DATA PROCESSING ADDENDUM - GDPR

This Data Processing Addendum ("**DPA**" or "Addendum") forms part of the existing agreement(s) between Customer and CA, and/or other written or electronic agreement between CA and Customer for the purchase of Services provided by CA (the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data of Customer, in accordance with the requirements of Data Protection Laws. The Effective Date of this DPA is the date of the last signature of a party below. All capitalized terms not defined herein shall have the meaning set out in the Agreement.

1. GENERAL TERMS

This DPA applies to the Processing of Personal Data, within the scope of the EU General Data Protection Regulation 2016/679 (as further defined in Section 11, and hereinafter "GDPR"), by CA on behalf of Customer. Effective May 25, 2018, CA will Process Personal Data in accordance with the GDPR requirements directly applicable to CA's provision of its Services. This DPA does not limit or reduce any data protection commitments relating to Processing of Customer Data previously negotiated by Customer in the Agreement (including any existing data processing addendum to the Agreement).

By signing this Addendum, Customer enters into the DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates, if and to the extent CA Processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates, unless otherwise indicated herein.

In the course of providing the Services to Customer pursuant to the Agreement, CA may Process Personal Data on behalf of Customer. CA agrees to comply with the following provisions with respect to any Personal Data Processed for Customer in connection with the provision of the Services. If not otherwise defined in the relevant section, all definitions applicable to this DPA have been consolidated into Section 11, titled "Definitions."

2. PROCESSING OF PERSONAL DATA

2.1 The parties agree that with regard to the Processing of Personal Data, Customer is the Data Controller, CA is a Data Processor and that CA or members of the CA Group will engage Subprocessors pursuant to the requirements set forth in Section 5 "Subprocessors" below.

2.2 Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Customer will ensure that its instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 CA will Process Personal Data in accordance with applicable Data Protection Laws, the GDPR requirements, directly applicable to CA's provision of its Services. CA shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions and shall treat Personal Data as Confidential Information. Customer instructs CA to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable orders; (ii) Processing to comply with other reasonable instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Agreement, and (iii) Processing of Personal Data that is required under applicable law to which CA or CA Affiliate is subject, including but not limited to applicable Data Protection Laws, in which case CA or the relevant CA Affiliate shall to the extent permitted by applicable law, inform the Customer of such legally required Processing of Personal Data.

2.4. As required under Article 28(3) of the GDPR, the subject matter and duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set forth in Annex I to this DPA Addendum (titled "Annex 1: Details of Processing Customer Personal Data"). The subject matter of Processing of Personal Data by CA is the performance of the Services provided under the Agreement. Upon prior written notice, Customer may request reasonable amendments to Annex 1 as Customer reasonably considers necessary to meet the requirements of Article 28(3) of the GDPR and CA will review such requested changes. Nothing in Annex 1 confers any right or imposes any obligation on any party to this Addendum.

3. RIGHTS OF DATA SUBJECTS

3.1. CA shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"). Taking into account the nature of the Processing, CA shall assist Customer by appropriate technical and organizational measures, to the extent possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Chapter III of the GDPR. Except to the extent required by applicable law, CA shall not respond to any such Data Subject Request without Customer's prior written consent except to confirm that the request relates to Customer.

3.2 Further, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, CA shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent CA is legally permitted to do so and provided that such Data Subject Request is required under applicable Data Protection Laws. Any costs arising from such provision of assistance shall be the responsibility of Customer, to the extent legally permitted.

4. PERSONNEL

4.1 CA shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality and such obligations survive the termination of that persons' engagement with CA.

4.2 CA shall take commercially reasonable steps to ensure the reliability of any CA personnel engaged in the Processing of Personal Data.

4.3 CA shall ensure that CA Group's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

4.4 Data Protection Officer. Members of the CA Group have appointed a data protection officer where such appointment is required by Data Protection Laws. The appointed person may be reached at datatransfers@ca.com.

5. SUBPROCESSORS

5.1 Customer acknowledges and agrees that (a) CA's Affiliates may be retained as Subprocessors; and (b) CA and CA's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. Any such Subprocessors will be permitted to obtain Personal Data only to deliver the services CA has retained them to provide, and they are prohibited from using Personal Data for any other purpose.

