ANEXO SOBRE EL TRATAMIENTO DE DATOS – RGPD

El presente Anexo sobre el tratamiento de datos ("**DPA**" o "Anexo") forma parte de los acuerdos existentes entre _____ (el "Cliente") y CA IT Management Solutions Spain, S.L.U., con domicilio en WTC Almeda Park, Edificio 2, planta 4, Plaça de la Pau s/n, 08940 Cornellá de Llobregat y provista de CIF B59303586 ("CA"), o de cualquier otro acuerdo escrito o por medios electrónicos entre CA y el Cliente, para la compra de los servicios ofrecidos por CA (el "**Acuerdo**"), con el fin de dejar constancia del acuerdo de las partes referente al tratamiento de los datos personales del Cliente, de conformidad con los requisitos establecidos en las leyes en materia de protección de datos. La fecha de entrada en vigor de este DPA es la fecha de la última firma por una de las partes. Los términos en mayúsculas no definidos en este Anexo tendrán el significado descrito en el Acuerdo.

1. CONDICIONES GENERALES

Este DPA se aplica al tratamiento de datos personales, en el marco del Reglamento General de Protección de Datos 2016/679 de la Unión Europea (tal como se define en la Cláusula 11, en adelante "RGPD"), ejercido por CA en nombre del Cliente. Desde su entrada en vigor el 25 de mayo de 2018, CA trata los datos personales de conformidad con los requisitos del RGPD que se apliquen directamente a la prestación de los Servicios de CA. Este DPA no limita ni reduce los compromisos de protección de datos relacionados con el tratamiento de los datos del Cliente negociados previamente en el Acuerdo (incluidos los anexos de tratamiento de datos existentes en dicho Acuerdo).

Con la firma de este Anexo, el Cliente suscribe el DPA en su nombre y, en la medida en que las leyes de protección de datos aplicables lo requieran, en nombre y por cuenta de sus Filiales Autorizadas, en el caso y en la medida en que CA realice el tratamiento de datos personales en los que dichas Filiales Autorizadas estén catalogadas como Responsables del tratamiento. Exclusivamente a efectos de este DPA, el término "Cliente" incluirá al Cliente y a las Filiales Autorizadas, si no se indica lo contrario.

En el transcurso de la prestación de los Servicios al Cliente en el marco del Acuerdo, CA puede tratar datos personales en nombre de éste. CA acepta cumplir las siguientes disposiciones con respecto a los datos personales tratados del Cliente en relación con la prestación de los Servicios. Salvo que se establezca otra cosa expresamente en este documento, todas las definiciones aplicables a este DPA se han unificado en la Cláusula 11, "Definiciones".

2. TRATAMIENTO DE DATOS PERSONALES

2.1 Las partes acuerdan que, con respecto al tratamiento de datos personales, el Cliente actúa como responsable del tratamiento y CA como encargado del tratamiento, y que CA o entidades pertenecientes al Grupo CA contratarán subencargados de conformidad con los requisitos establecidos en la Cláusula 5 siguiente, "Subencargados".

2.2 El Cliente, durante el uso o la recepción de los Servicios, tratará los datos personales de acuerdo con los requisitos establecidos en las Leyes de Protección de Datos y garantizará que sus instrucciones sobre el tratamiento de datos personales cumplan con dichas leyes. El Cliente es el único responsable de la precisión, la calidad y la legalidad de los Datos Personales y de los medios a través de los cuales ha recopilado dichos datos.

2.3 CA Tratará los datos personales de conformidad con las Leyes de Protección de Datos aplicables a la prestación de los Servicios de CA. CA únicamente Tratará los Datos Personales en nombre del Cliente, de conformidad con las instrucciones documentadas de éste. CA Tratará los Datos Personales como Información Confidencial. El Cliente encarga a CA el Tratamiento de Datos Personales para los siguientes fines: (i) Tratamiento conforme al Acuerdo y a las disposiciones aplicables; (ii) Tratamiento para cumplir con otras instrucciones razonables del Cliente (p. ej., mediante un ticket de soporte), que sean coherentes con las condiciones del Acuerdo, y (iii) Tratamiento de Datos Personales requerido por las leyes aplicables a las que están sujetos CA o sus Filiales, lo que incluye pero no está

limitado a las Leyes de Protección de Datos, y en cuyo caso CA (o la Filial de CA en cuestión) informará al Cliente, siempre que la ley lo permita, del tratamiento de datos personales exigido legalmente.

2.4. Según lo establecido en el Artículo 28(3) del RGPD, el objeto, la duración, la naturaleza y la finalidad del Tratamiento, los tipos de Datos Personales y las categorías de Interesados se establecen en el Apéndice I de este Anexo (titulado "Apéndice 1: Información sobre el Tratamiento de Datos Personales del Cliente"). El objeto del Tratamiento de Datos Personales por parte de CA es el desempeño de los Servicios prestados en virtud del Acuerdo. Previa notificación por escrito, el Cliente puede solicitar que se realicen modificaciones razonables en el Apéndice 1, si el Cliente lo considera necesario para cumplir los requisitos del Artículo 28(3) del RGPD, y CA revisará los cambios solicitados. Ningún punto del Apéndice 1 confiere ningún derecho ni impone ninguna obligación a las partes de este Anexo.

3. DERECHOS DE LOS INTERESADOS

3.1. CA debe, en la medida en que la ley lo permita, notificar de inmediato al Cliente si recibe una solicitud de un Interesado para ejercer su derecho de acceso, rectificación, limitación del tratamiento, supresión ("derecho al olvido"), portabilidad de los datos, oposición al tratamiento, o a no ser objeto de una decisión individual automatizada ("**Solicitud del interesado**"). Teniendo en cuenta la naturaleza del Tratamiento, CA debe ofrecer asistencia al Cliente mediante las medidas técnicas y organizativas apropiadas, en la medida de lo posible, para la consecución de la obligación del Cliente de dar respuesta a la Solicitud del interesado, según el Capítulo III del RGPD. Salvo en la medida en que la ley lo requiera, CA no responderá a ninguna Solicitud del interesado sin el consentimiento previo por escrito del Cliente, excepto para confirmar que la solicitud está relacionada con el Cliente.

