ADDENDUM SUL TRATTAMENTO DEI DATI - GDPR

Il presente Addendum sul Trattamento dei Dati Personali ("**DPA**" o "Addendum") è parte integrante dell'accordo o degli accordi esistenti tra il Cliente e CA, e/o di altro accordo in forma scritta o elettronica tra CA e il Cliente per l'acquisto di Servizi forniti da CA (il "**Contratto**"), e contiene gli accordi tra le parti in merito al Trattamento dei Dati Personali del Cliente, in conformità ai requisiti previsti dalla Normativa applicabile alla Protezione dei Dati. La Data di Efficacia del presente DPA è quella di apposizione dell'ultima firma di una parte in calce al presente documento. Salvo diversa indicazione, a tutti i termini con iniziale maiuscola utilizzati nel presente DPA si applicheranno le definizioni indicate nel Contratto.

1. TERMINI GENERALI

Il presente DPA si applica al Trattamento dei Dati Personali, nell'ambito del Regolamento UE in materia di protezione dei dati personali 2016/679 (come ulteriormente definito all'Articolo 11, e di seguito "**GDPR**"), da parte di CA per conto del Cliente. A partire dal 25 maggio 2018, CA effettuerà il Trattamento dei Dati Personali in conformità ai requisiti previsti dal GDPR direttamente applicabili alla fornitura dei propri Servizi. Il presente DPA non contiene limitazioni o riduce gli obblighi di protezione dei Dati Personali in relazione al Trattamento dei Dati dei Clienti precedentemente negoziati dal Cliente nel Contratto (compresi eventuali addendum al Contratto per il Trattamento dei Dati Personali).

Il Cliente sottoscrive il presente Addendum in nome e per conto proprio e, nella misura richiesta dalla Normativa applicabile alla Protezione dei Dati, in nome e per conto delle proprie Affiliate Autorizzate, se e nella misura in cui CA effettua il Trattamento di Dati Personali rispetto ai quali tali Affiliate Autorizzate sono Titolari del trattamento. Salvo diversa indicazione, unicamente nell'ambito del presente DPA, il termine "Cliente" includerà il Cliente e le Affiliate Autorizzate,.

Nell'ambito della fornitura dei Servizi al Cliente ai sensi del Contratto, CA potrà effettuare il Trattamento di Dati Personali per conto del Cliente. CA si impegna a rispettare le disposizioni nel Trattamento dei Dati Personali del Cliente nell'ambito della fornitura dei Servizi. Se non diversamente definito nel relativo articolo, tutte le definizioni applicabili al presente DPA sono state consolidate nell'Articolo 11, intitolato "Definizioni".

2. TRATTAMENTO DEI DATI PERSONALI

2.1 Le parti concordano che, per quanto riguarda il Trattamento dei Dati Personali, il Cliente è il Titolare del Trattamento e CA è Responsabile del Trattamento; e inoltre che CA o i membri del Gruppo CA nomineranno eventuali Sub-Responsabili del Trattamento in conformità ai requisiti previsti nell'Articolo 5 che segue intitolato, "Sub-Responsabili del Trattamento".

2.2 Il Cliente dovrà, al momento dell'utilizzo o della ricezione dei Servizi, procedere al Trattamento dei Dati Personali in conformità con i requisiti della Normativa applicabile alla Protezione dei Dati e garantirà che le proprie istruzioni per il Trattamento siano conformi con la Normativa applicabile alla Protezione dei Dati. Il Cliente è l'unico responsabile dell'accuratezza, della qualità e della liceità dei Dati Personali, nonché delle modalità della loro acquisizione.

2.3 CA procederà al Trattamento dei Dati Personali in conformità con la Normativa applicabile alla Protezione dei Dati e i requisiti del GDPR direttamente applicabili alla fornitura dei propri Servizi. CA effettuerà il Trattamento dei Dati Personali solo per conto del Cliente e in conformità con le istruzioni documentate di quest'ultimo, trattando tali Dati Personali come Informazioni riservate. Il Cliente indica a CA di effettuare il Trattamento dei Dati Personali per i seguenti scopi: (i) Trattamento in conformità con il Contratto e gli ordini applicabili; (ii) Trattamento per conformarsi

ad altre ragionevoli istruzioni fornite dal Cliente (ad esempio, tramite un ticket di assistenza), laddove tali istruzioni siano coerenti con i termini del Contratto e (iii) Trattamento di Dati Personali richiesto dalla legge applicabile a cui CA o un'Affiliata CA sia soggetta inclusa, a titolo esemplificativo ma non esaustivo, la Normativa applicabile alla Protezione dei Dati, nel qual caso CA o l'Affiliata CA dovrà, nella misura consentita dalla legge applicabile, informare il Cliente di tale Trattamento dei Dati Personali richiesto dalla legge.

2.4. Come richiesto dall'articolo 28, paragrafo 3, del GDPR, l'oggetto e la durata del Trattamento, la natura e la finalità del Trattamento, i tipi di Dati Personali e le categorie di Interessati sono riportati nell'allegato I al presente Addendum DPA (rubricato "Allegato 1: Dettagli sul Trattamento dei Dati Personali del cliente"). L'oggetto del Trattamento dei Dati Personali da parte di CA è la performance dei Servizi forniti ai sensi del Contratto. Previa comunicazione scritta, il Cliente può richiedere le opportune modifiche all'Allegato 1 che ritenga ragionevolmente necessarie per soddisfare i requisiti dell'Articolo 28 (3) del GDPR; CA rivedrà tali modifiche. Nulla di quanto contenuto nell'Allegato 1 conferisce alcun diritto o impone alcun obbligo a qualsiasi parte del presente Addendum.

3. DIRITTI DEGLI INTERESSATI

3.1. Nella misura consentita dalla legge, CA dovrà informare tempestivamente il Cliente qualora riceva da un Interessato una richiesta relativa all'esercizio di diritto di accesso, diritto di rettifica, limitazione del Trattamento, cancellazione ("diritto all'oblio"), portabilità dei Dati Personali, opposizione al Trattamento, o in relazione al suo diritto a non essere soggetto a un processo decisionale individuale automatizzato ("**Richiesta dell'Interessato**"). Tenendo conto della natura del Trattamento, CA assisterà il Cliente con adeguate misure tecniche e organizzative, per quanto possibile, per l'adempimento dell'obbligo del Cliente a rispondere a una Richiesta dell'interessato ai sensi del Capitolo III del GDPR. Fatto salvo quanto richiesto dalla legge applicabile, CA non risponderà a tale Richiesta dell'Interessato senza il preventivo consenso scritto del Cliente, salvo per confermare che la richiesta sia relativa al Cliente medesimo.