5.2 CA shall be liable for the acts and omissions of its Subprocessors to the same extent CA would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.3 CA or CA Affiliate has entered into a written agreement with each Subprocessor containing data protection obligations that are no less protective than the terms set forth in this Addendum with respect to the protection of Personal Data and meet the requirements of Article 28(3) of the GDPR or equivalent provisions of any other Data Protection Law, to the extent applicable to the nature of the Services provided by such Subprocessor.

5.4 Customer authorizes CA and each CA Affiliate to appoint Subprocessors in accordance with this Section 5. The list of CA Subprocessors used by CA in connection with its provision of the Services is set forth in Annex 2, and such list includes all Subprocessors' identities and country of location ("**Subprocessors List**"). In the event CA makes any changes or additions to such list, the current Subprocessor List is made available to Customer at: https://support.ca.com/us/product-content/admin-content/subprocessor-list.html, thereby giving Customer the opportunity to object to such changes (as set further set forth in section 5.5 below) .

5.5. Customer may object to CA's use of a new Subprocessor by notifying CA promptly in writing within ten (10) business days after any updates are made by CA to the Subprocessor list. In the event of such objection by Customer, CA will take commercially reasonable steps to address the objections raised by Customer and provide Customer with reasonable written explanation of the steps taken to address such objection.

5.6. Data Transfers. CA shall not transfer Personal Data of Customer except lawfully, in compliance with applicable Data Protection Laws and Personal Data will be transferred in accordance with CA's statement and terms set out at https://www.ca.com/us/legal/privacy/data-transfers.html . Solely for the provision of Services to Customer under the Agreement and subject to this Section 5.6, Customer hereby authorizes CA to make routine transfers of Personal Data to the local CA Group entity and/or approved Sub-processors of CA. Notwithstanding, in the event that Personal Data of Customer is transferred from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of the foregoing territories ("**Restricted Transfers**"), CA complies with the provisions of Section 5.6(a), with respect to such Restricted Transfers.

(a) **Transfer mechanisms for Restricted Transfers.** CA makes available the transfer mechanisms listed below which shall apply, with respect to any Restricted Transfers under this DPA, to the extent such transfers are subject to such Data Protection Laws:

(1) **Privacy Shield self-certifications**. CA has certified its compliance to the EU-US Privacy Shield Program. CA shall maintain its certification to the Privacy Shield for so long as it maintains any EEA Personal Data. In the event that EU authorities or courts determine that the Privacy Shield is not an appropriate basis for transfers, the parties shall promptly execute an approved EU Standard Contractual Clauses (Processors), which shall be incorporated herein upon execution.

(2) **EU Standard Contractual Clauses**. CA and CA Affiliates acting as Subprocessor (as listed in Annex 2) have previously entered into The EU Standard Contractual Clauses for a controller-processor relationship and for the benefit of the Customer. Further, CA hereby enters into approved EU Standard Contractual Clauses (Processors), as further set forth in Section 9 of this Addendum, and a copy of which is attached hereto in Attachment 1.

In the event that Services are covered by more than one transfer mechanism, the transfer of Customer's Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) Privacy Shield self-certifications; (ii) EU Standard Contractual Clauses.

6. SECURITY

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and CA shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. CA will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data that meet the requirements for a Data Processor under the GDPR, as set forth in Annex 2 "Security of Processing – GDPR Art. 32". CA regularly monitors compliance with these safeguards. CA will not materially decrease the overall security of the Services during the term of CA's provision of such Services pursuant to the applicable Agreement or order form thereunder.