3.2 Además, en la medida en la que el Cliente, en el uso de los Servicios, no tenga la capacidad de gestionar una Solicitud del interesado, CA debe, bajo petición del Cliente, realizar los esfuerzos comercialmente razonables para ofrecer asistencia al Cliente a la hora de responder a dicha Solicitud del Interesado, en la medida en la que CA tenga la capacidad legal de hacerlo y si dicha Solicitud del Interesado es necesaria conforme a las Leyes de Protección de Datos aplicables. Los costes que surjan de esta provisión de asistencia son responsabilidad del Cliente, en la medida en que la ley lo permita.

4. PERSONAL

4.1 CA debe garantizar que el personal involucrado en el Tratamiento de Datos Personales conozca el carácter confidencial de dichos datos, haya recibido la formación adecuada sobre sus responsabilidades y que esté sujeto a obligaciones de confidencialidad que se mantengan una vez que finalice la relación de estas personas con CA.

4.2 CA adoptará las medidas comercialmente razonables para garantizar la fiabilidad del personal de CA involucrado en el Tratamiento de Datos Personales.

4.3 CA garantizará que el acceso del Grupo CA a los Datos Personales esté limitado solo al personal necesario para cumplir el Acuerdo.

4.4 Delegado de Protección de Datos. Los miembros del Grupo CA han designado a un Delegado de protección de datos donde lo requieren las leyes en materia de protección de datos. La persona designada está disponible a través de la dirección de correo electrónico datatransfers@ca.com.

5. SUBENCARGADOS

5.1 El Cliente reconoce y acepta que (a) las Filiales de CA sean subencargados; y que (b) CA y las Filiales de CA puedan contratar, respectivamente, a terceros como subencargados, en relación con la prestación de los Servicios. Cualquiera de dichos subencargados estará autorizado para obtener datos personales solo con el fin de prestar los Servicios que ha acordado con CA, y no tendrá permiso para usar los datos personales para ningún otro fin.

5.2 CA será responsable de los actos y faltas de los Subencargados, en la misma medida en que CA sería responsable si realizara directamente los Servicios de cada Subencargado bajo las condiciones de este DPA, salvo que el Acuerdo establezca lo contrario.

5.3 CA o la Filial del Grupo CA correspondiente ha firmado un acuerdo por escrito con cada Subencargado que contiene obligaciones de protección de datos, que no son inferiores a las de este Anexo y que cumplen los requisitos del Artículo 28(3) del RGPD o las disposiciones equivalentes de otra ley de protección de datos aplicable, siempre que sean de aplicación a los Servicios suministrados por cada Subencargado.

5.4 El Cliente autoriza a CA y a las Filiales de CA a designar Subencargados de conformidad con la Cláusula 5. La lista de Subencargados de CA contratados para la prestación de los servicios se establece en el Apéndice 2; dicha lista incluye las identidades de los Subencargados y los países en los que se ubican ("**Lista de Subencargados**"). En caso de que CA realice algún cambio o añada información a dicha lista, la Lista de Subencargados actualizada estará a disposición del Cliente en el siguiente enlace: https://support.ca.com/us/product-content/admin-content/subprocessor-list.html; por tanto, se ofrece al Cliente la oportunidad de objetar dichos cambios (conforme se establece en la Cláusula 5.5).

5.5. El Cliente puede oponerse a que CA haga uso de un nuevo Subencargado mediante una notificación por escrito a CA en un plazo de diez (10) días hábiles a partir de la fecha de las modificaciones realizadas por CA en la Lista de Subencargados. En caso de que el Cliente se oponga, CA tomará medidas comercialmente razonables para afrontar las objeciones del Cliente y ofrecerle una explicación por escrito con las medidas tomadas para abordar dicha objeción.

5.6. Transferencias de datos. CA no transferirá datos personales del Cliente excepto si así lo exige la ley, y lo hará conforme a las Leyes de Protección de Datos aplicables. Los datos personales se transferirán de conformidad con la declaración y las condiciones de CA, que se recogen en https://www.ca.com/es/legal/privacy/data-transfers.html. Con el único fin de prestar los Servicios al Cliente de conformidad con el Acuerdo y sujeto a la Cláusula 5.6, el Cliente autoriza a CA a realizar transferencias rutinarias de Datos Personales a la entidad local del Grupo CA o a los Subencargados aprobados por CA. No obstante lo anterior, en caso de que los Datos Personales del Cliente se transfieran desde la Unión Europea, el Espacio Económico Europeo y/o sus estados miembros, Suiza y el Reino Unido, a países que no garanticen un nivel adecuado de protección de datos con respecto a las leyes de Protección de Datos de los citados territorios ("**Transferencias Restringidas**"), CA cumple con lo dispuesto en esta Cláusula 5.6(a) con respecto a las Transferencias Restringidas.

(a) **Mecanismos de transferencia para Transferencias Restringidas.** CA dispone de los mecanismos de transferencia que se enumeran a continuación, que se aplicarán con respecto a las Transferencias Restringidas realizadas al amparo de este DPA, en la medida en que dichas transferencias estén sujetas a las Leyes de Protección de Datos:

(1) **Autocertificación "Privacy Shield"**. La matriz estadounidense de CA ha certificado su cumplimiento del programa Privacy Shield UE-EE. UU y conservará

su certificación mientras conserve datos personales del EEE. En caso de que las autoridades europeas o los tribunales determinen que el "Privacy Shield" no es un principio adecuado para realizar transferencias, las partes deberán suscribri de inmediato las Cláusulas Contractuales Tipo de la UE aprobadas (para encargados del Tratamiento), que se incorporarán a este documento tras su firma.

