CONTRATO DE TRATAMIENTO DE DATOS PERSONALES PARA LOS SERVICIOS CLOUD DE SAP

1. ANTECEDENTES

1.1 **Finalidad y Aplicación.** Este documento ("**DPA**") se integra en el Contrato y pasa a formar parte de un contrato escrito (incluyendo formato electrónico) entre SAP y el Cliente. Este DPA se aplica a los Datos Personales procesados por SAP y sus Subencargados en relación con la prestación del Servicio Cloud. Este DPA no se aplica a los ambientes no productivos del Servicio Cloud si es SAP quien los pone a su disposición, y el Cliente no deberá almacenar Datos Personales en dichos entornos.

1.2 **Estructura.** Los Apéndices 1 y 2 se integran y pasan a formar parte de este DPA. Especifican el objeto acordado, la naturaleza y el propósito del procesamiento, el tipo de Datos Personales, las categorías de los titulares y las medidas técnicas y organizativas aplicables.

1.3 **GDPR.** SAP y el Cliente acuerdan que es responsabilidad de cada una de las partes revisar y adherirse a los requisitos impuestos a los Responsables y los Encargados con base al Reglamento General de Protección de Datos 2016/679 (**GDPR**" por sus siglas en ingles); en especial en lo relativo a los Artículos 28 y 32 a 36 del GDPR, en la medida aplicable a los Datos Personales del Cliente/Responsable del Tratamiento que se tratan en el DPA. A modo de ejemplo, el Apéndice 3 enumera los requisitos del GDPR relevantes, así como las secciones correspondientes de este DPA.

1.4 **Control.** De conformidad con el DPA, SAP ejerce de Encargado y el Cliente y aquellas entidades a las que se les permite el uso del Servicio Cloud ejercen de Responsables. El Cliente actúa como punto de contacto único y su única responsabilidad es obtener las autorizaciones, consentimientos y permisos relevantes para el tratamiento de los Datos Personales, según lo especificado en este DPA, incluyendo, cuando sea aplicable la autorización por parte de los Responsables para utilizar SAP como Encargado. Cuando el Cliente proporciona su autorización, consentimiento, instrucciones o permisos, no lo hace solo en su nombre, sino también en el nombre de cualquier otro Responsable que utilice el Servicio Cloud. Cuando SAP informa o envía algún tipo de notificación al Cliente, se considerará que dicha información o notificación la reciben también los Responsables a los que el Cliente ha autorizado el uso del Servicio Cloud, y es responsabilidad del Cliente reenviar dicha información o notificación a los Responsables relevantes.

2. SEGURIDAD DEL TRATAMIENTO

2.1 **Medidas Técnicas y Organizativas Adecuadas.** SAP ha implementado y aplicará las medidas técnicas y organizativas especificadas en el Apéndice 2. El Cliente ha revisado estas medidas y acepta que, en lo relativo al Servicio Cloud elegido por el Cliente en el Formulario de Pedido, las medidas son adecuadas teniendo en cuenta la tecnología de punta , los costos de implementación, la naturaleza, el alcance, el contexto y los propósitos del tratamiento de los Datos Personales.

2.2 **Modificaciones.** SAP aplica las medidas técnicas y organizativas especificadas en el Apéndice 2 a toda la base de clientes de SAP que se encuentra alojada en el mismo Centro de Datos y recibiendo el mismo Servicio Cloud. SAP puede modificar las medidas especificadas en el Apéndice 2 en cualquier momento, sin previo aviso, siempre que mantenga un nivel de seguridad comparable o superior. Las medidas individuales pueden sustituirse por nuevas medidas que tengan la misma finalidad, siempre que no reduzcan el nivel de seguridad que protege los Datos Personales.

3. OBLIGACIONES DE SAP

3.1 **Instrucciones del Cliente.** SAP tratará los Datos Personales únicamente de conformidad con las instrucciones documentadas del Cliente. El Contrato (incluido este DPA) constituye dichas instrucciones iniciales documentadas y cada uso del Servicio Cloud constituirá instrucciones adicionales. SAP empleará los esfuerzos razonables para seguir cualquier otra instrucción del

Cliente, siempre y cuando la Ley de Protección de Datos así lo exija, sea técnicamente viable y no requiera realizar ninguna modificación en el Servicio Cloud. Si se aplica cualquiera de las excepciones anteriormente mencionadas, o SAP no puede cumplir una instrucción por algún motivo o considera que una instrucción infringe la Ley de Protección de Datos, SAP se lo notificará inmediatamente al Cliente (se permite por correo electrónico).