3.2 Inoltre, nella misura in cui il Cliente, nell'ambito del proprio utilizzo dei Servizi, non sia in grado di rispondere alla Richiesta di un Interessato, CA sarà tenuta, su richiesta del Cliente medesimo, a fare quanto commercialmente ragionevole per supportare il Cliente nel rispondere alla Richiesta, nella misura in cui legalmente autorizzata a farlo e a condizione che la Richiesta medesima sia conforme con la Normativa applicabile alla Protezione dei Dati. Eventuali costi collegati a tale assistenza saranno a carico del Cliente, nella misura consentita dalla legge.

4. PERSONALE

4.1 CA dovrà garantire che il proprio personale impegnato nel Trattamento di Dati Personali sia informato della natura riservata di questi, abbia ricevuto un'adeguata formazione sulle proprie responsabilità e sia vincolato da obblighi di riservatezza; e che tali obblighi sopravvivano alla cessazione del rapporto di lavoro di tali soggetti con CA .

4.2 CA adotterà le misure commercialmente adeguate a garantire l'affidabilità di qualsiasi membro del personale CA impegnato nel Trattamento di Dati Personali.

4.3 CA dovrà garantire che l'accesso del Gruppo CA ai Dati Personali sia limitato al personale che necessiti di tale accesso per l'esecuzione del Contratto.

4.4 Responsabile della protezione dei dati. I membri del gruppo CA hanno nominato un responsabile della protezione dei dati laddove tale nomina sia richiesta dalla Normativa applicabile alla Protezione dei Dati. Il soggetto nominato può essere raggiunto all'indirizzo datatransfers@ca.com.

5. SUB-RESPONSABILI DEL TRATTAMENTO

5.1 Il Cliente riconosce e accetta che (a) le Affiliate CA possano fungere da Sub-Responsabili del Trattamento; e inoltre che (b) CA e le Affiliate CA, rispettivamente, possano incaricare terzi come Sub-Responsabili del Trattamento in relazione alla fornitura dei Servizi. A tali Sub-Responsabili del Trattamento sarà consentito ottenere i Dati Personali solo per fornire i servizi per i quali CA li abbia incaricati; non è consentito loro utilizzare i Dati Personali per qualsiasi altra finalità.

5.2 CA è responsabile degli atti e delle omissioni dei propri Sub-Responsabili del Trattamento nella stessa misura in cui sarebbe direttamente responsabile dell'esecuzione dei servizi da parte di ciascun Sub-Responsabile del Trattamento ai sensi del presente DPA, salvo per quanto diversamente stabilito nel Contratto.

5.3 CA o l'Affiliata CA ha stipulato un accordo scritto con ciascun Sub-Responsabile del Trattamento che prevede obblighi di protezione dei Dati Personali non meno restrittivi delle disposizioni del presente Addendum in relazione alla protezione dei Dati Personali e che soddisfano i requisiti dell'Articolo 28 (3) del GDPR, o disposizioni equivalenti di qualsiasi altra Legge in materia di protezione dei dati, nella misura applicabile alla natura dei Servizi forniti dal Sub-Responsabile del Trattamento in questione.

5.4 Il Cliente autorizza CA e ciascuna Affiliata CA a nominare Sub-Responsabili del Trattamento in conformità con il presente Articolo 5. L'elenco dei Sub-Responsabili del Trattamento utilizzati da CA in connessione con la fornitura dei Servizi è riportato nell'Allegato 2 e include identità e paese di ubicazione di tutti i Sub-Responsabili del Trattamento ("**Elenco dei Sub-Responsabili del Trattamento**"). Nel caso in cui CA apporti modifiche o aggiunte a tale elenco, l'Elenco aggiornato sarà reso disponibile al Cliente all'indirizzo: https://support.ca.com/us/product-content/admin-content/subprocessor-list.html, fornendo così al Cliente medesimo la possibilità di opporsi alle modifiche apportate (come previsto dall'Articolo 5.5 di seguito).

5.5. Il Cliente può opporsi all'utilizzo da parte di CA di un nuovo Sub-Responsabile del Trattamento dandone prontamente comunicazione in forma scritta a CA entro dieci (10) giorni lavorativi dalla data in cui eventuali aggiornamenti vengano apportati da CA all'Elenco dei Sub-Responsabili del Trattamento. Nel caso di tale opposizione da parte del Cliente, CA adotterà le misure commercialmente ragionevoli per risolvere le obiezioni sollevate dal Cliente e fornirgli ragionevole spiegazione scritta delle misure medesime.

5.6. Trasferimenti di Dati Personali. CA trasferirà i Dati Personali del Cliente solo mediante modalità lecite, in conformità con la Normativa applicabile alla Protezione dei Dati; inoltre, i Dati Personali saranno trasferiti in conformità con l'informativa di CA e le disposizioni reperibili qui https://www.ca.com/us/legal/privacy/data-transfers.html. Unicamente per la fornitura di Servizi al Cliente ai sensi del Contratto e in conformità con il presente Articolo 5.6, il Cliente autorizza CA a effettuare trasferimenti di routine dei Dati Personali all'entità locale del Gruppo CA e/o ai Sub-Responsabili del Trattamento autorizzati di CA . Fatto salvo quanto sopra, nel caso in cui i Dati Personali del Cliente siano trasferiti dall'Unione Europea, dallo Spazio Economico Europeo e/o dai relativi stati membri, dalla Svizzera e dal Regno Unito verso paesi che non garantiscono un livello adeguato di protezione dei Dati Personali ai sensi della Normativa applicabile alla Protezione dei Dati dei suddetti territori ("**Trasferimenti limitati**"), CA si atterrà alle disposizioni dell'Articolo 5.6 (a) in relazione a tali Trasferimenti limitati.

(a) **Meccanismi di trasferimento per i trasferimenti limitati.** CA rende disponibili i meccanismi di trasferimento indicati di seguito che si applicano, in relazione ai Trasferimenti limitati ai sensi del presente DPA, nella misura in cui tali trasferimenti siano soggetti alla Normativa applicabile alla Protezione dei Dati:

(1) **Autocertificazioni Privacy Shield**. CA ha certificato la propria conformità al programma Privacy Shield UE-USA. CA manterrà tale certificazione fino a quando conservi Dati Personali all'interno del SEE. Nel caso in cui autorità o tribunali UE stabiliscano che il Privacy Shield non costituisce un quadro di riferimento adeguato per i trasferimenti, le parti predisporranno senza ritardo Clausole contrattuali standard dell'UE approvate (Responsabili del trattamento), che dovranno essere integrate nel presente documento post-redazione.