(2) **Cláusulas Contractuales tipo de la UE**. CA y las Filiales de CA actuando como Subencargados (conforme al Listado del Apéndice 2) han firmado previamente las Cláusulas Contractuales Tipo de la UE relativas a la relación entre el responsable y el encargado del tratamiento y en beneficio del Cliente.

En caso de que los Servicios estén cubiertos por más de un mecanismo de transferencia, la transferencia de datos personales del Cliente estará sujeta a un único mecanismo de acuerdo con el siguiente orden de preferencia: (i) Autocertificación "Privacy Shield", (ii) Cláusulas Contractuales Tipo de la UE.

6. SEGURIDAD

6.1. Teniendo en cuenta la innovación, los costes de implementación y la naturaleza, alcance, contexto y objetivos del Tratamiento, así como el riesgo y la gravedad para los derechos y libertades de las personas físicas, el Cliente y CA adoptarán las medidas técnicas y organizativas correspondientes para garantizar un nivel de seguridad adecuado al riesgo. CA mantendrá una serie de medidas técnicas y organizativas apropiadas para la protección de la seguridad, la confidencialidad y la integridad de los datos, que cumplan los requisitos del encargado del tratamiento de conformidad con el RGPD, tal y como se establece en el Apéndice 2, "Seguridad del Tratamiento - Artículo 32 del RGPD". CA monitoriza de forma regular el cumplimiento de estas medidas de seguridad. CA no reducirá de forma sustancial la seguridad general de los Servicios durante el periodo de prestación de los mismos, de conformidad con el Acuerdo aplicable o con el formulario de pedido correspondiente.

6.2 Previa solicitud por escrito del Cliente en intervalos razonables, CA ofrecerá una copia de las certificaciones o auditorías más recientes de terceros, conforme sea aplicable, o resúmenes de éstas, relacionadas con el Tratamiento de los Datos Personales del Cliente. CA pondrá a disposición del Cliente, previa solicitud por escrito, la información necesaria para demostrar el cumplimiento de este Anexo, y permitirá que las solicitudes por escrito de auditoría realizadas por el Cliente o por un auditor independiente en relación con el Tratamiento de Datos Personales, comprueben que CA tiene establecidos procedimientos razonables de conformidad con este Anexo; ello siempre que el Cliente no haga ejercicio de este derecho más de una vez al año. Estos derechos de información y auditoría se establecen en esta Cláusula, en la medida en que el Acuerdo no garantice los derechos de auditoría que satisfagan los requisitos de las Leyes de Protección de Datos (incluido, si se aplica, el Artículo 28(3)(h) del RGPD). La información ofrecida por CA o las auditorías proporcionadas de conformidad con esta Cláusula, están sujetas a las obligaciones de confidencialidad establecidas en el Acuerdo.

6.3 CA ofrecerá al Cliente la asistencia razonablemente necesaria para cumplir con la obligación del Cliente de realizar una evaluación del impacto de la protección de datos conforme se establece en los Artículos 35 o 36 del RGPD, en relación con el uso de los Servicios por parte del Cliente. CA ofrecerá dicha asistencia previa solicitud del Cliente y en la medida en que el Cliente no tenga acceso a la información relevante, así como en la medida en que esta información esté a disposición de CA. De forma adicional, CA ofrecerá asistencia razonable al Cliente en la cooperación o consulta previa con la Autoridad de Control durante el desempeño de las tareas relacionadas con esta Cláusula 6.3, en la medida en que el RGPD lo permita.

7. NOTIFICACIÓN Y GESTIÓN DE LAS INFRACCIONES DE SEGURIDAD

7.1 CA notificará de inmediato al Cliente si descubre una destrucción ilegal o accidental, pérdida, alteración, divulgación no autorizada o acceso ilegal a los Datos Personales del Cliente transmitidos, almacenados o tratados por CA o sus Subencargados ("**Infracción de Seguridad**"). CA adoptará las medidas oportunas para identificar la causa de dicha Infracción de Seguridad y procederá de inmediato a: (a) Investigar la Infracción de Seguridad y ofrecer al

Cliente información sobre esta, incluido, si procede, la información que el Encargado del Tratamiento debe proporcionar al Responsable del Tratamiento según lo establecido en el Artículo 33(3) del RGPD, en la medida en que esta información esté disponible; y (b) adoptar las medidas necesarias para reducir los efectos y minimizar los daños causados por la Infracción de Seguridad, siempre y cuando las medidas correctivas estén bajo el control de CA. Las obligaciones establecidas en el presente documento no se aplicarán a las infracciones causadas por el Cliente o los Usuarios Autorizados. La notificación se enviará al Cliente de acuerdo con la Cláusula 7.3.

7.2 La obligación de CA de informar y responder ante una Infracción de Seguridad conforme se establece en esta Cláusula no es ni será entendida como una aceptación por parte de CA de ningún fallo o responsabilidad con respecto a la Infracción de Seguridad.

7.3. Las notificaciones de Infracciones de Seguridad, si las hubiera, se enviarán a uno o más contactos administrativos, técnicos o empresariales del Cliente a través de los medios elegidos por CA, incluido el correo electrónico. Es obligación del Cliente asegurarse de que mantiene información de contacto precisa y actualizada en los sistemas de soporte de CA en todo momento.

8. DEVOLUCIÓN Y SUPRESIÓN DE DATOS DEL CLIENTE

8.1 CA devolverá los Datos del Cliente a éste o los suprimirá de acuerdo con los procedimientos de CA y las Leyes de Protección de Datos y en consonancia con las condiciones del Acuerdo.

8.2 Previa solicitud del Cliente, CA suprimirá o devolverá todos los Datos Personales al Cliente una vez finalizada la prestación de los Servicios relacionados con el Tratamiento, y suprimirá todas las copias existentes, de acuerdo con los procedimientos establecidos en el Apéndice 2, "Seguridad del Tratamiento- Artículo 32 del RGPD", a menos que las Leyes de Protección de Datos requieran el almacenamiento de los Datos Personales.