3.2 **Tratamiento de Requisitos Legales.** SAP también puede tratar los Datos Personales siempre que la ley aplicable así lo exija. En ese caso, SAP informará al Cliente de dicho requisito legal antes de llevar a cabo el tratamiento, salvo que esa ley específica prohíba informar por motivos relacionados con el interés público.

3.3 **Personal.** Para tratar Datos Personales, SAP y sus Subencargados solo proporcionarán acceso al personal autorizado que se haya comprometido a mantener la confidencialidad de los Datos Personales. SAP y sus Subencargados capacitarán periódicamente en las medidas aplicables de seguridad y privacidad de los Datos Personales, al personal con autorización para acceder a los Datos Personales.

3.4 **Cooperación.** A petición del Cliente, SAP cooperará de forma razonable con el Cliente y con los Responsables a atender las solicitudes de los Titulares o de autoridades supervisoras con respecto al tratamiento de Datos Personales por parte de SAP o en caso de Brecha de los Datos Personales. SAP notificará al Cliente tan pronto como le sea posible, cualquier solicitud que reciba de un Titular en relación con el tratamiento de los Datos Personales y no responderá a dicha solicitud antes de recibir instrucciones adicionales del Cliente, si estas son aplicables. SAP proporcionará funcionalidades que ayuden al Cliente a corregir o eliminar los Datos Personales del Servicio Cloud, o a restringir su tratamiento de conformidad con la Ley de Protección de Datos. Donde no se proporcione esta funcionalidad, SAP corregirá o eliminará dichos Datos Personales, o restringirá su tratamiento, de conformidad con las instrucciones del Cliente y la Ley de Protección de Datos.

3.5 **Notificación de Brecha de los Datos Personales.** SAP notificará al Cliente tan pronto como sea posible y después de haber tenido conocimiento de cualquier Brecha de los Datos Personales y le proporcionará toda la información razonable que posea, para ayudar al Cliente a cumplir sus obligaciones de notificar cualquier Brecha de los Datos Personales, según exige la Ley de Protección de Datos. SAP puede proporcionar esta información por fases, a medida que esté disponible. Este tipo de notificaciones no se interpretará como una admisión de culpa o responsabilidad por parte de SAP.

3.6 **Evaluación del Impacto de Protección de Datos.** Si, de conformidad con la Ley de Protección de Datos, el Cliente (o sus Responsables) se ven obligados a realizar una evaluación de impacto de protección de datos o una consulta previa con un regulador, previa petición del Cliente, SAP proporcionará dichos documentos, que según están disponibles de manera general para el Servicio Cloud (por ejemplo, este DPA, el Contrato, informes de auditoría o certificaciones). Cualquier ayuda adicional deberá ser acordada por las Partes.

4. EXPORTACIÓN Y ELIMINACIÓN DE DATOS

4.1 **Exportación y Recuperación por parte del Cliente.** Durante el Plazo de Suscripción, y sujeto al Contrato, el Cliente puede acceder a sus Datos Personales en cualquier momento. El Cliente puede exportar y recuperar sus Datos Personales en un formato estándar. La exportación y la recuperación pueden estar sujetas a limitaciones técnicas, en cuyo caso SAP y el Cliente buscarán un método razonable para permitir al Cliente el acceso a los Datos Personales.

4.2 **Eliminación.** Antes de que expire el Plazo de Suscripción, el Cliente puede usar las herramientas de autoservicio de exportación de SAP (según la disponibilidad) para realizar una exportación final de los Datos Personales, desde el Servicio Cloud (lo que constituiría una "devolución" de los Datos Personales). Al finalizar el Plazo de Suscripción, mediante el presente el Cliente indica a SAP que debe eliminar los Datos Personales que queden en los servidores que alojan el Servicio Cloud en un período de tiempo razonable conforme a la Ley de Protección de Datos (no debe exceder los seis meses), salvo que la ley aplicable exija su conservación.

