Clauses contractuelles types, toutes les informations commerciales et les dispositions sans lien avec les Clauses contractuelles types ou leur équivalent soient supprimées en amont par l'Importateur de données ; et que lesdites copies soient transmises par l'Importateur de données à l'Exportateur de données, sur demande raisonnable de ce dernier.

9.5 Les parties acceptent que les audits décrits dans la Clause 5, point f), la Clause 11 et la Clause 12, § 2 des Clauses contractuelles types soient réalisés conformément aux spécifications suivantes : À la demande de l'Exportateur de données et sous réserve des obligations de confidentialité établies dans le Contrat, l'Importateur de données doit, dans un délai raisonnable suivant ladite demande, mettre à disposition de l'Exportateur de données (ou de l'auditeur tiers indépendant engagé par l'Exportateur de données, qui n'est pas un concurrent de CA) les informations relatives au respect par le Groupe CA des obligations établies dans le présent ATD, sous la forme de certifications et d'audit tiers réalisés tel que décrit dans le Contrat et/ou le Document de pratiques de sécurité, dans la mesure où CA rend ces informations généralement accessibles à ses clients. Le Client peut prendre contact avec l'Importateur de données dans le respect de l'article « Notifications » du Contrat, afin de demander un audit sur site des procédures applicables en matière de protection des Données à caractère personnel. Le Client doit rembourser à l'Importateur de données les frais relatifs à tout audit sur site, conformément aux tarifs horaires de services professionnels appliqués à ce moment-là par le Groupe CA, et qui doivent être indiqués à l'Exportateur de données à sa demande. Avant de réaliser un audit sur site, l'Exportateur et l'Importateur de données doivent s'accorder sur la périmètre, le calendrier et la durée de l'audit, ainsi que sur le tarif de remboursement des frais qui seront à la charge de l'Exportateur de données. Les tarifs de remboursement doivent être raisonnables et tenir compte des ressources réelles engagées par l'Importateur de données. L'Exportateur de données doit fournir rapidement à l'Importateur de données les informations relatives à tout problème de conformité détecté lors de cet audit.

9.6 Les parties acceptent que la certification de suppression des Données à caractère personnel décrite dans la Clause 12, § 1 soit fournie par l'Importateur de données à l'Exportateur de données uniquement à la demande ce dernier.

9.7 En cas de conflit ou de divergence entre le présent ATD et les Clauses contractuelles types, ces dernières prévalent. Si le présent document a été signé électroniquement par l'une ou l'autre des parties, la signature électronique aura la même valeur légale qu'une signature manuscrite.

10. PARTIES DU PRÉSENT ADDENDA

10.1 Limitation de responsabilité. La responsabilité des différentes parties et de leurs Entités affiliées, considérées comme un tout, découlant de ou au titre du présent ATD, et de tous les ATD signés entre les Entités affiliées autorisées et CA, que ce soit en vertu d'un contrat, de la responsabilité délictuelle ou de toute autre théorie de responsabilité, est soumise à l'article « Limitation de responsabilité » du Contrat régissant les Services en vigueur, et toute référence dans ledit article à la responsabilité d'une partie désigne la responsabilité collective de cette partie et de l'ensemble de ses Entités affiliées, au titre du Contrat et des différents ATD réunis. Pour éviter toute confusion, chaque référence à l'ATD dans le présent ATD désigne le présent ATD ainsi que ses Annexes, Calendriers et/ou Appendices.

10.2 Entités affiliées autorisées et relation contractuelle. En appliquant le présent ATD, le Client accepte de s'y conformer en son nom propre et, dans la mesure exigée par les Lois de protection des données en vigueur, au nom et pour le compte de ses Entités affiliées autorisées, si et dans la mesure où CA assure le Traitement de Données à caractère personnel pour lequel ces Entités affiliées autorisées sont qualifiées en tant que Responsable du traitement des données. Chaque Entité affiliée autorisée accepte d'être liée par les obligations établies dans le présent ATD et, dans la mesure applicable, dans le Contrat. Pour éviter toute confusion, l'Entité affiliée autorisée n'est et ne deviendra pas l'une des parties prenantes du Contrat, mais uniquement de l'ATD. Tout(e) accès et utilisation des Services par les Entités affiliées autorisées doit être conforme aux conditions générales du Contrat et toute violation de celles-ci par une Entité affiliée autorisée sera considérée comme une violation par le Client. Dans le cadre du présent ATD uniquement, le terme « Client » désigne à la fois le Client et ses Entités affiliées autorisées, excepté en cas de mention contraire spécifique.