(2) **Clausole contrattuali standard UE**. CA e le Affiliate CA che agiscano come Sub-Responsabili del Trattamento (come indicati nell'Allegato 2) hanno stipulato in precedenza Clausole contrattuali standard UE in relazione a un rapporto tra titolare del trattamento e responsabile del trattamento e a beneficio del Cliente.

Nel caso in cui ai Servizi si applichino più meccanismi di trasferimento, il trasferimento dei Dati Personali del Cliente sarà soggetto a un meccanismo unico, in conformità con il seguente ordine di priorità: (i) autocertificazioni Privacy Shield; (ii) Clausole contrattuali standard dell'UE.

6. SICUREZZA

6.1. Tenendo conto dello stato dell'arte, dei costi di attuazione e della natura, dell'ambito, del contesto e delle finalità del Trattamento nonché del rischio, di probabilità e gravità variabili, per i diritti e le libertà delle persone fisiche, il cliente e CA adotteranno misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio. CA manterrà misure tecniche e organizzative adeguate alla protezione della sicurezza, della riservatezza e dell'integrità dei Dati Personali, che soddisfino i requisiti per un Responsabile del trattamento ai sensi del GDPR, come stabilito nell'Allegato 2 "Sicurezza del trattamento - GDPR art. 32". CA monitora regolarmente la conformità con tali misure di sicurezza. CA non ridurrà materialmente la sicurezza complessiva dei Servizi durante il relativo periodo di fornitura da parte sua in conformità con il Contratto applicabile o il modulo d'ordine relativo.

6.2 Su richiesta scritta del Cliente e con periodicità ragionevole, CA fornirà una copia degli audit o delle certificazioni, a seconda dei casi, svolti più di recente da terzi e aventi a oggetto CA medesima, o di qualsiasi sintesi dei medesimi, relativamente al Trattamento dei Dati Personali del Cliente, che CA metta generalmente a disposizione alla clientela, all'atto di tale richiesta. CA metterà a disposizione del Cliente, previa ragionevole richiesta scritta, le informazioni necessarie a dimostrare la conformità al presente Addendum e dovrà consentire richieste scritte di audit da parte del Cliente o di un revisore indipendente in relazione al Trattamento dei Dati Personali, per verificare che CA adotti procedure ragionevoli in conformità al presente Addendum, a condizione che il Cliente non eserciti tale diritto più di una volta all'anno. Tali informazioni e diritti di audit vengono resi disponibili ai sensi del presente Articolo 6.2 nella misura in cui il Contratto non preveda diritti di questo tipo che soddisfino i requisiti della Normativa applicabile alla Protezione dei Dati (incluso, ove applicabile, l'articolo 28 (3) (h) del GDPR). Qualsiasi informazione fornita da CA e/o audit eseguito in conformità con il presente articolo è soggetto agli obblighi di riservatezza stabiliti nel Contratto.

6.3 CA fornirà al Cliente ragionevole assistenza come necessaria per soddisfare l'obbligo a carico di questi di eseguire una valutazione dell'impatto della protezione dei dati ai sensi dell'articolo 35 o 36 del GDPR, per quanto concerne l'utilizzo dei Servizi da parte del Cliente. CA fornirà tale assistenza dietro ragionevole richiesta del Cliente, nella misura in cui questi non abbia altrimenti accesso alle informazioni pertinenti e nella misura in cui tali informazioni siano disponibili a CA . Inoltre, CA fornirà ragionevole assistenza al Cliente nella cooperazione o preventiva consultazione con l'Autorità di Vigilanza per quanto concerne l'esecuzione dei suoi compiti in relazione al presente Articolo 6.3, nella misura richiesta ai sensi del GDPR.

7. GESTIONE E NOTIFICA DELLE VIOLAZIONI DELLA SICUREZZA

7.1 CA informerà tempestivamente il Cliente, senza indebito ritardo, qualora venga a conoscenza di qualsiasi distruzione, perdita, alterazione, divulgazione non autorizzata o illecita di Dati Personali del Cliente che siano trasmessi, archiviati o altrimenti oggetto di trattamento da parte di CA o di suoi Sub-Responsabili del Trattamento ("**Violazione della sicurezza**"). CA compirà ogni ragionevole sforzo per identificare la causa di tale Violazione della sicurezza e dovrà, tempestivamente e senza indebito ritardo: (a) indagare sulla Violazione della sicurezza e fornire

al Cliente informazioni al riguardo incluse, se del caso, quelle dovute da un Responsabile del Trattamento a un Titolare del Trattamento ai sensi dell'Articolo 33, paragrafo 3, del GDPR, nella misura in cui siano ragionevolmente disponibili; e (b) adottare misure adeguate a mitigare gli effetti della Violazione e ridurre al minimo eventuali danni da essa derivanti, nella misura in cui tale mitigazione rientri nel ragionevole controllo di CA . Gli obblighi qui previsti non si applicano alle violazioni causate dal Cliente o dai suoi Utenti autorizzati. La notifica verrà trasmessa al Cliente in conformità con l'Articolo 7.3 di seguito.

7.2 L'obbligo di CA a segnalare una Violazione della sicurezza o a prendere provvedimenti al riguardo ai sensi del presente Articolo non costituirà e non potrà essere interpretato come ammissione da parte di CA di colpa o responsabilità in relazione alla Violazione della sicurezza.

7.3. L'eventuale notifica o le eventuali notifiche relative a Violazioni della sicurezza verranno trasmesse a uno o più contatti commerciali, tecnici o amministrativi del Cliente con qualsiasi mezzo selezionato da CA, anche via e-mail. È responsabilità esclusiva del Cliente assicurarsi sempre di conservare la correttezza dei propri recapiti all'interno dei sistemi di assistenza di CA .

8. RESTITUZIONE ED ELIMINAZIONE DEI DATI DEL CLIENTE

8.1 CA restituirà o eliminerà i Dati Personali del Cliente in conformità con le proprie procedure e con la Normativa applicabile alla Protezione dei Dati e/o in conformità con le disposizioni del Contratto.