5. CERTIFICACIONES Y AUDITORÍAS

5.1 Auditoría de Cliente. El Cliente, o su auditor externo independiente y razonablemente aceptable por SAP (que no debe ser ningún auditor externo que sea competencia de SAP, que no esté adecuadamente caalificado o que no sea independiente), podrá auditar el ambiente de control y las prácticas de seguridad de SAP en lo relativo a los Datos Personales tratados por SAP, únicamente si:

(a) SAP no ha proporcionado suficiente evidencia de cumplimiento de las medidas técnicas y organizativas que protegen los sistemas de producción del Servicio Cloud mediante: (i) una certificación del cumplimiento de la norma ISO 27001 o de otras normas (su alcance está definido en el certificado); o (ii) un informe válido de certificación de ISAE3402 y/o ISAE3000, o SOC1-3. Previa solicitud del Cliente, los informes de auditoría o las certificaciones ISO están disponibles a través del auditor externo o SAP;

(b) Se ha producido un Incumplimiento de los Datos Personales;

(c) La autoridad responsable de la protección de datos del Cliente solicita formalmente una auditoría; o

(d) Si la Ley de Protección de Datos aplicable proporciona al Cliente el derecho directo a realizar una auditoría y siempre que el Cliente audite una única vez en un período de doce meses, salvo que la Ley de Protección de Datos aplicable exija auditorías más frecuentes.

5.2 Auditoría de otro Responsable del Tratamiento de Datos. Cualquier otro Responsable del Tratamiento de Datos puede auditar el entorno de control y las prácticas de seguridad de SAP en lo relativo a los Datos Personales tratados por SAP según lo indicado en la Sección 5.1 únicamente si se aplica a dicho Responsable del Tratamiento de Datos cualquiera de los casos especificados en la Sección 5.1. El Cliente debe llevar a cabo esta auditoría de conformidad con lo especificado en la Sección 5.1 a menos que, según la Ley de Protección de Datos, el otro Responsable del Tratamiento de Datos deba ser quien lleve a cabo la auditoría. Si varios Responsables del Tratamiento de Datos cuyos Datos Personales ha tratado SAP en base al Contrato requieren una auditoría, el Cliente deberá utilizar todos los medios razonables para combinar las auditorías y evitar la necesidad de llevar a cabo múltiples auditorías.

5.3 Alcance de la Auditoría. El Cliente deberá notificar con al menos 60 (sesenta) días de anticipación cualquier auditoría, salvo que la Ley de Protección de Datos aplicable o una autoridad de protección de datos competente exija una notificación más corta. La frecuendia y el alcance de cualquier auditoría se acordará mutuamente entre las partes, que actúen de manera razonable y de buena fe. Las auditorías del Cliente estarán limitadas, en lo relativo al tiempo, a un máximo de tres días laborables. Además de estas limitaciones, las partes utilizarán las certificaciones actuales u otros informes de auditoría para evitar o minimizar auditorías repetitivas. El Cliente deberá proporcionar los resultados de cualquier auditoría a SAP.

5.4 Costos de las Auditorías. El Cliente asumirá los costos de cualquier auditoría, salvo que dicha auditoría revele un incumplimiento sustancial de este DPA por parte de SAP; en ese caso, SAP asumirá los costos de la auditoría. Si una auditoría determina que SAP ha incumplido sus obligaciones de conformidad con el DPA, SAP deberá solventar dicho incumplimiento de inmediato asumiendo todos los costos.

6. SUBENCARGADOS DEL TRATAMIENTO DE DATOS

6.1 Uso Permitido. Se le otorga a SAP una autorización general para subcontratar el tratamiento de los Datos Personales a Subencargados del Tratamiento de Datos, siempre que:

(a) SAP o SAP SE en su nombre contraten a los Subencargados del Tratamiento de Datos mediante un contrato escrito (se acepta formato electrónico) el contrato será cosistente con las condiciones de este DPA en lo relativo al tratamiento de los Datos Personales por parte del Subencargado del Tratamiento de Datos. SAP será responsable de cualquier

incumplimiento que cometa el Subencargado del Tratamiento de Datos de acuerdo con las condiciones de este Contrato;

(b) SAP evaluará las prácticas de seguridad, privacidad y confidencialidad de un Subencargado del Tratamiento de Datos antes de decidir si es capaz de proporcionar el nivel de protección de Datos Personales exigido por este DPA; y

(c) SAP publique, en la fecha de entrada en vigor del Contrato, la lista de Subencargados del Tratamiento de Datos, o SAP la ponga a disposición del Cliente previa solicitud, incluido el nombre, la dirección y el puesto de cada Subencargado del Tratamiento de Datos que SAP utiliza para prestar el Servicio Cloud.