10.2.1 Communication. Le Client qui est partie contractante du Contrat reste responsable de la coordination de l'ensemble des communications avec CA au titre du présent ATD et sera chargé de l'envoi et de la réception de toute communication en relation avec cet ATD, au nom de ses Entités affiliées autorisées.

10.2.2 Droits des Entités affiliées autorisées. Lorsqu'une Entité affiliée autorisée devient partie contractante de l'ATD avec CA, elle se voit octroyer, dans la mesure requise par les Lois sur la protection des données en vigueur, les droits et les voies de recours au titre du présent ATD, conformément aux conditions suivantes :

10.2.2.1 Excepté lorsque les Lois sur la protection des données en vigueur exigent que l'Entité affiliée autorisée exerce un droit ou une voie de recours contre CA au titre du présent ATD, en son nom propre, les parties acceptent (i) que seul le Client qui est partie contractante du Contrat exerce ledit droit ou ladite voie de recours au nom de l'Entité affiliée autorisée et (ii) que le Client qui est partie contractante du Contrat exerce lesdits droits au titre de l'ATD sans se séparer de l'Entité affiliée autorisée, mais de façon collective pour l'ensemble de ses Entités affiliées autorisées.

11. DÉFINITIONS

« Entités affiliées CA » : désigne toute entité contrôlée par CA, qui contrôle CA ou qui est en contrôle conjoint avec CA.

« CA » : désigne l'entité du Groupe CA, partie contractante du présent Addenda de Traitement des Données (ATD), le cas échéant.

« Groupe CA » : désigne la société CA et ses Entités affiliées impliquées dans le Traitement des Données à caractère personnel.

« **Entité affiliée autorisée** » : désigne toute Entité affiliée du Client qui (a) est soumise aux Lois sur la protection des données de l'Union européenne, de l'Espace économique européen et/ou de ses États membres, de la Suisse et/ou du Royaume-Uni et qui (b) est autorisée à utiliser les Services conformément aux dispositions du Contrat signé entre le Client et CA, mais qui n'a pas elle-même signé de Bon de commande avec CA et qui n'est pas « Client » dans le sens défini par le Contrat. Dans le cadre du présent ATD uniquement, le terme « Client » désigne à la fois le Client et ses Entités affiliées autorisées, excepté en cas de mention contraire spécifique. Pour éviter toute confusion, le terme « **Entité affiliée client »** désigne une entité que le Client détient directement ou indirectement en majorité, ou contrôle par un intérêt majoritaire.

Les termes **« Responsable du traitement », « Sous-traitant », « Personne concernée », « Commission », « État membre » et « Autorité de contrôle »** sont à interpréter dans le sens indiqué dans le Chapitre 1, Article 4 du RGPD, de même que les termes associés.

« Lois sur la protection des données » : désigne toutes les lois et réglementations en vigueur, y compris les lois et réglementations de l'Union européenne, de l'Espace économique européen et des États membres, notamment le RGPD (défini ci-dessous), applicables au Traitement des Données à caractère personnel au titre du Contrat.

« **RGPD » :** désigne le Règlement général sur la protection des données de l'Union européenne n° 2016/679 (*Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016*) relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

« Données à caractère personnel » : désigne toute information relative (i) à une personne physique identifiée ou identifiable et (ii) à une personne morale identifiée ou identifiable (lorsque lesdites informations sont protégées de façon similaires à des données à caractère personnel ou des informations d'identification personnelle, au titre des Lois sur la protection des données en vigueur), lorsque pour chaque personne physique (i) ou morale (ii), lesdites données sont des Données du Client (telles que définies dans le Contrat applicable) fournies en relation avec le Contrat.

« Traitement » : désigne toute opération ou ensemble d'opérations réalisées sur des Données à caractère personnel, que ce soit de façon automatisée ou non, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (ci-après désigné par les termes « Traiter » et « Traitement »).