8.2 Su richiesta del Cliente, CA eliminerà o restituirà tutti i Dati Personali al Cliente al termine della fornitura dei Servizi in connessione con il Trattamento, eliminandone eventuali copie, in conformità con le procedure di cui all'Allegato 2 "Sicurezza del trattamento - GDPR art. 32", salvo la Normativa applicabile per la Protezione dei Dati Personali non richieda la conservazione dei Dati Personali.

9. TERMINI AGGIUNTIVI APPLICABILI AI DATI PERSONALI NELL'UE

9.1 Le Clausole contrattuali standard e le clausole aggiuntive del presente Articolo 9 si applicano al Trattamento dei Dati Personali da parte di CA nell'ambito della fornitura dei Servizi.

> **9.1.1** Le Clausole contrattuali standard si applicano solo ai Dati Personali trasferiti dallo Spazio economico europeo (SEE) o dalla Svizzera al di fuori del SEE o della Svizzera, direttamente o tramite trasferimento successivo, verso qualsiasi paese o destinatario:(i) che secondo la Commissione europea non fornisca un livello adeguato di protezione dei Dati Personali (come descritto ai sensi della Normativa applicabile per la Protezione dei Dati Personali e (ii) non sia oggetto di un quadro di protezione adeguato che, secondo autorità o tribunali competenti, fornisca un livello adeguato di protezione dei Dati Personali incluse, a titolo esemplificativo ma non esaustivo, le Regole aziendali vincolanti per i Responsabili del Trattamento.
>
> **9.1.2** Le Clausole contrattuali standard si applicano (i) alla persona giuridica che ha sottoscritto le Clausole contrattuali standard come Esportatore di Dati e inoltre (ii) a tutte le Affiliate del Cliente (come definite nel Contratto) con sede all'interno dello Spazio Economico Europeo (SEE) e in Svizzea che abbiano acquistato servizi in base a un ordine ai sensi del Contratto. Ai fini delle Clausole contrattuali standard e del presente Articolo 9, il Cliente e le Affiliate del Cliente sono considerati "Esportatori di Dati".

9.2 Il presente DPA e il Contratto rappresentano le istruzioni complete e finali dell'Esportatore di Dati all'Importatore di Dati per il Trattamento dei Dati Personali. Eventuali istruzioni aggiuntive o alternative devono essere concordate separatamente. Ai fini della Clausola 5 (a) delle Clausole contrattuali standard, quanto segue è considerato un'istruzione dell'Esportatore di Dati per il Trattamento dei Dati Personali: (a) la conformità con il Contratto e gli

ordini applicabili e (b) la conformità con le altre ragionevoli istruzioni fornite dal Cliente (ad esempio, tramite un ticket di assistenza), laddove siano coerenti con i termini del Contratto.

9.3 In conformità con la Clausola 5(h) delle Clausole contrattuali standard, l'Esportatore di Dati riconosce e accetta espressamente che le Affiliate CA possano fungere da Sub-Responsabili del Trattamento; e inoltre che (b) CA e le Affiliate CA, rispettivamente, possano incaricare terzi come Sub-Responsabili del Trattamento in relazione alla fornitura dei Servizi. L'Importatore di Dati metterà a disposizione del Cliente un elenco aggiornato dei Sub-Responsabili del Trattamento per i rispettivi Servizi, indicando i nomi di tali soggetti in conformità all'Articolo 5.5 del presente DPA, che specifica ulteriori dettagli sulla fornitura da parte di CA dell'elenco medesimo.

9.4 Le parti concordano che, nelle copie dei contratti relativi ai Sub-Responsabili del Trattamento che devono essere trasmesse dall'Importatore di Dati all'Esportatore di Dati ai sensi della Clausola 5 (j) delle Clausole contrattuali standard, possono venire preventivamente rimosse dall'Importatore dei Dati tutte le informazioni commerciali, o le disposizioni non correlate allo Clausole o loro equivalenti; e che tali copie saranno fornite dall'Importatore di Dati solo dietro ragionevole richiesta dell'Esportatore di Dati.

9.5 Le parti concordano che gli audit descritti nella Clausola 5 (f), nella Clausola 11 e nella Clausola 12 (2) delle Clausole contrattuali standard debbano essere eseguiti secondo le seguenti specifiche: Su richiesta dell'Esportatore di Dati e in conformità agli obblighi di riservatezza stabiliti nel Contratto, l'Importatore di Dati, entro un termine ragionevole dopo la richiesta, metterà a disposizione dell'Esportatore di Dati (o di un suo revisore indipendente che non sia un concorrente di CA) informazioni relative alla conformità del gruppo CA rispetto agli obblighi previsti nel presente DPA, sotto forma di certificazioni e audit di terzi eseguiti secondo le modalità descritte nel Contratto e/o nel Documento sulle pratiche di sicurezza, nella misura in cui CA li renda generalmente disponibili ai propri clienti. Il Cliente può contattare l'Importatore di Dati in conformità con l'Articolo rubricato "Comunicazioni" del Contratto per richiedere un audit in loco delle procedure relative alla protezione dei Dati Personali. Il Cliente rimborserà l'Importatore dei Dati in relazione a qualsiasi periodo di tempo dedicato all'esecuzione di tali audit sul posto, alle tariffe previste per i servizi professionali del Gruppo CA in quel momento in vigore, che saranno messe a disposizione dell'Esportatore di Dati su richiesta. Prima dell'inizio di tale audit sul posto, l'Esportatore di Dati e l'Importatore di Dati concorderanno reciprocamente l'ambito, i tempi e la durata dell'audit, oltre alla quota del rimborso a carico dell'Esportatore di Dati. Tutte le quote dovranno essere ragionevoli, tenendo conto delle risorse allocate dall'Importatore di Dati. L'Esportatore di Dati dovrà immediatamente informare l'Importatore di Dati di eventuali non conformità rilevate nel corso di un audit.

9.6 Le parti concordano che la certificazione relativa alla cancellazione dei Dati Personali di cui alla Clausola 12 (1) sarà fornita dall'Importatore di Dati all'Esportatore solo dietro richiesta di questi.

9.7 In caso di conflitto o di incoerenza tra il presente DPA e le Clausole contrattuali standard, queste ultime si intenderanno prevalenti. Qualora il presente documento sia stato firmato elettronicamente da entrambe le parti, tale firma avrà lo stesso effetto legale di una firma autografa.