6.2 Nuevos Subencargados del Tratamiento de Datos. El uso de Subencargados del Tratamiento de Datos por parte de SAP se realizará a decisión exclusiva de SAP, siempre y cuando:

(a) SAP informará al Cliente por anticipado (por correo electrónico o mediante publicación en el portal de soporte disponible a través de Soporte de SAP) acerca de cualquier intención de añadir o sustituir entradas de la lista de Subencargados del Tratamiento de Datos, incluyendo el nombre, la dirección y el puesto del nuevo Subencargado del Tratamiento de Datos; y

(b) El Cliente pueda oponerse a dichos cambios, de conformidad con lo especificado en la Sección 6.3.

6.3 Objeciones a los nuevos Subencargados del Tratamiento de Datos.

(a) Si el Cliente tiene un motivo legítimo, según la Ley de Protección de Datos, para oponerse al tratamiento de los Datos Personales por parte del nuevo Subencargado del Tratamiento de Datos, el Cliente podrá terminar el Contrato (únicamente por lo que respecta al Servicio Cloud para el cual se iba a utilizar el nuevo Subencargado del Tratamiento de Datos) previa notificaicon por escrito a SAP. Dicha terminación tendrá efecto en el momento especificado por el Cliente, que nunca será superior a los treinta días a partir de la fecha de la notificaicón de SAP que envióa al Cliente acerca del nuevo Subencargado del Tratamiento de Datos. En caso de que el Cliente no termine el Contrato dentro de este plazo de treinta días, se entenderá que el Cliente acepta al nuevo Subencargado del Tratamiento de Datos.

(b) Dentro del plazo de treinta días a partir del aviso de SAP que informa al Cliente acerca del nuevo Subencargado del Tratamiento de Datos, el Cliente podrá solicitar a las partes que se reúnan de buena fe para buscar una resolución a la objeción. Estas reuniones no deberían extenderse más allá del período de terminación y no afectan al derecho de SAP a usar el nuevo Subencargado del Tratamiento de Datos una vez transcurrido este período de treinta días.

(c) Cualquier terminación conforme a esta Sección 6.3 se considerará sin culpa por cualquiera de las partes y estará sujeta a las condiciones del Contrato.

6.4 Sustitución de Emergencia. SAP puede sustituir a un Subencargado del Tratamiento de Datos sin previo aviso siempre que el motivo del cambio esté fuera del control razonable de SAP y que la situación exija una sustitución inmediata por seguridad o por cualquier otro motivo de urgencia. En este caso, SAP informará al Cliente sobre la sustitución del Subencargado del Tratamiento de Datos lo antes posible según sus indicaciones. En consecuencia, se aplicará la Sección 6.3.

7. TRATAMIENTO INTERNACIONAL

7.1 Condiciones para el Tratamiento Internacional. SAP tendrá derecho a tratar los Datos Personales, de conformidad con este DPA, fuera del país en el que el Cliente está ubicado, según lo permitido por la Ley de Protección de Datos.

7.2 Cláusulas Contractuales Tipo. Siempre que (i) los Datos Personales de un Responsable del Tratamiento de Datos ubicado en el EEE o en Suiza se traten en un país fuera del EEE, Suiza y cualquier otro país, organización o territorio reconocido en la Unión Europea como país seguro con un nivel adecuado de protección de datos, según el artículo 45 del GDPR, o que (ii) los Datos Personales de otro Responsable del Tratamiento de Datos se traten de manera internacional y

dicho tratamiento internacional exija medios de adecuación de conformidad con las leyes del país del Responsable del Tratamiento de Datos y dichos medios de adecuación se puedan cumplir mediante la formalización de unas Cláusulas Contractuales tipo:

(a) SAP y el Cliente formalizarán las Cláusulas Contractuales Tipo;

(b) El Cliente formalizará las Cláusulas Contractuales Tipo con cada Subencargado del Tratamiento de Datos relevante de la manera siguiente, o bien (i) el Cliente se adherirá a las Cláusulas Contractuales Tipo formalizadas por SAP, o SAP SE, y el Subencargado del Tratamiento de Datos como propietario independiente de derechos y obligaciones ("Modelo de Adhesión"), o bien (ii) el Subencargado del Tratamiento de Datos (representado por SAP) formalizará las Cláusulas Contractuales Tipo con el Cliente ("Modelo de Poder Notarial"). El Modelo de Poder Notarial se aplicará siempre que SAP haya confirmado explícitamente que un Subencargado del Tratamiento de Datos tiene derecho a esta opción de modelo a través de la lista de Subencargados del Tratamiento de Datos especificada en la Sección 6.1(c), o un aviso al Cliente; y/o