6.2 Upon Customer's written request at reasonable intervals, CA shall provide a copy of CA's then most recent third-party audits or certifications, as applicable, or any summaries thereof, related to the Processing of Personal Data of Customer, that CA generally makes available to its customers at the time of such request. CA shall make available to Customer, upon reasonable written request, such information necessary to demonstrate compliance with this Addendum, and shall allow for written audit requests by Customer or an independent auditor in relation to the Processing of Personal Data to verify that CA employs reasonable procedures in compliance with this Addendum, provided that Customer shall not exercise this right more than once per year. Such information and audit rights are provided under this section 6.2 to the extent the Agreement does not provide such audit rights that meet the requirements of applicable Data Protection Laws (including, where applicable, Article 28(3)(h) of the GDPR). Any information provided by CA and/or audits performed pursuant to this section are subject to the confidentiality obligations set forth in the Agreement.

6.3 CA shall provide Customer with reasonable assistance as needed to fulfil Customer's obligation to carry out a data protection impact assessment under Article 35 or 36 of the GDPR as related to Customer's use of the Services. CA will provide such assistance upon Customer's reasonable request and to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to CA. Additionally, CA will provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 6.3, to the extent required under the GDPR.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 CA will promptly notify Customer, without undue delay, after CA becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unlawful access to any Customer's Personal Data that is transmitted, stored or otherwise Processed by CA or its Subprocessors of which CA becomes aware ("**Security Breach**"). CA will use reasonable efforts to identify the cause of such Security Breach and shall promptly and without undue delay: (a) investigate the Security Breach and provide Customer with information about the Security Breach, including if applicable, such information a Data Processor must provide to a Data Controller under Article 33(3) of the GDPR to the extent such information is reasonably available; and (b) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Breach to the extent the remediation is within CA's reasonable control. The obligations herein shall not apply to any breach that is caused by Customer or it Authorized Users. Notification will be delivered to Customer in accordance with Section 7.3 below.

7.2 CA's obligation to report or respond to a Security Breach under this Section is not and will not be construed as an acknowledgement by CA of any fault or liability with respect to the Security Breach.

7.3. Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means CA selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on CA's support systems at all times.

8. RETURN AND DELETION OF CUSTOMER DATA

8.1 CA shall return Customer Data to Customer and/or delete Customer Data in accordance with CA's procedures and Data Protection Laws and/or consistent with the terms of the Agreement.

8.2 At Customer's request, CA shall delete or return all Personal Data to Customer after the end of the provision of Services relating to Processing, and delete existing copies, in accordance with the procedures set forth in Annex 2 "Security of Processing – GDPR Art. 32", unless applicable Data Protection Law requires storage of the Personal Data.

9. ADDITIONAL TERMS FOR EU PERSONAL DATA

9.1 The Standard Contractual Clauses in Attachment 1 and the additional terms in this Section 9 will apply to the Processing of Personal Data by CA in the course of providing the Services.

> **9.1.1** The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) or Switzerland to outside the EEA or Switzerland, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described pursuant to applicable Data Protection Law, and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors.
>
> **9.1.2** The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an order under the Agreement. For the purpose of the Standard Contractual Clauses and this Section 9, the Customer and its Affiliates shall be deemed to be "Data Exporters".

9.2 This DPA and the Agreement are Data Exporter's complete and final instructions to Data Importer for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Data Exporter to Process Personal Data: (a) in accordance with the Agreement and applicable orders thereunder; and (b) in compliance with other reasonable instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Agreement.

9.3 Pursuant to Clause 5(h) of the Standard Contractual Clauses, the Data Exporter acknowledges and expressly agrees that CA's Affiliates may be retained as Subprocessors; and (b) CA and CA's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. Data Importer shall make available to Customer a current list of Subprocessors for the respective Services with the identities of those Subprocessors in accordance with Section 5.5 of this DPA, further detailing CA's provision of the Subprocessor List.

9.4 The parties agree that the copies of the Sub-processor agreements that must be sent by the Data Importer to the Data Exporter pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses or their equivalent, removed by the Data Importer beforehand; and that such copies will be provided by Data Importer only upon reasonable request by Data Exporter.