9. CONDICIONES ADICIONALES PARA LOS DATOS PERSONALES DE LA UE

9.1 Las Cláusulas Contractuales Tipo y las condiciones adicionales de esta Cláusula 9 se aplicarán al Tratamiento de Datos Personales por parte de CA en el transcurso de la prestación de los Servicios.

> **9.1.1** Las Cláusulas Contractuales Tipo solo se aplican a los datos personales que se transfieran desde el Espacio Económico Europeo (EEE) o Suiza hasta zonas fuera del EEE o Suiza, tanto de forma directa como mediante transferencias ulteriores, a cualquier país o destinatario: (i) cuyo nivel de protección de datos personales no esté considerado como adecuado por la Comisión Europea (como se describe según la Ley de Protección de Datos aplicable), y (ii) que no se encuentre dentro de un marco apropiado reconocido por las autoridades o tribunales pertinentes, de forma que proporcionen un nivel de protección adecuado de los datos personales, lo que incluye, sin limitación, las Normas Corporativas Vinculantes para los Encargados del Tratamiento.
>
> **9.1.2** Las Cláusulas Contractuales Tipo se aplican a (i) la entidad legal que ha suscrito dichas Cláusulas como Exportador de Datos, y (ii) a todas las Filiales (conforme se definen en el Acuerdo) del Cliente establecidos dentro del Espacio Económico Europeo (EEE) y Suiza que hayan adquirido Servicios sobre la base de un pedido realizado al amparo del Acuerdo. A efectos de las Cláusulas Contractuales Tipo y de esta Cláusula 9, el Cliente y sus Filiales se considerarán "Exportadores de Datos".

9.2 Este DPA y el Acuerdo son las instrucciones completas y finales del Exportador de Datos para el Importador de Datos relativas al Tratamiento de Datos Personales. Cualquier instrucción adicional o alternativa debe acordarse de forma separada. A efectos de la Cláusula 5(a) de las Cláusulas Contractuales Tipo, lo que sigue a continuación se consideran instrucciones del Exportador de Datos para Tratar Datos Personales: (a) de conformidad con el Acuerdo

y los pedidos aplicables; y (b) con arreglo a otras instrucciones suministradas por el Cliente (p. ej., a través de un ticket de soporte) que sean coherentes con las condiciones del Acuerdo.

9.3 A efectos de la Cláusula 5(h) de las Cláusulas Contractuales Tipo, el Exportador de Datos reconoce y acepta que (a) las Filiales de CA se mantengan como Subencargados; y que (b) CA y sus Filiales contraten respectivamente a terceros como Subencargados, en relación con la prestación de los Servicios. Los Importadores de Datos pondrán a disposición del Cliente la lista actualizada de los Subencargados para los respectivos Servicios, debidamente identificadas de acuerdo con la Cláusula 5.5 de este DPA.

9.4 Las partes acuerdan que las copias de los acuerdos con los Subencargados que debe enviar el Importador de Datos al Exportador de Datos conforme a la Cláusula 5(j) de las Cláusulas Contractuales Tipo es posible que no incluyan clausulado o disposiciones que no estén relacionadas con las Cláusulas Contractuales Tipo o sus equivalentes, que habrán sido previamente suprimidas por el Importador de Datos. El Importador de Datos únicamente proporcionará dichas copias previa solicitud del Exportador de Datos.

9.5 Las partes acuerdan que las auditorías establecidas en las Cláusulas 5(f), 11 y 12(2) de las Cláusulas Contractuales Tipo se realizarán de acuerdo con las siguientes especificaciones: Previa solicitud del Exportador de Datos y sujeto a las obligaciones de confidencialidad establecidas en el Acuerdo, el Importador de Datos, dentro de un periodo razonable de tiempo tras la solicitud, pondrá a disposición del Exportador de Datos (o del auditor externo independiente del Exportador Datos que no sea un competidor de CA) la información relativa al cumplimiento del Grupo CA con las obligaciones establecidas en este DPA, en forma de certificaciones y auditorías de terceros realizadas según lo descrito en el Acuerdo y/o en el Documento de Prácticas de Seguridad, en la medida en que CA ponga a disposición de sus clientes dicha información. El Cliente puede ponerse en contacto con el Importador de Datos de acuerdo con la Cláusula "Notificaciones" del Acuerdo para solicitar una auditoría in situ de los procedimientos relacionados con la protección de los Datos Personales. El Cliente reembolsará al Importador de Datos por el tiempo invertido en la auditoría in situ conforme a lo honorarios previstos para los servicios profesionales del Grupo CA, que se proporcionarán al Exportador de Datos previa solicitud. Antes del comienzo de una auditoría in situ, el Exportador y el Importador de Datos acordarán mutuamente el alcance, los plazos y la duración de la auditoría, así como el importe de los honorarios de reembolso de los que se hará cargo el Exportador de Datos. Todos los honorarios serán razonables, teniendo en cuenta los recursos invertidos por parte del Importador de Datos. El Exportador de Datos notificará con carácter inmediato al Importador la información relativa a las disconformidades descubiertas en el transcurso de la auditoría.

9.6 Las partes acuerdan que el Importador de Datos solo ofrecerá la certificación de supresión de datos personales descrita en la Cláusula 12(1) al Exportador de Datos previa solicitud de este último.

9.7 En caso de que exista algún tipo de conflicto o incoherencia entre este DPA y las Cláusulas Contractuales Tipo, prevalecerán estas últimas.

10. PARTES DE ESTE DPA

10.1 Limitación de responsabilidad. La responsabilidad de cada parte y sus Filiales en conjunto, resultante o relacionada con este DPA, y de todos los DPAs entre Filiales Autorizadas y CA, se regulará por la Cláusula "Limitación de Responsabilidad" del Acuerdo que rige los Servicios pertinentes; las referencias en dicha Cláusula a la responsabilidad de una de las partes se refiere a la responsabilidad total de dicha parte y de todas sus Filiales al amparo del Acuerdo y los DPAs conjuntamente. Para evitar cualquier duda, las referencias al DPA incluidas en el presente documento se refieren a este DPA, incluidos los Anexos y Apéndices adjuntos.