(c) Otros Responsables del Tratamiento de Datos cuyo uso de los Servicios Cloud haya sido autorizado por el Cliente de acuerdo con el Contrato, pueden formalizar Cláusulas Contractuales Tipo con SAP y/o los Subencargados del Tratamiento de Datos relevantes de la misma manera que el Cliente, de conformidad con las anteriores Secciones 7.2 (a) y (b). En ese caso, el Cliente formalizará las Cláusulas Contractuales Tipo en el nombre del resto de Responsables del Tratamiento de Datos.

7.3 Relación de las Cláusulas Contractuales Tipo con el Contrato. Ninguna de las disposiciones especificadas en el Contrato prevalecerá ante cualquier cláusula en conflicto de las Cláusulas Contractuales Tipo. Para evitar cualquier duda, si este DPA especifica reglas relativas a las auditorías y al subencargado del tratamiento de datos en las secciones 5 y 6, dichas especificaciones se aplicarán también en lo relativo a las Cláusulas Contractuales Tipo.

7.4 Ley aplicable a las Cláusulas Contractuales Tipo. Las Cláusulas Contractuales Tipo se regirán por la legislación del país en el que se encuentre el Responsable del Tratamiento de Datos relevante.

8. DOCUMENTACIÓN; REGISTROS DEL TRATAMIENTO

Cada una de las partes es responsable de cumplir sus requisitos de documentación, en especial en lo relativo al mantenimiento de los registros de tratamiento que exija la Ley de Protección de Datos.Cada una de las partes ayudará dentro de los límites razonables a la otra parte con sus requisitos de documentación, por ejemplo, proporcionando (mediante un sistema electrónico) la información que la otra parte necesite y solicite, a fin de permitir a la otra parte cumplir sus obligaciones relativas al mantenimiento de los registros de tratamiento.

9. ACCESO DESDE LA UE

9.1 Servicio opcional. El Acceso desde la UE es un servicio opcional que SAP puede ofrecer. Si así se acuerda en el Formulario de Pedido para el Servicio Cloud compatible con este servicio identificado explícitamente en él como sujeto al Acceso desde la UE, SAP proporcionará el Servicio Cloud únicamente mediante instancias de producción, de conformidad con esta Sección 9. Si no se acuerda el Acceso desde la UE en el Formulario de Pedido, esta Sección 9 no se aplicará.

9.2 Acceso desde la UE. SAP solo utilizará Subencargados Europeos del Tratamiento de Datos para prestar cualquier soporte que requiera acceso a los Datos Personales en el Servicio Cloud; SAP no exportará los Datos Personales fuera del EEE o Suiza salvo que el Cliente lo haya autorizado expresamente por escrito (se acepta por correo electrónico) caso por caso; o según se excluya en la Sección 9.4.

9.3 Ubicación del Centro de Datos. A partir de la fecha de entrada en vigor del Contrato, los Centros de Datos que se utilizan para alojar Datos Personales en el Servicio Cloud se ubicarán en el EEE o en Suiza. SAP no migrará la instancia del Cliente a un Centro de Datos fuera del EEE o

de Suiza sin un consentimiento previo por escrito del Cliente (se acepta por correo electrónico). En caso de que SAP tenga previsto migrar la instancia del Cliente a un Centro de Datos dentro del EEE o Suiza, SAP notificará dicha migración por escrito al Cliente (se acepta por correo electrónico) con una antelación mínima de treinta días antes de que se lleve a cabo la migración planificada.

9.4 Exclusiones. Los siguientes Datos Personales no están sujetos a 9.2 y 9.3:

(a) Los datos de contacto del remitente de un ticket de soporte; y

(b) Cualquier otro Dato Personal enviado por el Cliente a la hora de completar un ticket de soporte. El Cliente puede optar por no transmitir los Datos Personales al completar un ticket de soporte. En caso de que esos datos sean necesarios para el proceso de gestión de la incidencia, el Cliente puede optar por anonimizar estos Datos Personales antes de transmitir a SAP el mensaje de la incidencia.

10. DEFINICIONES

Los términos en mayúscula que no se definan en el presente documento tendrán el significado que se les haya atribuido en el Contrato.