10. PARTI DI QUESTO DPA

10.1 Limitazione di responsabilità. La responsabilità di ciascuna delle parti e di tutte le Affiliate, considerate nel complesso, derivante dal presente DPA o a esso correlata, e in relazione a tutti i DPA tra Affiliate Autorizzate e CA, a titolo di responsabilità contrattuale, civile o altrimenti, è soggetta all'articolo "Limitazione di responsabilità" del Contratto che disciplina i Servizi applicabili, e qualsiasi riferimento in tale articolo alla responsabilità di una parte indica la responsabilità aggregata di tale parte e di tutte le sue Affiliate ai sensi del Contratto e di tutti i DPA nel loro complesso. Per chiarezza, ogni riferimento al DPA in questo DPA indica questo DPA, inclusi i suoi Allegati e/o Appendici.

10.2 Affiliate Autorizzate e rapporto contrattuale. Sottoscrivendo il presente DPA, il Cliente ne diventa parte per conto proprio e, nella misura richiesta dalla Normativa applicabile alla Protezione dei Dati, in nome e per conto delle proprie Affiliate Autorizzate, se e nella misura in cui CA effettui il Trattamento dei Dati Personali per i quali tali entità si qualificano come Titolari del trattamento. Ogni Affiliata Autorizzata accetta di essere vincolata dagli obblighi previsti dal presente DPA e, nella misura applicabile, dal Contratto. Per chiarezza, un'Affiliata Autorizzata non è e non diventa parte del Contratto, ma è unicamente parte del DPA. L'accesso ai Servizi e il loro utilizzo da parte delle Affiliate Autorizzate devono rispettare i termini e le condizioni del Contratto, qualsiasi violazione dei quali da parte di un'Affiliata Autorizzata sarà considerata violazione da parte del Cliente. Solo per gli scopi del presente DPA, il termine "Cliente" includerà il Cliente e le Affiliate Autorizzate, se non diversamente indicato nel presente documento.

10.2.1 Comunicazione. Il Cliente che costituisce la parte contraente del Contratto rimarrà responsabile del coordinamento di tutte le comunicazioni con CA ai sensi del presente DPA e avrà diritto a effettuare e ricevere qualsiasi comunicazione in relazione al presente DPA per conto delle proprie Affiliate Autorizzate.

10.2.2 Diritti delle Affiliate Autorizzate. Laddove un'Affiliata Autorizzata diventi parte del DPA insieme a CA, nella misura richiesta dalla Normativa applicabile alla Protezione dei Dati avrà il diritto a esercitare i diritti e ricercare i mezzi di tutela previsti dal presente DPA, alle seguenti condizioni:

10.2.2.1 Salvo i casi in cui la Normativa applicabile alla Protezione dei Dati imponga all'Affiliata Autorizzata di esercitare un diritto o di ricercare un mezzo di tutela ai sensi del presente DPA in autonomia e direttamente nei confronti di CA, le parti concordano che (i) unicamente il Cliente che è parte del Contratto eserciterà tali diritti o ricercherà tali rimedi per conto dell'Affiliata Autorizzata, e che (ii) il Cliente che rappresenta la parte contraente eserciterà tali diritti ai sensi del presente DPA non separatamente per ogni singola Affiliata Autorizzata, ma congiuntamente per tutte le proprie Affiliate Autorizzate.

11. DEFINIZIONI

"Affiliate CA " si indica qualsiasi persona giuridica sulla quale CA esercita un controllo diretto o indiretto o qualsiasi persona giuridica che eserciti un controllo diretto o indiretto su CA, o che sia soggetta al controllo diretto o indiretto da parte di uno stesso soggetto che esercita il controllo su CA.

"CA " indica l'entità del Gruppo CA parte di questo DPA, a seconda dei casi.

"Gruppo CA " indica CA e le Affiliate CA coinvolte nel Trattamento di dati Personali.

"**Affiliata Autorizzata**" indica qualsiasi Affiliata del Cliente che (a) sia soggetta alla Normativa applicabile alla Protezione dei Dati dell'Unione Europea, dello Spazio Economico Europeo e/o dei suoi stati membri, della Svizzera e/o del Regno Unito, e (b) sia autorizzata a utilizzare i Servizi ai sensi del Contratto tra il Cliente e CA, ma non abbia sottoscritto un proprio Modulo d'ordine con CA e non sia un "Cliente" come definito dal Contratto. Salvo diversa indicazione nel presente documento nell'ambito del presente DPA, il termine "Cliente" include il Cliente e le Affiliate Autorizzate. A titolo di chiarimento, "**Affiliata del Cliente** " indica una società sui cui il Cliente ha la proprietà o il controllo su oltre il 50% delle azioni o delle quote o il potere di esercitare il controllo sulle decisioni del consiglio di amministrazione di tale società in virtù della legge applicabile, di accordi contrattuali o per cause analoghe.

"Responsabile del Trattamento ", "Titolare del Trattamento ", "interessato", "Commissione", "Stato membro" e "Autorità di Controllo" hanno il significato a loro attribuito nel Capo I, Articolo 4 del GDPR; i termini collegati saranno interpretati di conseguenza.

"Normativa applicabile alla Protezione dei Dati" indica tutte le leggi e i regolamenti, comprese leggi e regolamenti dell'Unione europea, dello Spazio economico europeo e dei loro stati membri, incluso il GDPR (come definito di seguito), applicabili al Trattamento dei Dati Personali ai sensi del Contratto.

"**GDPR**" indica il Regolamento generale UE sulla protezione dei dati 2016/679 (*Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016*) sulla tutela delle persone fisiche in relazione al Trattamento dei dati Personali e sulla libera circolazione di tali dati, in abrogazione della Direttiva UE 95/46/CE.

"Dati Personali" indica qualsiasi informazione relativa a (i) una persona fisica identificata o identificabile e (ii) una persona giuridica identificata o identificabile (laddove tali informazioni siano protette in modo analogo ai dati Personali o alle informazioni di identificazione personale ai sensi del con la Normativa applicabile alla Protezione dei Dati), dove per ciascuna categoria di cui ai punti (i) o (ii), tali dati siano Dati del Cliente (come definiti nel Contratto applicabile) forniti in connessione con il Contratto.

"Trattamento" indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione ("eseguire il trattamento", "esegue il trattamento" e "oggetto di trattamento" avranno il medesimo significato).

"Violazione della sicurezza" ha il significato indicato nell'Articolo 7 del DPA.