« Violation de sécurité » : désigne une violation au sens défini dans l'Article 7 du présent Addenda.

« Document de pratiques de sécurité » : désigne le document spécifiant les pratiques de sécurité des informations en vigueur (ou la partie applicable, suivant les Services achetés par le Client auprès de CA), qui est régulièrement mis à jour et disponible à l'adresse https://www.ca.com/content/dam/ca/us/files/supportingpieces/ca-information-security-practices.pdf, ou intégré au Contrat entre CA et le Client, le cas échéant.

« Annexe de sécurité » : désigne les mesures de sécurité techniques et organisationnelles mises en œuvre par CA pour la protection des Données à caractère personnel, telles qu'indiquées dans l'Annexe 2 « Sécurité du traitement – RGPD Art. 32 ». En cas de conflit entre le Document des pratiques de sécurité de CA et les dispositions de l'Annexe de sécurité, ces dernières ont préséance en ce qui concerne les mesures de sécurité et la protection des Données à caractère personnel, conformément aux exigences du RGPD.

« Services » : désigne la prestation de services de maintenance et de support et/ou de services professionnels ou de conseil et/ou la fourniture de logiciels en tant que service (SaaS) et/ou de tout autre service fourni dans la cadre du Contrat, et dans lequel CA Traite les Données à caractère personnel du Client.

« Clauses contractuelles types » : désigne les dispositions en vigueur suite à la décision de la Commission européenne du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers et qui n'appliquent pas un degré de protection des données adéquat.

« Sous-traitant secondaire » : désigne un sous-traitant engagé par CA ou un membre du Groupe CA.

Liste des annexes et pièces jointes

Annexe 1 : Détails relatifs au traitement des données à caractère personnel du Client
Annexe 2 : Sécurité du traitement – RGPD Art. 32

EN FOI DE QUOI, le présent Addenda relatif au traitement des données (ATD) est intégré à et devient partie exécutoire du ou des Contrats existant entre le Client et CA, à compter de la Date d'effet spécifiée. Si le présent document a été signé électroniquement par l'une ou l'autre des parties, la signature électronique aura la même valeur légale qu'une signature manuscrite.

Accepté pour et au nom de CA	**Accepté pour et au nom du Client**
Entité CA :_____	**Entité client :**_____
Signature :_____	**Signature :**_____
Nom :_____	**Nom :**_____
Titre :_____	**Titre :**_____
Date :_____	**Date :**_____

ANNEXE 1 : DÉTAILS RELATIFS AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DU CLIENT

La présente Annexe 1 contient différents détails sur le Traitement des Données à caractère personnel du Client, dans le sens de l'Article 28, § 3 du RGPD (ou, le cas échéant, conformément aux dispositions des Lois sur la protection des données en vigueur).

Objet et durée du Traitement des Données à caractère personnel du Client

L'objet et la durée du Traitement des Données à caractère personnel du Client sont définis dans le Contrat principal et dans le présent Addenda.

Nature et finalité du Traitement des Données à caractère personnel du Client

Nature :

- ☒ Collecte
- ☒ Enregistrement
- ☐ Communication
- ☒ Suppression
- ☐ Modification
- ☐ Opposition
- ☒ Utilisation

Finalité :
Les Données à caractère personnel du Client sont utilisées aux fins de fournir des services de Support ou SaaS, comme indiqué dans le Contrat principal.

Types de Données à caractère personnel du Client à Traiter

Données à caractère personnel sur des personnes physique	☒
Données à caractère personnel sur des personnes morales	☒
Données sur les employés	☒
Autres Données à caractère personnel	☐

Catégories de personnes concernées par ces Données à caractère personnel Client

Catégories spéciales de Données à caractère personnel (Art. 9 RGPD)

Santé/Préférences sexuelles	☐
Appartenance à un syndicat	☐
Croyances religieuses ou philosophique	☐
Opinions politiques	☐
Origine ethnique ou raciale	☐

Obligations et droits du Client et des Entités affiliées Client

Les obligations et les droits du Client et de ses Entités affiliées sont définis dans le Contrat et dans le présent ATD, notamment dans les Annexes, Pièces jointes ou Calendriers des présentes, le cas échéant.