10.1 "Responsable" es la persona física o jurídica, autoridad pública, agencia u otro organismo que, de manera independiente o mediante colaboración con otros, determina la finalidad y los medios del tratamiento de los Datos Personales; en el contexto de este DPA, cuando el Cliente actúe como encargado del tratamiento de datos para otro responsable del tratamiento de datos, por lo que respecta a SAP se considerará un Responsable del Tratamiento de Datos adicional e independiente con los derechos y obligaciones correspondientes a un Responsable del Tratamiento de Datos de conformidad con este DPA.

10.2 "Centro de Datos" es la ubicación donde se aloja la instancia de producción del Servicio Cloud para el Cliente en su región, tal como está publicado en: http://www.sap.com/corporate-en/about/our-company/policies/data-privacy-and-security/location-of-data-center.html , o tal como se ha notificado al Cliente o se ha acordado de cualquier otra forma en un Formulario de Pedido.

10.3 "Ley de Protección de Datos" es la legislación aplicable en lo relativo a los derechos y libertades fundamentales de las personas, así como el derecho a la privacidad en el tratamiento de los Datos Personales de conformidad con el Contrato (e incluye, por lo que respecta a la relación entre las partes en lo relativo al tratamiento de Datos Personales por parte de SAP en nombre del Cliente, (i) el GDPR como estándar mínimo, independientemente de si los Datos Personales están sujetos al GDPR o no, ya que el tratamiento de los Datos Personales opera en la Union Europea y (ii) las otras leyes de protección de datos de Colombia, como es la Ley 1581 de 2012, y sus decretos reglamentarios colombianos, dependiendo en la jurisdicción que protege al Titular).

10.4 " Titular" es una persona física identificada o identificable, según se define en la Ley de Protección de Datos.

10.5 "EEE" es el Espacio Económico Europeo y, específicamente, los Estados Miembros de la Unión Europea junto con Islandia, Liechtenstein y Noruega.

10.6 "Subencargado Europeo" es un Subencargado del Tratamiento de Datos que trata físicamente los Datos Personales en el EEE o en Suiza.

10.7 "Datos Personales" es cualquier información relativa a un Titular protegido por la Ley de Protección de Datos. En el contexto con este DPA, incluye únicamente los datos personales (i) introducidos por el Cliente o sus Usuarios Autorizados durante o a partir de su uso del Servicio Cloud, o (ii) suministrados a o accedidos por SAP o sus Subencargados para prestar soporte bajo el Contrato. Los Datos Personales son un subconjunto de Datos del Cliente (conforme a lo definido en el Contrato).

10.8 "Brecha de los Datos Personales" es (1) la destrucción accidental o ilícita, la pérdida, la alteración, la revelación no autorizada o el acceso no autorizado de terceros a Datos Personales, o (2) incidentes similares que involucren Datos Personales, en cada caso, para el cual un

Responsable está obligado por la Ley de Protección de Datos a notificar a las autoridades competentes de protección de datos o a los Titulares.

10.9 **"Encargado"** es una persona física o jurídica, autoridad pública, agencia u otro organismo que trate los datos personales en nombre del Responsable del Tratamiento de Datos, ya sea directamente como encargado del tratamiento de datos de un responsable del tratamiento de datos, o indirectamente como subencargado del tratamiento de datos de un encargado del tratamiento de datos que trata los datos personales en nombre del responsable del tratamiento de datos.

10.10 **"Cláusulas Contractuales Tipo"**, también denominadas "Cláusulas Modelo de la UE", son las Cláusulas Contractuales Tipo (encargados del tratamiento de datos) o cualquier versión posterior de estas publicadas por la Comisión Europea (que se aplicarán automáticamente).

10.11 **"Subencargado "** son las Subsidiraias de SAP, SAP SE, las Subsidiarias de SAP SE y los terceros contratados por SAP, SAP SE o las Subsidiariasde SAP SE en relación con el Servicio Cloud y que tratan los Datos Personales de conformidad con este DPA.

Apéndice 1 al DPA y, si aplica, a las Cláusulas Contractuales Tipo

Exportador de Datos
El Exportador de Datos es el Cliente suscrito a un Servicio Cloud que permite a los Usuarios Autorizados grabar, modificar, utilizar, eliminar o tratar de cualquier otra forma los Datos Personales. Cuando el Cliente permita a otros Responsables del Tratamiento de Datos utilizar también el Servicio Cloud, estos otros Responsables del Tratamiento de Datos serán también Exportadores de Datos.