10.2 Filiales Autorizadas y Relaciones Contractuales. Mediante la suscripción de este DPA, el Cliente lo suscribe en su nombre y, en la medida en que las Leyes de Protección de Datos aplicables lo requieran, en nombre y por cuenta de sus Filiales Autorizadas, en la medida en que CA realice el Tratamiento de Datos Personales en los que dichas

Filiales Autorizadas estén consideradas Responsables del Tratamiento. Las Filiales Autorizadas aceptan cumplir las obligaciones de este DPA y, en la medida en que sea aplicable, del Acuerdo. Para evitar cualquier duda, las Filiales Autorizadas no son ni se convierten en una parte del Acuerdo; solo son parte del DPA. El acceso y el uso de los Servicios por parte de las Filiales Autorizadas debe cumplir con los términos y condiciones del Acuerdo; cualquier vulneración de las condiciones del Acuerdo por parte de las Filiales Autorizadas se considerará un incumplimiento por parte del Cliente. Exclusivamente a efectos de este DPA, el término "Cliente" incluirá al Cliente y a las Filiales Autorizadas , si no se indica lo contrario.

10.2.1 Comunicación. El Cliente que es la parte contratante del Acuerdo, será responsable de coordinar toda la comunicación con CA con respecto a este DPA y estará autorizado para realizar y recibir comunicaciones relacionadas con este DPA en nombre de sus Filiales Autorizadas.

10.2.2 Derechos de las Filiales Autorizadas. Si una Filial Autorizada se convierte en parte del DPA con CA, estará autorizada, en la medida en que lo exijan las Leyes de Protección de Datos aplicables, para ejercer sus derechos y presentar recursos bajo este DPA, sujeto a los siguientes puntos:

10.2.2.1 Excepto en el caso en que las Leyes de Protección de Datos Aplicable requieran que la Filial Autrizada ejerza un derecho o presente una reclamación de forma directa al amparo de este DPA frente a CA, las partes aceptan que (i) solo el Cliente que constituya parte contratante del Acuerdo ejercerá sus derechos o presentará recursos en nombre de la Filial Autorizada, y que (ii) el Cliente que constituya la parte contratante del Acuerdo ejercerá sus derechos bajo este DPA no de forma individual para cada Filial Autorizada, sino de forma conjunta para todas las Filiales Autorizadas.

11. DEFINICIONES

"Filiales de CA": en relación con CA, cualquier entidad que esté controlada por ésta, que la controle, o que controle conjuntamente con CA.

"CA": entidad del Grupo CA que constituye una parte de este DPA.

"Grupo CA": conjunto de CA y sus Filiales involucradas en el Tratamiento de Datos Personales.

"Filial Autorizada": cualquier Filial del Cliente que (a) está sujeta a las Leyes de Protección de Datos de la Unión Europea, del Espacio Económico Europeo y/o de los estados miembros, Suiza o el Reino Unido, y (b) este autorizada para usar los Servicios conforme al Acuerdo entre el Cliente y CA, pero no han firmado su propio Formulario de Pedido con CA y no es un "Cliente" conforme se define en el Acuerdo. Exclusivamente a efectos de este DPA, el término "Cliente" incluirá al Cliente y a las Filiales Autorizadas, si no se indica lo contrario. Para evitar cualquier duda, **"Filial Autorizada del Cliente"** hace referencia a cualquier entidad legal que el Cliente, directa o indirectamente controla o es propietario mayoritario, mediante la titularidad de la mayoría del capital social.

"Responsable del Tratamiento", "Encargado del Tratamiento", "Interesado", "Comisión", "Estado Miembro" y "Autoridad de Control": tendrán el mismo significado que en el Capítulo 1, Artículo 4 del RGPD y sus términos afines se interpretarán de forma acorde a dicho significado.

"Leyes de Protección de Datos": todas las leyes y normativas aplicable al Tratamiento de Datos Personales bajo el Acuerdo, lo que incluye las leyes y normativa de la Unión Europea, del Espacio Económico Europeo y sus estados miembros (incluido el RGPD, definido a continuación).

"RGPD": Reglamento General de Protección de Datos 2016/679 de la Unión Europea (*Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

"Datos Personales": cualquier información relacionada con (i) una persona física identificada o identificable y (ii) una persona jurídica identificada o identificable (donde dicha información se protege de forma similar a los datos personales o la información personal identificable bajo las Leyes de Protección de Datos), donde, tanto en (i) como en (ii), dichos datos son datos del Cliente (según se define en el Acuerdo aplicable) proporcionados de conformidad con el Acuerdo.

"Tratamiento": operación o conjunto de operaciones realizadas con los datos personales, ya sea con medios automáticos o no, como la recopilación, registro, organización, almacenamiento, adaptación o modificación, recuperación, consulta, uso, divulgación mediante transmisión, distribución o cualquier forma de puesta a disposición, alineación o combinación, bloqueo, supresión o destrucción ("Tratamiento", "Tratamientos" y "Tratado" tienen el mismo significado).

"Infracción de Seguridad": tiene el significado que se establece en la Cláusula 7 de este Anexo.

"Documento de Prácticas de Seguridad": Significa el documento titulado "Information Security Practices Document" o la parte que sea de aplicación en función del Servicio de CA que adquiera el Cliente; se actualiza de forma periódica y está disponible a través del enlace https://www.ca.com/content/dam/ca/us/files/supportingpieces/ca-information-security-practices.pdf, o adjunto al Acuerdo entre CA y el Cliente.

"Apéndice de Seguridad": significa las medidas de seguridad organizativas y técnicas implementadas por CA para la protección de los Datos Personales, establecidas en el Apéndice 2, "Seguridad del Tratamiento - Artículo 32 del RGPD". En caso de que existan contradicciones entre las condiciones del Documento de Prácticas de Seguridad de CA y las condiciones del Apéndice de seguridad, las condiciones del Apéndice 2 sobre seguridad prevalecen con respecto a las medidas de seguridad y a la protección de los Datos Personales, conforme a los requisitos del RGPD.