9.5 The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Data Exporter's request, and subject to the confidentiality obligations set forth in the Agreement, Data Importer shall, within a reasonable period following such request, make available to Data Exporter (or Data Exporter's independent, third-party auditor that is not a competitor of CA) information regarding CA Group's compliance with the obligations set out in this DPA in the form of the third- party certifications and audits it carries out as described in the Agreement and/or the Security Practices Document to the extent CA makes them generally available to its customers. Customer may contact Data

Importer in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Data Importer for any time expended for any such on-site audit at the CA Group's then-current professional services rates, which shall be made available to Data Exporter upon request. Before the commencement of any such on-site audit, Data Exporter and Data Importer shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Data Exporter shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Data Importer. Data Exporter shall promptly notify Data Importer with information regarding any non-compliance discovered during the course of an audit.

9.6 The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) shall be provided by the Data Importer to the Data Exporter only upon Data Exporter's request.

9.7 In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1, the Standard Contractual Clauses shall prevail. If this document has been electronically signed by either party such signature will have the same legal affect as a hand written signature.

10. PARTIES TO THIS DPA

10.1 Limitation of Liability. CA, Inc. is a party to the Standard Contractual Clauses in Attachment 1. If CA, Inc. is not a party to the Agreement, the Section of the Agreement 'Limitation of Liability' shall apply as between Customer and CA, Inc., and in such respect any reference to 'CA' shall include both CA, Inc. and the CA entity who is a party to the Agreement. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and CA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement governing the applicable Services, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes, Schedules and/or Appendices.

10.2 Authorized Affiliates & Contractual Relationship. By executing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Authorized Affiliates if and to the extent CA Processes Personal Data for which such Authorized Affiliates qualify as the Data Controller. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement, and such Authorized Affiliate is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates, unless otherwise indicated herein.

10.2.1 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with CA under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.2.2 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with CA, it shall to the extent required under applicable Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.2.2.1 Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against CA directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately

for each Authorized Affiliate individually, but in a combined manner for all of its Authorized Affiliates together.

11. DEFINITIONS

"CA Affiliates" means any entity which is controlled by, controls or is in common control with CA.

"CA" means the CA Group entity that is a party to this DPA, as applicable.

"CA Group" means CA and its Affiliates engaged in the Processing of Personal Data.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which (a) is subject to the Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and CA, but has not signed its own Order Form with CA and is not a "Customer" as defined under the Agreement. For the purposes of this DPA only, the term "Customer" shall include Customer and Authorized Affiliates, unless otherwise indicated herein. For the avoidance of doubt, "**Customer Affiliate**" means a legal entity that Customer directly or indirectly majority owns or controls through a majority interest.

"Data Controller", "Data Processor", "Data Subject", "Commission", "Member State", and "Supervisory Authority" shall have the meaning given to them in Chapter 1, Article 4 of the GDPR and their cognate terms shall be construed accordingly.

"Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, including the GDPR (as defined below), applicable to the Processing of Personal Data under the Agreement.

"**GDPR**" means EU General Data Protection Regulation 2016/679 (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*) on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing EU Directive 95/46/EC.

"Personal Data" means any information relating to (i) an identified or identifiable person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws), where for each (i) or (ii), such data is Customer Data (as defined in the applicable Agreement) provided in connection with the Agreement.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning).
"Security Breach" has the meaning given in Section 7 of this Addendum.

"Security Practices Document" means the Information Security Practices Document (or the applicable part dependent on what Services Customer purchases from CA), as updated from time to time, accessible at https://www.ca.com/content/dam/ca/us/files/supportingpieces/ca-information-security-practices.pdf, or as otherwise incorporated in the Agreement between CA and Customer.

"Security Annex" means the technical and organizational security measures implemented by CA for the protection of Personal Data, set forth in Annex 2 "Security of Processing – GDPR Art. 32". To the extent that the terms of the

CA Security Practices Document and the terms of the Security Annex conflict, the terms of the Security Annex 2 shall govern with respect to the security measures and protection of Personal Data in accordance with the requirements of the GDPR.

"Services" means the provision of maintenance and support services and/or consultancy or professional services and/or the provision of software as a service and/or any other services provided under the Agreement where CA Processes Personal Data of Customer.

"Standard Contractual Clauses" means the agreement executed by and between Customer and CA, Inc. and attached as Attachment 1 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Subprocessor" means any Data Processor engaged by CA or a member of the CA Group.