"Documento sulle misure di sicurezza" indica il documento sulle misure di sicurezza dei Dati Personali(o la parte di esso che sia applicabile, a seconda dei Servizi che il Cliente acquisti da CA), come di volta in volta aggiornato, accessibile all'indirizzo https://www.ca.com/content/dam/ca/us/files/supportingpieces/ca-information-security-practices.pdf, o come altrimenti incorporato nel Contratto tra CA e il Cliente.

"Allegato sulla sicurezza" indica le misure di sicurezza tecniche e organizzative implementate da CA per la protezione dei Dati Personali, di cui all'Allegato 2 "Sicurezza del trattamento - GDPR art. 32". Nella misura in cui le disposizioni del Documento sulle misure di sicurezza CA e le disposizioni dell'Allegato sulla sicurezza siano in conflitto, le misure dell'Allegato 2 sulla sicurezza 2 prevarranno in relazione alle misure di sicurezza e alla protezione dei Dati Personali in conformità con i requisiti del GDPR.

"Servizi" indica la fornitura di servizi di manutenzione e supporto e/o i servizi di consulenza o professionali e/o la fornitura di software come servizio e/o gli altri servizi forniti ai sensi del Contratto laddove CA esegua il trattamento dei Dati Personali del Cliente.

Per **"Clausole contrattuali tipo"** si intende l'accordo ai sensi della decisione della Commissione europea del 5 febbraio 2010 sulle Clausole contrattuali tipo per il trasferimento di Dati Personali a Responsabili del Trattamento con sede in paesi terzi che non garantiscano un livello adeguato di protezione dei Dati Personali.

Per **"Sub-Responsabile del Trattamento"** si intende qualsiasi Responsabile del Trattamento incaricato da CA o un membro del Gruppo CA .

Elenco degli allegati

Allegato 1: Dettagli sul Trattamento dei Dati Personali del Cliente
Allegato 2: Sicurezza del Trattamento - art. 32 GDPR

Il presente DPA è stipulato e diventa una parte vincolante del Contratto/dei Contratti tra Cliente e CA, a partire dalla Data di Efficacia. Qualora il presente documento sia stato firmato elettronicamente da entrambe le parti, tale firma avrà lo stesso valore legale di una firma autografa.

Sottoscritto in nome e per conto di CA	**Sottoscritto in nome e per conto del Cliente**
Entità CA _____	**Entità Cliente:_____**
Firma:_____	**Firma:_____**
Nome:_____	**Nome:_____**
Titolo:_____	**Titolo:_____**
Data:_____	**Data:_____**

ALLEGATO 1: DETTAGLI SUL TRATTAMENTO DEI DATI PERSONALI DEL CLIENTE

Il presente Allegato 1 include alcuni dettagli sul Trattamento dei Dati Personali del Cliente come richiesto dall'articolo 28 (3) del GDPR (o, come applicabile, da disposizioni equivalenti di qualsiasi altra Normativa Applicabile per la Protezione dei Dati).

Oggetto e durata del Trattamento dei Dati Personali del Cliente

L'oggetto e la durata del Trattamento dei Dati Personali del Cliente sono definiti nel Contratto e nel presente DPA.

Natura e finalità del Trattamento dei Dati Personali del Cliente

Natura:

- ☒ Raccolta
- ☒ Registrazione
- ☐ Divulgazione
- ☒ Eliminazione
- ☐ Alterazione
- ☐ Limitazione
- ☒ Uso

Finalità:
I Dati Personali del Cliente vengono utilizzati per fornire il servizio di supporto o il SaaS come stabilito nel Contratto.

Tipi di Dati Personali del Cliente da sottoporre a Trattamento

Dati dei clienti di persone fisiche	☒
Dati dei clienti di società	☒
Dati dei dipendenti	☒
Altri Dati Personali	☐

Categorie di Interessati cui si riferiscono i Dati Personali del Cliente

Categorie speciali di Dati Personali (articolo 9 GDPR)

Salute/orientamento sessuale	☐
Appartenenza a sindacati	☐
Credenze religiose o filosofiche	☐
Opinioni politiche	☐
Origine razziale/etnica	☐

Obblighi e diritti del Cliente e delle Affiliate del Cliente

Gli obblighi e i diritti del Cliente e delle Affiliate del Cliente sono definiti nel Contratto e nel DPA, inclusi eventuali appendici o allegati al DPA.

ALLEGATO 2 - SICUREZZA DEL TRATTAMENTO - ART. 32 GDPR

Premessa

Tenendo conto dello stato dell'arte, dei costi di attuazione , nonché della natura, dell'oggetto,, del contesto e delle finalità del trattamento come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

§ 1 Misure tecniche e organizzative implementate per garantire un livello di sicurezza adeguato (SaaS e On-premise)

(1a) Misure relative alla **pseudonimizzazione/all'anonimizzazione** dei Dati Personali:
I dati memorizzati in questo prodotto non sono generalmente di natura tale da richiedere la pseudonimizzazione o l'anonimizzazione. Se necessario, il Cliente dovrà effettuare l'escalation a CA . **On-premise:** Non applicabile

(1b) Misure relative alla **crittografia** dei Dati Personali:
CRITTOGRAFIA Tutti i dati sono crittografati in transito utilizzando TLS, con le versioni 1.0, 1.1 (verrà deprecato in futuro) e 1.2 attualmente supportate. Inoltre, i Dati del Cliente sono crittografati sui server o dispositivi eventualmente rimossi dalle sedi di CA per il backup o l'archiviazione fuori sede (ove applicabile). Vengono utilizzate procedure di gestione delle chiavi che assicurano la riservatezza, l'integrità e la disponibilità del materiale delle chiavi crittografiche. L'uso di prodotti di crittografia è conforme alle limitazioni e ai regolamenti locali sull'uso della crittografia in una giurisdizione pertinente. Policy in materia di crittografia La policy di sicurezza dei dati che prevede l'utilizzo della crittografia è documentata. Il livello di robustezza della crittografia dei Dati del Cliente nella trasmissione è definito. Gestione delle chiavi di crittografia Le procedure di gestione delle chiavi crittografiche sono documentate e automatizzate. Vengono implementati prodotti o soluzioni per mantenere crittografate le chiavi di crittografia dei dati (ad esempio, soluzioni basate su software, Hardware Security Module (HSM)). Utilizzi della crittografia La trasmissione dei Dati dei Clienti sulla rete Internet pubblica avviene sempre tramite canale crittografato. I dettagli di crittografia sono documentati se la trasmissione è automatizzata. Personale autorizzato e dedicato è responsabile della crittografia/decrittografia dei dati, se eseguita manualmente. I Dati dei Clienti devono essere crittografati anche mentre in transito su qualsiasi rete. Le trasmissioni VPN avvengono su canale crittografato. **On-premise:** Il titolare del trattamento trasmette i dati del caso di assistenza in modalità crittografata al responsabile del trattamento. La risoluzione dei casi viene eseguita in un ambiente protetto. 30 giorni dopo la chiusura del caso, i dati relativi vengono eliminati