ANNEXE 2 – SECURITE DU TRAITEMENT – RGPD ART. 32

Préambule

Compte tenu de l'état de la technique, des coûts d'implémentation et de la nature, de la portée, du contexte et de la finalité du Traitement, ainsi que du degré de probabilité et de gravité variable des droits et des libertés des personnes, le Responsable du traitement et le Sous-traitant s'engagent à mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer que le degré de sécurité appliqué est adapté aux risques, y compris les éléments suivants, si approprié :

§ 1 Mesures techniques et organisationnelles mises en œuvre pour garantir un niveau de sécurité adéquat (SaaS et On Premise)

(1a) Mesures **de pseudonymisation/d'anonymisation** des Données à caractère personnel :
Les données conservées dans ce produit ne sont généralement pas de nature à exiger une pseudonymisation ou une anonymisation. Si nécessaire, le Client peut faire remonter le problème à CA. **On Premise :** Sans objet

(1b) Mesures de **chiffrement** des Données à caractère personnel :
CHIFFREMENT Toutes les données sont chiffrées en transit avec la technologie TLS, version 1.0, 1.1 (bientôt abandonnée) et 1.2 prise en charge actuellement. En outre, les Données à caractère personnel sont chiffrées sur tout serveur ou périphérique retiré des locaux de CA aux fins de sauvegarde ou de stockage hors site (le cas échéant). Des procédures de gestion de clés sont utilisées pour garantir la confidentialité, l'intégrité et la disponibilité des données de clé cryptographique. L'utilisation de produits de chiffrement est conforme aux restrictions et réglementations locales sur l'utilisation du chiffrement dans les juridictions pertinentes. Politique de chiffrement La politique de sécurité des données qui régit l'utilisation du chiffrement est documentée. La puissance du chiffrement des Données client en transmission y est définie. Gestion des clés de chiffrement Les procédures de gestion des clés cryptographiques sont documentées et automatisées. Les produits ou solutions nécessaires sont déployés pour préserver le cryptage des clés de chiffrement des données (ex., solutions logicielles, module de sécurité matérielle (HSM)). Utilisations du chiffrement La transmission des Données Client sur le réseau Internet public fait toujours appel à un canal chiffré. Le détail de ce chiffrement est documenté si la transmission est automatisée. Un personnel agréé et dédié est responsable du chiffrement/déchiffrement des données, lorsqu'il est manuel. Les Données Client doivent également être chiffrées lorsqu'elles transitent par un réseau, quel qu'il soit. Les transmissions VPN sont réalisées sur un canal chiffré. **On Premise :**

Le Responsable du traitement fournit au Sous-traitant les données de dossier de support sous forme chiffrée. La résolution des dossiers s'effectue dans un environnement sécurisé. Les données d'un dossier de support sont supprimées 30 jours après la clôture de ce dernier.

(1c) Mesures visant à garantir en permanence la **confidentialité** des Données à caractère personnel :
L'accès aux data centers au sein desquels sont conservées les Données Client est réservé aux équipes de production CA, dans le respect des Politiques de contrôle de l'accès aux informations de CA et de la Politique de séparation des fonctions de CA (CA applique le principe du privilège minimum et octroie un accès uniquement en fonction du rôle et du scénario d'utilisation métier). Les droits d'accès sont réexaminés régulièrement ou en cas de changement de rôle/de départ d'un employé. L'accès à l'environnement de stockage des Données Client est strictement contrôlé et surveillé. Le Client a la responsabilité de gérer l'accès à ses données d'abonnement et le cycle de vie de ses comptes. Les administrateurs d'abonnement client sont responsables de l'administration des utilisateurs et des politiques associées en matière de mot de passe au sein de l'application. Le Client est responsable de la gestion du cycle de vie de ses comptes. **On Premise :** Le travail est effectué dans un environnement sécurisé ; le transfert des données est également sécurisé. Les données d'un dossier de support sont supprimées une fois celui-ci clôturé.