List of Annexes & Attachments
Annex 1: Details of Processing Customer Personal Data
Annex 2: Security of Processing – Art. 32 GDPR
Attachment 1: Standard Contractual Clauses - https://www.ca.com/us/legal/privacy/data-transfers.html?intcmp=footernav

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement(s) between Customer and CA, as of the Effective Date. If this document has been electronically signed by either party such signature will have the same legal affect as a hand-written signature.

Agreed for and on behalf of CA	**Agreed for and on behalf of Customer**
CA Entity:	**Customer Entity:**
Signed:_____	Signed:_____
Name:_____	Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

ANNEX 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR (or as applicable, equivalent provisions of any other Data Protection Law).

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Customer Personal Data

Nature:

- ☒ Collection
- ☒ Recording
- ☐ Disclosure
- ☒ Deletion
- ☐ Alteration
- ☒ Restriction
- ☒ Use

Purpose:

Customer Personal Data is used to provide Support or SaaS as set out in the Principal Agreement.

The types of Customer Personal Data to be Processed

Customer Data of natural persons		☒
Customer Data of companies	☒	
Employee Data		☒
Other Personal Data		☐

The categories of Data Subject to whom the Customer Personal Data relates

Special Categories of Personal Data (Art. 9 GDPR)

Health/sex Life	☐
Trade Union Membership	☐
Religious or Philosophical Beliefs	☐
Political Opinions	☐
Racial/Ethnic Origin	☐

The obligations and rights of Customer and Customer Affiliates

The obligations and rights of Customer and Customer Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 2 - SECURITY OF PROCESSING – ART. 32(1) GDPR

Preamble

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

§ 1 Technical and organisational measures implemented to ensure an appropriate level of security (SaaS)

(1a) Measures on **pseudonymisation /anonymisation** of personal data:
Personal Data stored in this product is either encrypted, or has pseudonymization or anonymization applied where required. Personal Data that could directly identify a Data Subject is not stored in clear form.

(1b) Measures on the **encryption** of personal data:
ENCRYPTION All data is encrypted in-transit using the TLS 1.2 encryption standard, or subsequent versions as may be required by compliance frameworks to which CA is subject (e.g. PCI DSS) over public networks. In addition, Customer Data is encrypted on any server or device that is removed from CA's premises for backup or off-site storage (where applicable). Key management procedures are employed that assure the confidentiality, integrity and availability of cryptographic key material. Encryption Policy CA has defined policies that specify encryption and hashing function usage. The encryption strength of Customer Data in transmission is defined as per the PCI DSS compliance standards. Encryption Key Management Cryptographic key management policies and procedures are documented in a key management policy document. Compliance with key management procedures is audited. Cryptographic materials, including keys, are secured as per the Visa ACS Security Requirements and PCI DSS guidelines. CA has a restricted and controlled set of Security Officers who are authorized to handle cryptographic materials and access manual encryption or decryption processes. Encryption Uses Customer Data transmission over the public internet always utilizes encrypted channels. The data of each Customer on the CA platform is segregated from every other Customer on the platform through the use of encryption. Personal Data is stored in encrypted, pseudonymized, or anonymized formats and not in clear. Certain data and messages are digitally signed to ensure integrity. Bulk data ingested from customers is stored and transmitted in encrypted form. Encryption is used to protect certain cryptographic keys.

(1c) Measures of ensuring the **ongoing confidentiality** of personal data:
In addition to the measures detailed in 1(a) and 1(b): All access to the data centers where Customer Data is stored, is restricted to CA's Operations Team according to CA Information Access Control Policies and CA Segregation of Duties Policy (CA follows the principle of least privilege and only grants access based on role and business use case). Access rights are reviewed regularly or upon change of role/termination of an employee. Access to the environment where Customer Data is stored is strictly controlled and monitored. Customer has control over its own personnel access to the administration tools provided by the CA Payment Security Suite. Customer can define administrator accounts, their disposition (active/inactive), the role and associated privileges within the CA Payment Security Suite. The CA platform is subject to regular audits to applicable industry standards (e.g. PCI DSS, SOC 1, SOC 2, SSAE 18). Product development is required to follow CA's internal Privacy by Design guidelines. The CA platform is subject to application development and deployment security measures defined by industry standards and compliance requirements to which CA is subject (e.g. PCI DSS). All CA employees are required to comply with CA's privacy policies. Third party suppliers or subcontractors who provide services, components, technologies, or data feeds which are directly integrated with the CA platform are reviewed to ensure compliance with the GDPR as well as applicable compliance standards to which CA is subject.