"Servicios": significa la prestación de servicios de mantenimiento y soporte técnico y/o servicios profesionales o de consultoría y/o el suministro de software como un servicio ("SaaS") y/o cualquier otro servicio prestado bajo el Acuerdo en el que CA Trate Datos Personales del Cliente.

"Cláusulas Contractuales Tipo": acuerdo recogido en la decisión de la Comisión Europea de 5 de febrero de 2010 sobre Cláusulas Contractuales Tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen un nivel adecuado de protección de datos.

"Subencargado": significa cualquier Encargado del Tratamiento contratado por CA o por una entidad perteneciente al Grupo CA.

Lista de Apéndices adjuntos
Apéndice 1: Información sobre el Tratamiento de Datos Personales del Cliente
Apéndice 2: Seguridad del Tratamiento - art. 32 del RGPD

En virtud de todo lo anterior se formaliza este DPA y se convierte en parte vinculante del Acuerdo entre el Cliente y CA, a partir de la fecha de entrada en vigor. Si las partes han firmado este documento de forma electrónica, dicha firma tiene la misma validez legal que una firma manuscrita.

Acordado en nombre y por cuenta de CA	Acordado en nombre y por cuenta del Cliente
Entidad de CA_____	**Entidad del Cliente:**_____
Firmado:_____	**Firmado:**_____
Nombre:_____	**Nombre:**_____
Título:_____	**Título:**_____
Fecha:_____	**Fecha:**_____

APÉNDICE 1: INFORMACIÓN SOBRE EL TRATAMIENTO DE DATOS PERSONALES DEL CLIENTE

Este Apéndice 1 incluye cierta información sobre el Tratamiento de los Datos Personales del Cliente, de conformidad con el artículo 28(3) del RGPD (o según proceda, disposiciones equivalentes de cualquier otra Ley de Protección de Datos).

Objeto y duración del Tratamiento de los Datos Personales del Cliente

El objeto y la duración del Tratamiento de los Datos Personales del Cliente se recoge en el Acuerdo principal y en este Anexo.

Naturaleza y finalidad del Tratamiento de los Datos Personales del Cliente

Naturaleza:

- ☒ Recopilación
- ☒ Registro
- ☐ Divulgación
- ☒ Eliminación
- ☐ Alteración
- ☐ Restricción
- ☒ Uso

Finalidad:
Los datos personales del Cliente se utilizan para proporcionar Soporte o SaaS de conformidad con lo recogido en el Acuerdo principal.

Tipos de Datos Personales del Cliente que se Tratan

Datos del Cliente de personas físicas	☒
Datos del Cliente de empresas	☒
Datos de empleados	☒
Otros datos personales	☐

Categorías de Datos Tratados respecto de los Interesados

Categorías especiales de datos personales (art. 9 del RGPD)

Salud/Vida sexual	☐
Afiliación a sindicatos	☐
Creencias religiosas o filosóficas	☐
Opiniones políticas	☐
Origen racial/étnico	☐

Derechos y obligaciones del Cliente y de los afiliados del Cliente

Los derechos y obligaciones del Cliente y de las Filiales del Cliente se recogen en el Acuerdo y en el DPA, incluidos cualquier Apéndice, o documento adjunto al mismo.

APÉNDICE 2. SEGURIDAD DEL TRATAMIENTO - ART. 32 DEL RGPD

Introducción

Si se tienen en cuenta la innovación, los costes de implementación y la naturaleza, alcance, contexto y objetivos del tratamiento, así como el riesgo y la gravedad para los derechos y libertades de las personas físicas, el Responsable del Tratamiento y el Encargado del Tratamiento adoptarán las medidas técnicas y organizativas correspondientes para garantizar un nivel de seguridad adecuado al riesgo según proceda, incluyento, entre otras:

§ 1 Medidas técnicas y organizativas adoptadas para garantizar un nivel de seguridad adecuado (SaaS e *in situ*)

(1a) Medidas sobre la **seudonimización/anonimización** de los datos personales:
La naturaleza de los datos almacenados en este producto no suele requerir la seudonimización ni la anonimización. En caso necesario, el Cliente debe solicitarlo/escalarlo a CA. ***In situ*:** No aplicable

(1b) Medidas sobre el **cifrado** de los datos personales:
CIFRADO Todos los datos están cifrados en tránsito mediante TLS compatible con 1.0, 1.1 (se discontinuará) y actualmente con 1.2. Además, los datos del Cliente están cifrados en cualquier servidor o dispositivo que se haya retirado de las instalaciones de CA para la creación de copias de seguridad o el almacenamiento fuera de las instalaciones (cuando corresponda). Se emplean procedimientos de gestión de claves que garantizan la confidencialidad, integridad y disponibilidad de claves criptográficas. El uso de productos de cifrado cumple las restricciones locales y los reglamentos sobre el uso del cifrado en la jurisdicción pertinente. Política de cifrado La política de seguridad de los datos que dicta el cifrado está documentada. El nivel de cifrado de los datos del Cliente en transmisión aparece definido. Gestión de Claves de Cifrado Los procedimientos de gestión de las claves criptográficas están documentados y automatizados. Se implementan productos o soluciones para que las claves de cifrado de los datos permanezcan cifradas (p. ej., soluciones basadas en software, módulos de seguridad de hardware [HSM]). Usos del Cifrado La transmisión de los datos del Cliente a través del Internet público utiliza siempre un canal cifrado. Los detalles del cifrado están documentados si la transmisión se realiza de manera automatizada. El personal aprobado y especializado es responsable del cifrado y descifrado de los datos, en caso de realizarse de manera manual. Los datos del Cliente también deben estar cifrados mientras estén en tránsito por cualquier red. Las transmisiones VPN se realizan a través de un canal cifrado. ***In situ*:**

El Responsable del Tratamiento proporciona datos de los casos de soporte de manera cifrada al encargado del tratamiento. Los casos se resuelven en un entorno seguro. Los datos de los casos de soporte se eliminan a los 30 días del cierre del caso