(1d) Mesures visant à garantir en permanence l'**intégrité** des Données à caractère personnel :
INTÉGRITÉ DES DONNÉES Les politiques et procédures de CA Technologies ont été définies dans le but de garantir que toutes les données stockées, reçues, contrôlées ou accédées de quelque autre manière que ce soit, restent intactes et ne soient pas compromises. Des procédures d'inspection sont en place pour valider l'intégrité des données. Contrôle de la transmission des données Les processus et procédures de contrôle de la transmission des données visant à garantir leur intégrité sont documentés. Des sommes de contrôle et des comptages sont appliqués pour vérifier que les données transmises sont identiques aux données reçues. Contrôle des transactions de données Les contrôles visant à prévenir ou identifier les transactions dupliquées dans les messages financiers sont documentés. Les certificats numériques (ex., signature numérique, serveur à serveur) utilisés pour garantir l'intégrité des données durant la transmission respectent un processus et une procédure documentés. **On Premise :** Sans objet ; les données sont supprimées à la clôture du dossier de Support (voir section 2 a) à e)).

(1e) Mesures visant à garantir en permanence la **disponibilité des services et des systèmes de traitement :**
CONTRÔLE DE LA DISPONIBILITÉ - Protection anti-incendie et mesures en cas de panne de courant, pour les data centers chargés du traitement des données et notamment des sauvegardes Contrôles physiques CA Technologies a mis en place des contrôles efficaces pour se protéger contre les intrusions physiques par des personnes malveillantes ou non autorisées. Ces contrôles physiques couvrant l'ensemble des infrastructures sont documentés. Des restrictions d'accès complémentaires sont mises en œuvre pour les salles serveurs/informatiques/de télécommunications, par rapport aux locaux non spécialisés. Sauvegarde et stockage hors site CA Technologies a mis en place une politique de sauvegarde spécifique et des procédures associées pour réaliser la sauvegarde des données de façon planifiée et en temps opportun. Des contrôles efficaces sont en place pour protéger les données sauvegardées (sur et hors site). CA Technologies s'assure également que les Données Client sont transférées ou transportées en toute sécurité de et vers les sites de sauvegarde. D'autre part, CA Technologies réalise des tests périodiques afin de garantir que les données peuvent être récupérées correctement et en toute sécurité sur les périphériques de sauvegarde. Processus de sauvegarde Les procédures de sauvegarde et de stockage hors site sont documentées. Ces procédures incluent la capacité à restaurer entièrement les applications et les systèmes d'exploitation. Des tests sont effectués périodiquement pour confirmer que la restauration s'effectue correctement, à partir des supports de sauvegarde. La zone de stockage intermédiaire sur site fait l'objet de contrôles d'environnement éprouvés et documentés (ex., humidité, température). Destruction des supports de sauvegarde Des procédures sont en place pour expliquer au personnel les méthodes adéquates de destruction des supports de sauvegarde. La destruction des supports de sauvegarde par un tiers doit être accompagnée de procédures documentées (ex., certificat de destruction), qui valident la destruction. Stockage hors site Un plan de sécurité physique pour les infrastructures hors site est documenté. Des contrôles d'accès sont mis en place aux points d'entrée et dans les salles de stockage. L'accès aux infrastructures hors site est limité et un processus d'approbation est en place pour l'octroi des droits d'accès. La transmission électronique des données vers les infrastructures hors site s'effectue via un canal sécurisé. **On Premise :** Environnement d'atelier fermé ; sans objet. Les données restent auprès du Responsable du traitement.