(1d) Measures to ensure **ongoing integrity** of personal data:
DATA INTEGRITY Monitoring measures and operational policies, controls, and supporting procedures exist to monitor the platform for events which may affect integrity of data: • Hardware failures • Software / application errors • System compromise Bulk data ingestion from Customer: data uploaded to the CA platform by Customer is checked for integrity by the tools used by the CA to load the data to its platform, however Customer must also take reasonable care to ensure the integrity of any data it intends to upload to the CA platform. Data Transmission Controls In addition to integrity controls available via standard data transmission protocols, data is encrypted during transmission over public networks which ensures integrity as well as confidentiality. Data Storage. The CA platform uses industry standard hardware capabilities to ensure integrity of stored data (redundancy, checksums, parity checks, etc.) Transaction Integrity Controls to prevent or identify duplicate transactions in financial messages are implemented in the application as per the 3D Secure protocol.

(1e) Measures to ensure **ongoing availability and resilience of processing systems and services:**
AVAILABILITY CONTROL - Protection against fire and measures in case of power outages in the data processing centers including backup Physical Controls CA Technologies has effective controls in place to protect against physical penetration by malicious or unauthorized people. Physical controls covering the entire facility are documented. Additional access restrictions such as anti-pass back, CCTV Camera's, enhanced background checks for personnel with access to the CA Payment Security environment, visitor logs, etc are enforced for servers/ computer/ telecommunications room compared to the general area. Backup and Offsite Storage CA Technologies has a defined backup policy and associated procedures for performing backup of data in a scheduled and timely manner. Effective controls are established to safeguard backed up data (onsite and off-site). CA Technologies also ensures that Customer Data is securely transferred or transported to and from backup locations. Furthermore, CA Technologies conducts periodic tests to ensure that data can be safely recovered from backup devices. Backup Process Backup and offsite storage procedures are documented. Procedures encompass ability to fully restore applications and operating systems. Periodic testing of successful restoration from back-up media is demonstrated. CA Payment Security Suite platform has active DDos mitigation solution in place which ensures availability and resilience against such attacks. The primary and disaster recovery sites are geographically apart and are running in active passive mode to mitigate any site wide disaster. Each site uses component level redundancy, clustering and fault tolerant architecture for continuous availability and resiliency at the site level. CA Payment Security Suite follow state of the art application design standards like Secure Coding, Secure Software Development Life Cycle (SSDLC), rigorous QA Testing and Input Validation as per the 3D Secure protocol.

(1f) Measures to restore **availability and access to personal data in the event of a technical or physical incident and incident response measures:**

INCIDENT RESPONSE MEASURES
CA Technologies documents a plan and associated procedures in case of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant notification parties. Incident response personnel are trained.
Incident Response Process
Information security incident management policy and procedures are documented. The incident management policy and/ or procedures include the following attributes:
• Organizational structure is defined
• Response team is identified
• Response team availability is documented
• Timelines for incident detection and disclosure are documented
• Incident process lifecycle is defined including the following discrete steps:
  • Identification
  • Assignment of severity to each incident
  • Communication
  • Resolution
  • Training

• Reporting • incidents must be classified and prioritized • incident response procedures must include Customer notification to the relationship (delivery) manager or another contact listed in the contract Escalation/Notification Incident response process is executed as soon as CA Technologies is aware of the incident (irrespective of time of day). CA Technologies performs yearly functional disaster recovery testing of all the components and provides certification. This ensures all the data and cryptographic materials are present and functioning. CA Technologies has a documented disaster recovery and business continuity policy. The data is replicated to the disaster recovery site in almost real time and software components are also updated as in the primary site. Both primary and disaster recovery data centers are actively monitored.