(1c) Misure volte a garantire la **riservatezza continua** dei Dati Personali:
Tutti gli accessi ai data center in cui sono archiviati i Dati dei Clienti sono limitati al team operativo di CA in base alle policy di CA in materia di controllo dell'accesso alle informazioni e di separazione dei doveri (CA segue il principio del minimo privilegio e concede l'accesso unicamente in base al ruolo e al caso di utilizzo di business). I diritti di accesso vengono rivisti regolarmente o in occasione del cambio di ruolo/cessazione del rapporto di lavoro di un dipendente. L'accesso all'ambiente in cui sono archiviati i Dati dei Clienti è rigorosamente controllato e monitorato. Il Cliente è responsabile della gestione dell'accesso ai propri dati di abbonamento e del ciclo di vita di tali account. Gli amministratori degli abbonamenti dei clienti sono responsabili dell'amministrazione degli utenti e delle policy relative alle password all'interno dell'applicazione. Il cliente è responsabile del ciclo di vita di tale account. **On-premise:** Il lavoro viene svolto in un ambiente sicuro; il trasferimento dei dati è protetto. Cancellazione dei dati dopo la chiusura del caso di supporto.

(1d) Misure atte a garantire **l'integrità continua** dei Dati Personali:
INTEGRITÀ DEI DATI Le policy e le procedure di CA sono pensate per garantire che tutti i dati archiviati, ricevuti, controllati o comunque utilizzati non siano compromessi e rimangano integri. Sono in atto procedure di ispezione per convalidare l'integrità dei dati. Controlli sulla trasmissione dei dati I processi e le procedure di controllo della trasmissione dei dati per garantire l'integrità dei dati sono documentati. Check sum e conteggi vengono utilizzati per confermare la corrispondenza tra dati trasmessi e dati ricevuti. Controlli sulle transazioni dei dati I controlli per prevenire o identificare transazioni duplicate nei messaggi finanziari sono documentati. I certificati digitali (ad esempio, firma digitale, da server a server) utilizzati per garantire l'integrità dei dati durante la trasmissione seguono un processo e una procedura documentati. **On-premise:** Non applicabile; i dati vengono eliminati dopo la chiusura del caso di supporto, vedere l'articolo 2 da a) a e)

(1e) Misure atte a garantire **la disponibilità continua dei sistemi e dei servizi di elaborazione:**

CONTROLLO DELLA DISPONIBILITÀ

- Protezione antincendio e contromisure in caso di interruzione di corrente nei centri di elaborazione dati, incluso backup

Controlli fisici

CA dispone di controlli efficaci per la protezione contro la penetrazione fisica da parte di soggetti malintenzionati o non autorizzati. I controlli fisici relativi all'intera struttura sono documentati. Ulteriori limitazioni di accesso sono applicate a server/computer/sale telecomunicazioni rispetto all'area generale.

Backup e archiviazione fuori sede

CA ha definito una policy di backup e procedure associate per eseguire il backup dei dati in modo pianificato e tempestivo. Sono definiti controlli efficaci per salvaguardare i dati di backup (in sede e fuori sede). CA garantisce inoltre che i Dati del Cliente vengano trasferiti o trasportati in modo sicuro da e verso le posizioni di backup. Inoltre, CA esegue test periodici per garantire che i dati possano essere recuperati in modo sicuro dai dispositivi di backup.

Processo di backup

Le procedure di backup e archiviazione fuori sede sono documentate. Le procedure includono la capacità di ripristinare completamente applicazioni e sistemi operativi. Il testing periodico del corretto ripristino da supporti di backup è dimostrato. L'area di staging in sede è dotata di controlli ambientali documentati e dimostrati (ad esempio, umidità, temperatura).

Distruzione dei supporti di backup

Sono definite procedure per istruire il personale sui metodi corretti di distruzione dei supporti di backup. La distruzione dei supporti di backup da parte di terzi avviene mediante procedure documentate (ad esempio certificato di distruzione) per la conferma della distruzione.

Archiviazione fuori sede

È documentato un piano di sicurezza fisica per la struttura fuori sede. Controlli di accesso vengono applicati in corrispondenza dei punti di ingresso e delle stanze di archiviazione. L'accesso alla struttura fuori sede è limitato ed esiste un processo di approvazione per ottenere l'accesso. La trasmissione elettronica dei dati alla posizione fuori sede viene eseguita su canale criptato.

On-premise:

Ambiente closed-shop; non applicabile. I dati rimangono presso il titolare del trattamento esistente

(1f) Misure atte a garantire **la resilienza continua dei sistemi e dei servizi di elaborazione:**

MONITORAGGIO DELLA VULNERABILITÀ

CA raccoglie e analizza continuamente informazioni relative a minacce e vulnerabilità nuove ed esistenti, ad attacchi effettivi all'entità o ad altri soggetti e all'efficacia dei controlli di sicurezza esistenti. I controlli di monitoraggio includono policy e procedure correlate, virus e codice dannoso, rilevamento delle intrusioni e monitoraggio di eventi e stati. Il processo di logging relativo fornisce un controllo efficace per individuare gli eventi di sicurezza e indagare al riguardo.

Policy e procedura in materia di vulnerabilità

Vengono eseguiti test di penetrazione/vulnerabilità delle reti interne/esterne e/o di host specifici. I test vengono solitamente eseguiti esternamente da un'azienda esterna di fama. Gli ambienti del cliente sono inclusi nell'ambito di test. Tutti i problemi classificati come ad alto rischio vengono corretti con tempistiche appropriate.