(1f) Mesures visant à garantir en permanence la **résilience des services et des systèmes de traitement :**
SUPERVISION DE LA VULNERABILITÉ CA Technologies recueille et analyse en continu les informations relatives aux menaces et vulnérabilités existantes et nouvelles, aux attaques qui se sont produites dans d'autres établissements ou sociétés, et à l'efficacité des contrôles de sécurité existants. Les contrôles de supervision incluent des procédures et des politiques, le contrôle des virus et du code malveillant, la détection des intrusions et la surveillance des événements et des états. Le processus de journalisation associé offre un contrôle efficace permettant de mettre en lumière et d'étudier les événements de sécurité. Politique et procédure relatives aux vulnérabilités Des tests de pénétration/de vulnérabilité des réseaux internes/externes et/ou d'hôtes spécifiques sont réalisés. Ces tests sont généralement effectués par un intervenant externe réputé. Les environnements client sont couverts comme faisant partie du périmètre des tests. Tous les problèmes identifiés comme étant à haut risque sont résolus dans des délais appropriés. Solutions antivirus et anti-code malicieux Les équipements des serveurs, des postes de travail et des passerelles Internet sont mis à jour régulièrement avec les définitions antivirus les plus récentes. La procédure en place détecte toutes les mises à jour antivirus. Les outils antivirus sont configurés pour réaliser des analyses hebdomadaires, une détection des virus, une activité d'écriture sur fichier en temps réel et les mises à jour des fichiers de signature. Les ordinateurs portables et les utilisateurs distants sont couverts par la protection antivirus. Les procédures permettant de détecter et d'éliminer les applications non autorisées ou non supportées (ex., les programmes gratuits) sont documentées. Les événements d'alerte incluent les attributs suivants : Identifiant unique Date Heure Identifiant du niveau de priorité Adresse IP source Adresse IP de destination Description de l'événement Notification envoyée à l'équipe de sécurité État de l'événement Supervision des événements de sécurité Les événements de sécurité sont consignés dans des fichiers journaux, supervisés (utilisateurs appropriés) et pris en charge (action opportune documentée et exécutée). Les composants de réseau, les postes de travail, les applications et les outils de surveillance sont configurés pour permettre une supervision de l'activité utilisateur. Des responsabilités organisationnelles sont définies pour répondre à ces événements. Des outils de vérification de la configuration (ou d'autres journaux) sont utilisés pour consigner les modifications de configuration des systèmes critiques. Seuls les administrateurs sont autorisés à modifier un fichier journal. Le délai de conservation des différents journaux est défini et respecté.

(1g) Mesures visant à restaurer **la disponibilité et l'accès aux données à caractère personnel en cas d'incident technique physique :**
Voir ci-dessus, CONTRÔLE DE LA DISPONIBILITÉ RÉPONSE AUX INCIDENTS CA Technologies documente un plan d'action et les procédures associées dans l'éventualité d'un incident touchant à la sécurité des informations. Le plan de réponse aux incidents établit clairement les responsabilités du personnel et identifie les différentes parties prenantes à notifier. Le personnel chargé de la réponse aux incidents est correctement formé. L'exécution du plan de réponse aux incidents est testée périodiquement. Processus de réponse aux incidents La politique et les procédures de gestion des incidents touchant à la sécurité des informations sont documentés. La politique et/ou les procédures de gestion des incidents incluent les attributs suivants : • Une structure organisationnelle est définie. • Une équipe de réponse est identifiée. • La disponibilité de l'équipe de réponse est documentée. • Le calendrier de détection des incidents et de diffusion est documenté. • Le cycle de vie du processus de gestion des incidents est défini, notamment les différentes étapes suivantes : • Identification • Affectation d'un degré de sévérité à chaque incident • Communication • Résolution • Formation • Tests (fréquence de contrôle) • Reporting • Les incidents doivent être classifiés et hiérarchisés. • Les procédures de réponse aux incidents doivent inclure la notification client au responsable de la relation (prestation) ou tout autre interlocuteur indiqué dans le Contrat. Escalade/Notification Le processus de réponse aux incidents est exécuté dès que CA Technologies est informée de la survenue d'un incident (quelle que soit l'heure du jour ou de la nuit). **On Premise :** Applicable seulement partiellement ; les données sont supprimées à la clôture du dossier de support.

(1h) Mesures visant à effectuer **des analyses, des évaluations et des tests réguliers de l'efficacité des mesures techniques et organisationnelles :**
CONTRÔLE ORGANISATIONNEL PRODUCTION CA Technologies a documenté ses procédures opérationnelles IT afin de garantir un fonctionnement correct et sécurisé de ses ressources informatiques. Procédures opérationnelles et responsabilités. Les procédures opérationnelles sont documentées dans un manuel d'exploitation, puis exécutées avec succès.