(1g) Measures for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures:**
CA Technologies is audited to industry standard security and operational frameworks such as PCI-DSS, SSAE 18, SOC 1, SOC 2, where the effectiveness of technical and organization security measures are thoroughly audited.

§ 2 Data Protection Officer/Data Privacy Officer

Name:	Contact Details:
Bonnie Yeomans	CA, Inc. 520 Madison Avenue New York, NY 10022 Assistant General Counsel and Privacy Officer
Yasmin Brook	CA Deutschland GmbH Marienburgstr. 35 64297 Darmstadt Germany Senior Counsel & Global Field Privacy Officer

§ 3 List of agreed Current Subprocessors is below. An updated list can be found at https://support.ca.com/us/product-content/admin-content/subprocessor-list.html

For Payment Security	
Name	Location
N/A – CA Payment Security does not use any subprocessors.	

Support for all products	
Name	Location
SFDC (Service Cloud)	USA

§ 4 CA Entities providing support and maintenance in accordance with the Principal Agreement

CA Entities		
Name	**Contact Details**	**Location**
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	Belgium
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	Brazil
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	Chile
CA CZ, s.r.o	Praha 4 - Chodov, V Parku 2316/12, PSČ 148 00	Czech Republic
CA Software ApS	Borupvang 5B, DK - 2750, Ballerup, Denmark	Denmark
CA Limited (formerly CA Plc and fomerly Computer Associates Plc)	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
CA Technology R&D Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
Computer Associates Holding Ltd.	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England
Computer Associates UK Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	England

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	Germany
CA Computer Associates Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
CA Computer Associates Technology GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
CA Deutschland GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Germany
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	Israel
CA Technologies R&D Israel Ltd.	CA Building, 16 Shenkar Street, P.O. Box 2207, Herzliya 46120, Israel	Israel
CA S.r.l.	Via Francesco Sforza 3, 20080 Milano Tre, Basiglio (MI)	Italy
CA Japan, Ltd.	JA Kyosai Bldg., 2-7-9 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093, Japan	Japan
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	Mexico
CA Software de Mexico, S.A. de C.V	see above	Mexico
CA Europe Holding B.V.	Orteliuslaan 1001, 3528 BE, Utrecht, Netherlands	Netherlands
CA software BV	see above.	Netherlands
CA Software Holding BV	See above.	Netherlands
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	Spain

Attachment 1

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel.: ..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

……
(the data **exporter**)

And

Name of the data importing organisation: **CA, Inc.**

Address: **520 Madison Avenue, 22nd Floor, New York, NY, USA, 1002**
Tel.: **1-800- 225-5224**
fax: **N/A**

e-mail: **datatransfers@ca.com**

Other information needed to identify the organisation:

……
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful

destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely…….

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ……
……
……

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address: **520 Madison Avenue, 22nd Floor, New York, NY, USA, 1002**

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is a non-CA party which is a user of CA's products and services including software, support and maintenance, software as a service.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):

The data importer is CA, Inc. a global producer and provider of software, software as a service and other services ("Software and Services").

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

The data subject includes the data exporter's end-users, employees, contractors, collaborators, and customers of the data exporter.

Categories of data
The personal data transferred concern the following categories of data (please specify):

The personal data transferred concern the following categories of data (please specify) includes documents and other data in an electronic form in the context of Software and Services.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the agreement between CA and the Customer. The objective of the data processing is the provision and performance of Software and Services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the agreement between CA and Customer. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities.

c. Data Exporter's Instructions. For Software and Services, CA will only act upon Customer's instructions as conveyed to CA by Customer.

d. Customer Data Deletion or Return. Upon expiration or termination of the agreement with the Customer or in the case of data supplied as part of a support ticket after 30 days of the closure of such support ticket, data importer will delete customer data.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer's Personal Data, as described in CA's "**Security of Processing – GDPR Art. 32**" attached as Annex 2 of the Data Processing Agreement (updated versions will be made available on request), or otherwise made reasonably available by data importer. The relevant parts of the document may differ based on the applicable products and services Customer purchases from CA.

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name: ……

Authorised Signature ……