(1c) Medidas para garantizar la **confidencialidad permanente** de los datos personales:

Todos los accesos a los centros de datos en los que están almacenados los datos del Cliente están limitados al equipo de operaciones de CA, de conformidad con las Políticas de control de accesos a la información de CA y la Política de segregación de funciones de CA (CA se rige por el principio de privilegios mínimos y solo concede acceso con base en la función y el caso práctico de negocio). Los derechos de acceso se revisan con regularidad o tras el cambio de función/cese de un empleado. El acceso al entorno en el que se almacenan los datos del Cliente está estrictamente controlado y monitorizado. El Cliente es responsable de gestionar el acceso a sus datos de suscripción, así como el ciclo de vida de dichas cuentas. Los administradores de la suscripción del Cliente son responsables de las políticas de administración de usuarios y contraseñas relacionadas dentro de la aplicación.
El Cliente es responsable del ciclo de vida de esta cuenta.

***In situ*:**
El trabajo se realiza en entornos seguros; la transferencia de datos está protegida. Eliminación de los datos tras el cierre del caso de soporte.

(1d) Medidas para garantizar la **integridad permanente** de los datos personales:

INTEGRIDAD DE LOS DATOS
Las políticas y los procedimientos de CA Technologies están diseñados para garantizar que todos los datos almacenados, recibidos, controlados o usados no se hayan puesto en peligro y permanezcan intactos. Los procedimientos de inspección permiten validar la integridad de los datos.
Controles de transmisión de datos
Los procesos y procedimientos de control de la transmisión de datos para garantizar la integridad de los datos están documentados. “Check sums” y recuentos se emplean para validar que los datos transmitidos sean los mismos que los recibidos.
Control de la transacción de datos
Los controles para evitar o identificar las transacciones duplicadas en los mensajes financieros están documentados. Los certificados digitales (p. ej., firmas digitales, de servidor a servidor) empleados para garantizar la integridad de los datos durante la transmisión siguen un proceso y un procedimiento documentado.

***In situ*:**
No aplicable; los datos se eliminan después del cierre del caso de soporte, véase la Cláusula 2 apartados del a) al e).

(1e) Medidas para garantizar la **disponibilidad permanente de los sistemas y servicios de tratamiento:**

CONTROL DE DISPONIBILIDAD

- Protección contra incendios y medidas en caso de fallos eléctricos en los centros de tratamiento de datos, incluidas las copias de seguridad

Controles Físicos

CA Technologies cuenta con controles eficaces que protegen contra el acceso físico de personas maliciosas o no autorizadas. Los controles físicos aplicados a toda la instalación están documentados. Se aplican restricciones de acceso adicionales para los servidores/equipos/salas de telecomunicaciones, en comparación con el área general.

Copias de seguridad y Almacenamiento fuera de las Instalaciones

CA Technologies cuenta con una política de copias de seguridad definida y con procedimientos asociados para la creación de copias de seguridad de los datos de manera programada y oportuna. Los controles eficaces se establecen para proteger los datos de copia de seguridad (dentro y fuera de las instalaciones). CA Technologies también garantiza que los datos del Cliente se transfieran o se transportarán de manera desde y hasta las ubicaciones de copia de seguridad. Además, CA Technologies realiza pruebas periódicas para garantizar que los datos se puedan recuperar de manera segura de los dispositivos de copia de seguridad.

Proceso de Copia de Seguridad

Los procedimientos para las copias de seguridad y el almacenamiento fuera de las instalaciones están documentados. Los procedimientos comprenden la recuperación completa de aplicaciones y sistemas operativos. Las pruebas periódicas para la correcta recuperación de los medios de copia de seguridad han sido probadas. El área de preparación dentro de las instalaciones cuenta con controles ambientales documentados y probados (p. ej., humedad, temperatura).

Destrucción de Medios de Copia de Seguridad

Los procedimientos se definen para formar al personal sobre los métodos adecuados para destruir los medios de copia de seguridad. La destrucción de medios de copia de seguridad por parte de terceros va acompañada de procedimientos documentados (p. ej., certificados de destrucción) para confirmar la destrucción.

Almacenamiento fuera de las Instalaciones

Los planes de seguridad físicos para la instalación externa están documentados. Los controles de acceso se realizan en los puntos de entrada y en las salas de almacenamiento. El acceso a la instalación externa está restringido y existe un proceso de aprobación para obtener acceso. La transmisión electrónica de los datos a una ubicación fuera de las instalaciones se realiza a través de un canal cifrado.

***In situ*:**

Entorno cerrado; no aplicable. Los datos permanecen con el responsable del tratamiento que exista.

(1f) Medidas para garantizar la **resiliencia permanente de los sistemas y servicios de tratamiento:**

MONITORIZACIÓN DE LA VULNERABILIDAD

CA Technologies recopila y analiza constantemente información sobre amenazas y vulnerabilidades nuevas y existentes, ataques reales a la institución u otros, y la eficacia de los controles de seguridad existentes. Los controles de monitorización afectan a las políticas y procedimientos relacionados, los virus y códigos malintencionados, la detección de intrusiones