Ce manuel d'exploitation inclut les éléments suivants :
- Planification des exigences
- Gestion des erreurs (ex., transport des données, impression, copies)
- Génération et traitement des sorties spéciales
- Maintenance et dépannage des systèmes
- Procédures documentées pour gérer les SLA/KPI et structure de reporting pour les escalades

Des audits de sécurité internes sont régulièrement réalisés chez le Responsable du traitement, notamment par le Délégué à la protection des données (extérieur).

§ 2 Délégués à la protection des données

Nom :	Coordonnées du contact :
Bonnie Yeomans	CA, Inc. 520 Madison Avenue New York, NY 10022, États-Unis Assistant General Counsel and Chief Privacy Officer
Yasmin Brook	CA Deutschland GmbH Marienburgstr. 35 64297 Darmstadt Allemagne Senior Counsel and Global Field Privacy Officer

§ 3 Une liste à jour des sous-traitants secondaires est disponible à l'adresse https://support.ca.com/us/product-content/admin-content/subprocessor-list.html

§ 4 Entités CA proposant des services de maintenance et de support dans le cadre du Contrat principal

Entités CA		
Nom	**Coordonnées du contact**	**Lieu**
CA Argentina S.A.	Av. Alicia Moreau de Justo 400, Piso 4, Buenos Aires, Argentina C.P. C1107AAH	Argentine
CA (Pacific) Pty Ltd	6 Eden Park Drive, North Ryde, New South Wales 2113, Australia	Australie
CA Software Österreich GmbH	EURO PLAZA, Am Europlatz 5, Gebäude C, 1120 Vienna	Autriche
CA Belgium SA	Da Vincilaan 11, Building Figueras, B-1935 Zaventem - Belgium	Belgique
CA Programas de Computador Participacoas Servicos Ltda	Avenida Dr Chucri Zaidan, 1240 – 26º e 27º andares, Golden Tower, Vila São Francisco, CEP 04711-130 - São Paulo/SP, Brasil - CNPJ/MF 08.469.511/0001-69	Brésil
CA Canada Company	2700 Matheson Blvd East, Suite 800E, Mississauga, Ontario, L4W 5M2, Canada	Canada
CA de Chile, S.A.S.	Avenida Providencia, 1760, piso 15, Edificio Palladio, oficina 1501, Providencia, Chile, inscrita bajo el Registro RUT 96.724.010-9	Chili
CA CZ, s.r.o	Praha 4 - Chodov, V Parku 2316/12, PSČ 148 00	République tchèque
CA Software ApS	Borupvang 5B, DK - 2750, Ballerup, Denmark	Danemark
CA Limited (formerly CA Plc and fomerly Computer Associates Plc)	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Angleterre
CA Technology R&D Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Angleterre
Computer Associates Holding Ltd.	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Angleterre
Computer Associates UK Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Angleterre
CA SAS	Tour Opus 12, 4 Place des Pyramides, La Défense 9, 92914 Paris La Défense Cedex, France,	France
CA Computer Associates European Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Allemagne
CA Computer Associates Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Allemagne

CA Computer Associates Technology GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Allemagne
CA Deutschland GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Allemagne
CA (India) Technologies Private Limited	Ground Floor, Vibgyor Tower, Plot C-62, G-Block, Bandra Kurla Complex, Bandra (East), Mumbai - 400 051	Inde
CA Software Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israël
CA Technologies R&D Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israël
CA S.r.l.	Via Francesco Sforza 3, 20080 Milano Tre, Basiglio (MI)	Italie
CA Japan, Ltd.	JA Kyosai Bldg., 2-7-9 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093, Japan	Japon
CA Services, S.A. DE C.V.	Miguel de Cervantes Saavedra 193 piso 5, Col. Granada, 11500, Ciudad de México, México; inscrita bajo el registro CSM 9505032G1	Mexique
CA Software de Mexico, S.A. de C.V	Voir ci-dessus	Mexique
CA Europe Holding B.V.	Orteliuslaan 1001, 3528 BE, Utrecht, Netherlands	Pays-Bas
CA software BV	Voir ci-dessus	Pays-Bas
CA Software Holding BV	Voir ci-dessus	Pays-Bas
CA IT Management Solutions Spain, S.L.U.	WTC Almeda Park, Edificio 2, planta 4, Plaça de la Pau s/n, 08940 Cornellá de Llobregat	Espagne