Antivirus e codice dannoso
Server, workstation e dispositivi Internet gateway vengono aggiornati periodicamente con le definizioni antivirus più recenti. La procedura definita evidenzia tutti gli aggiornamenti antivirus eseguiti. Gli strumenti antivirus sono configurati per eseguire scansioni settimanali, rilevamento dei virus, attività di scrittura dei file in tempo reale e aggiornamenti dei file delle firme. La protezione antivirus si estende a computer portatili e utenti remoti. Le procedure per rilevare e rimuovere eventuali applicazioni non autorizzate o non supportate (ad esempio, freeware) sono documentate.
Gli eventi di avviso includono gli attributi seguenti:
Identificatore univoco
Data
Ora
Identificatore del livello di priorità
Indirizzo IP di origine
Indirizzo IP di destinazione
Descrizione dell'evento
Notifica inviata al team di sicurezza
Stato dell'evento
Monitoraggio degli eventi di sicurezza
Gli eventi di sicurezza vengono registrati (file di log), monitorati (individui appropriati) e gestiti (azione tempestiva documentata ed eseguita). I componenti di rete, le workstation, le applicazioni e tutti gli strumenti di monitoraggio sono abilitati per monitorare l'attività degli utenti. Sono definite le responsabilità organizzative di risposta agli eventi. Vengono utilizzati strumenti di verifica della configurazione (o altri tipi di log) che registrano le modifiche critiche delle configurazioni di sistema. L'autorizzazione sui log limita le modifiche da parte degli amministratori. Il calendario di conservazione per i vari log è definito e rispettato.

(1g) Misure per ripristinare la **disponibilità e l'accesso ai Dati Personali in caso di incidente tecnico o fisico:**

Vedere sopra alla voce CONTROLLO DELLA DISPONIBILITÀ
RISPOSTA AGLI INCIDENTI
CA documenta piano e procedure associate in caso di incidente di sicurezza informatica. Il piano di risposta agli incidenti articola chiaramente le responsabilità del personale e identifica i soggetti competenti per la notifica. Il personale addetto alla risposta agli incidenti è addestrato. L'esecuzione del piano di risposta agli incidenti viene testata periodicamente.
Processo di risposta agli incidenti
La policy e le procedure di gestione degli incidenti di sicurezza informatica sono documentate. La policy e/o le procedure di gestione degli incidenti includono i seguenti attributi:
- La struttura organizzativa è definita
- Il team di risposta è identificato
- La disponibilità del team di risposta è documentata
- Le tempistiche per il rilevamento e la divulgazione degli incidenti sono documentate
- Il ciclo di vita del processo di incidente è definito includendo i seguenti passaggi discreti:
  - Identificazione
  - Assegnazione del livello di gravità a ciascun incidente
  - Comunicazione

• Risoluzione • Formazione • Test (frequenza dei controlli) • Reporting • Gli incidenti devono essere classificati e categorizzati per priorità • Le procedure di risposta agli incidenti devono includere la notifica del Cliente al responsabile del rapporto (delivery manager) o altro referente indicato nel contratto Escalation/notifica Il processo di risposta agli incidenti viene avviato non appena CA viene a conoscenza dell'incidente (indipendentemente dall'ora del giorno). **On-premise:** Solo parzialmente applicabile; i dati vengono eliminati alla chiusura del caso di supporto.

(1h) Misure per **testare e valutare periodicamente l'efficacia delle misure tecniche e organizzative:**
CONTROLLO ORGANIZZATIVO OPERATIONS CA ha documentato le procedure operative IT per garantire un funzionamento corretto e sicuro delle risorse IT. Procedure e responsabilità operative. Le procedure operative sono documentate in un manuale operativo e correttamente implementate. Il manuale operativo include i componenti seguenti: Requisiti di pianificazione Gestione degli errori (ad esempio trasporto di dati, stampa, copie) Generazione e gestione di output speciali Manutenzione e risoluzione dei problemi relativi ai sistemi Procedure documentate per gestire SLA/KPI e struttura di reporting per escalation Gli audit di sicurezza interni vengono eseguiti periodicamente presso il responsabile del trattamento, includendo il responsabile della protezione dei dati (esterno)

§ 2 Responsabili della privacy dei dati

Nome:	Recapiti:
Bonnie Yeomans	CA, Inc. 520 Madisfon Avenue New York, NY 10022 Assistant General Counsel e Chief Privacy Officer
Yasmin Brook	CA Deutschland GmbH Marienburgstr. 35

	64297 Darmstadt Germania Senior Counsel e Global Field Privacy Officer

§ 3 Un elenco aggiornato dei Sub-Responsabilidel Trattamento è disponibile all'indirizzo https://support.ca.com/us/product-content/admin-content/subprocessor-list.html

§ 4 Affiliate CA che forniscono supporto e manutenzione in conformità con il Contratto

Entità CA		
Nome	**Recapiti**	**Sede**
CA Argentina S.A.	Av. Alicia Moreau de Justo 400, Piso 4, Buenos Aires, Argentina C.P. C1107AAH	Argentina
CA (Pacific) Pty Ltd	6 Eden Park Drive, North Ryde, New South Wales 2113, Australia	Australia
CA Software Österreich GmbH	EURO PLAZA, Am Europlatz 5, Gebäude C, 1120 Vienna	Austria
CA Belgium SA	Da Vincilaan 11, Building Figueras, B-1935 Zaventem - Belgium	Belgio
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	Brasile
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	Cile
CA CZ, s.r.o	Praha 4 - Chodov, V Parku 2316/12, PSČ 148 00	Repubblica Ceca
CA Software ApS	Borupvang 5B, DK - 2750, Ballerup, Denmark	Danimarca
CA Limited (formerly CA Plc and fomerly Computer Associates Plc)	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inghilterra
CA Technology R&D Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inghilterra
Computer Associates Holding Ltd.	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inghilterra
Computer Associates UK Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inghilterra
CA SAS	Tour Opus 12, 4 Place des Pyramides, La Défense 9, 92914 Paris La Défense Cedex, France,	Francia
CA Computer Associates European Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germania
CA Computer Associates Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germania

CA Computer Associates Technology GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germania
CA Deutschland GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germania
CA (India) Technologies Private Limited	Ground Floor, Vibgyor Tower, Plot C-62, G-Block, Bandra Kurla Complex, Bandra (East), Mumbai - 400 051	India
CA Software Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israele
CA Technologies R&D Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israele
CA S.r.l.	Via Francesco Sforza 3, 20080 Milano Tre, Basiglio (MI)	Italia
CA Japan, Ltd.	JA Kyosai Bldg., 2-7-9 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093, Japan	Giappone
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	Messico
CA Software de Mexico, S.A. de C.V	vedere sopra	Messico
CA Europe Holding B.V.	Orteliuslaan 1001, 3528 BE, Utrecht, Netherlands	Paesi Bassi
CA software BV	vedere sopra.	Paesi Bassi
CA Software Holding BV	vedere sopra.	Paesi Bassi
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	Spagna