y la monitorización de eventos y estados. El proceso de registro relacionado ofrece un control eficaz para destacar e investigar eventos de seguridad.
Política y Procedimiento de Vulnerabilidad
Se realizan pruebas de acceso/vulnerabilidad de las redes internas/externas o hosts específicos. Las pruebas suele realizarlas de manera externa una reputada organización ajena. Se incluyen los entornos del Cliente como parte del alcance de las pruebas. Todas las cuestiones consideradas de alto riesgo se resuelven en plazos adecuados.
Antivirus y Código Malintencionado
Los servidores, las estaciones de trabajo y los "gateways" de Internet se actualizan de manera periódica con las últimas definiciones de antivirus. El procedimiento definido subraya todas las actualizaciones de antivirus. Las herramientas antivirus están configuradas para realizar análisis semanales, detecciones de virus y actualizaciones de actividades de escritura de archivos en tiempo real y de archivos de firmas. Los portátiles y los usuarios remotos están incluidos en la protección antivirus. Los procedimientos para detectar y eliminar las aplicaciones no autorizadas o incompatibles (p. ej., software gratuito) están documentados.
Los eventos de alerta incluyen los siguientes atributos:
Identificador único
Fecha
Tiempo
Identificador del nivel de prioridad
Dirección IP de origen
Dirección IP de destino
Descripción del evento
Notificación enviada al equipo de seguridad
Estado del evento
Monitorización de eventos de seguridad
Los eventos de seguridad se registran (archivos de registro), monitorizan (personas adecuadas) y abordan (medidas documentadas y adoptadas de manera oportuna). Los componentes de la red, las estaciones de trabajo, las aplicaciones y todas las herramientas de monitorización se habilitan para monitorizar la actividad del usuario. Las responsabilidades organizativas para responder a eventos se definen. Las herramientas de comprobación de la configuración se utilizan (o se utilizan otros registros) y registran cambios críticos en la configuración del sistema. El permiso de registro restringe las modificaciones que pueden hacer los administradores. La programación de retención para varios registros se define y cumple.

(1g) Medidas para recuperar **la disponibilidad y el acceso a los datos personales en caso de una incidencia técnica o física:**

Véase anteriormente CONTROL DE DISPONIBILIDAD
RESPUESTA ANTE INCIDENCIAS
CA Technologies documenta un plan y procedimientos asociados en caso de que se produzca una incidencia relacionada con la seguridad de la información. El plan de respuesta ante incidencias articula claramente las responsabilidades del personal e identifica a las partes de notificación pertinentes. El personal de respuesta ante incidencias recibe formación. La aplicación del plan de respuesta ante incidencias se comprueba de manera periódica.

Proceso de Respuesta ante Incidencias
La política y los procedimientos de gestión de incidencias relacionadas con la seguridad de la información están documentados. La política o los procedimientos de gestión de incidencias incluyen los siguientes atributos:
• La definición de la estructura organizativa
• La identificación del equipo de respuesta
• La documentación de la disponibilidad del equipo de respuesta
• La documentación de plazos para la detección y divulgación de incidencias
• La definición del ciclo de vida del proceso de incidencias incluye los siguientes pasos discretos:
  • Identificación
  • Asignación de la gravedad de cada incidencia
  • Comunicación
  • Resolución
  • Formación
  • Pruebas (frecuencia de las comprobaciones)
  • Generación de informes
• Las incidencias se deben clasificar y priorizar
• Los procedimientos de respuesta ante incidencias deben incluir notificaciones del Cliente al gestor de relaciones (entrega) u otro contacto enumerado en el contrato
Comunicación/Notificación
El proceso de respuesta ante incidencias se inicia tan pronto como CA Technologies tenga constancia de la incidencia (independientemente de la hora).

***In situ*:**
Solo parcialmente aplicable; los datos se eliminan después del cierre del caso de soporte.

(1h) Medidas para **la comprobación, el análisis y la evaluación de la eficacia de las medidas técnicas y organizativas:**

CONTROL ORGANIZATIVO
OPERACIONES
CA Technologies ha documentado procedimientos operativos de TI para garantizar que el funcionamiento de los activos de TI sea correcto y seguro.

Procedimientos Operativos y Responsabilidades.
Los procedimientos operativos se documentan en un manual de operaciones y se aplican correctamente.
El manual de operaciones incluye los siguientes componentes:
Requisitos de planificación
Errores de tratamiento (p. ej., transporte de los datos, impresión, copias)
Generación y tratamiento de resultados especiales
Mantenimiento y detección de problemas de los sistemas
Procedimientos documentados para gestionar los SLA/KPI y la estructura de generación de informes para escalaciones

Se realizan auditorías de seguridad internas de manera regular al encargado del tratamiento, incluido el delegado (externo) de protección de datos

§ 2 Delegados de Protección de Datos

Nombre:	Datos de contacto:
Bonnie Yeomans	CA, Inc. 520 Madison Avenue Nueva York, NY 10022 Asesor general adjunto y delegado de privacidad
Yasmin Brook	CA Deutschland GmbH Marienburgstr. 35 64297 Darmstadt Alemania Asesor principal y delegado de privacidad de campo mundial

§ 3 Se conserva una lista actual de subencargados en https://support.ca.com/us/product-content/admin-content/subprocessor-list.html

§ 4 Entidades de CA que ofrecen soporte y mantenimiento en virtud del Acuerdo

Entidades de CA		
Nombre	**Datos de contacto**	**Ubicación**
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	Bélgica
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	Brasil
CA Canada Company	2700 Matheson Blvd East, Suite 800E, Mississauga, Ontario, L4W 5M2, Canada	Canadá
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	República Checa
CA Software ApS	Borupvang 5B, DK - 2750, Ballerup, Denmark	Dinamarca
CA Limited (formerly CA Plc and fomerly Computer Associates Plc)	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inglaterra
CA Technology R&D Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inglaterra
Computer Associates Holding Ltd.	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inglaterra
Computer Associates UK Limited	Ditton Park, Riding Court Road, Datchet, Slough, Berkshire, UK, SL3 9LL	Inglaterra
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	Alemania
CA Computer Associates Holding GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Alemania

CA Computer Associates Technology GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Alemania
CA Deutschland GmbH	Marienburgstrasse 35,64297 Darmstadt, Germany	Alemania
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)	Italia
CA Japan, Ltd.	JA Kyosai Bldg., 2-7-9 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093, Japan	Japón
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	México
CA Software de Mexico, S.A. de C.V	véase anteriormente	México
CA Europe Holding B.V.	Orteliuslaan 1001, 3528 BE, Utrecht, Netherlands	Países Bajos
CA software BV	véase anteriormente.	Países Bajos
CA Software Holding BV	Véase anteriormente.	Países Bajos
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	España