Importador de Datos
SAP y sus Subprocesadores proporcionan el Servicio Cloud, que incluye el siguiente soporte:

Las Subsidiarias de SAP SE prestan soporte a los centros de datos del Servicio Cloud de forma remota desde las instalaciones de SAP en St. Leon/Rot (Alemania), India y otras ubicaciones en las que SAP contrata personal para las funciones de Operaciones/Prestación del Servicio Cloud. Este soporte incluye:

- Supervisión del Servicio Cloud
- Copias de seguridad y restauración de los Datos del Cliente almacenados en el Servicio Cloud
- Lanzamiento y desarrollo de correcciones y mejoras en el Servicio Cloud
- Supervisión, solución de problemas y administración de la infraestructura y la base de datos del Servicio Cloud
- Control de la seguridad, soporte para la detección de intrusiones en la red, realización de pruebas de penetración

Las Afiliadas de SAP SE prestan soporte cuando un Cliente abre un ticket de soporte porque el Servicio Cloud no está disponible o no funciona de la manera esperada para algunos o todos los Usuarios Autorizados. SAP responde a los teléfonos, aplica soluciones básicas y gestiona los tickets de soporte en un sistema de seguimiento que es independiente de la instancia de producción del Servicio Cloud.

Interesados
Salvo que el Exportador de Datos lo establezca de otra forma, los Datos Personales transferidos se relacionan con la siguientes categorías de Interesados: empleados, contratistas, socios empresariales u otros individuos cuyos Datos Personales estén almacenados en el Servicio Cloud.

Categorías de Datos
Los Datos Personales transferidos abarcan las siguientes categorías de datos:

El Cliente determina las categorías de datos por Servicio Cloud suscrito. El Cliente puede configurar los campos de datos proporcionados por el Servicio Cloud durante la implementación del Servicio Cloud o de cualquier otra manera. Los Datos Personales transferidos normalmente hacen referencia a las siguientes categorías de datos: nombre, números de teléfono, direcciones de correo electrónico, zona horaria, datos de dirección, datos de acceso / uso / autorización del sistema, nombre de la empresa, datos de contratos, datos de factura, además de otros datos específicos de la aplicación que los Usuarios Autorizados introducen en el Servicio Cloud y que pueden incluir datos sobre cuentas bancarias o tarjetas de crédito o débito.

Categorías Especiales de Datos (si procede)
Los Datos Personales transferidos afectan a las siguientes categorías especiales de datos: las que se especifican en el Contrato (incluido el Formulario de Pedido), de haberlas.

Operaciones/Finalidades del Tratamiento
Los Datos Personales transferidos están sujetos a las siguientes actividades básicas de tratamiento:

- Uso de los Datos Personales para configurar, funcionar, supervisar y proporcionar el Servicio Cloud (incluido el Soporte Operativo y Técnico)
- Prestación de Servicios de Consultoría
- Comunicación con Usuarios Autorizados
- Almacenamiento de los Datos Personales en Centros de Datos específicos (arquitectura para varios clientes)
- Subida de correcciones o mejoras en el Servicio Cloud
- Copia de seguridad de los Datos Personales
- Tratamiento informático de Datos Personales, incluida la transmisión, la recuperación y el acceso de datos
- Acceso a la red para permitir la transferencia de Datos Personales
- Formalización de las instrucciones del Cliente de acuerdo con el Contrato.

Apéndice 2 al DPA y, si aplica, a las Cláusulas Contractuales Tipo – Medidas técnicas y organizativas

1. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Las siguientes secciones definen las medidas técnicas y organizativas vigentes de SAP. SAP podrá modificarlas en cualquier momento, sin previo aviso, siempre que mantenga un nivel de seguridad comparable o superior. Las medidas individuales pueden sustituirse por nuevas medidas que tengan la misma finalidad, siempre que no reduzcan el nivel de seguridad que protege los Datos Personales.

1.1 Control de Acceso Físico. Las personas no autorizadas no obtendrán acceso físico a las instalaciones, los edificios o las salas en las que estén ubicados los sistemas de tratamiento de datos que tratan y/o utilizan los Datos Personales.

Medidas:

- SAP protege sus activos e instalaciones con los medios apropiados basados en la Política de Seguridad de SAP.
- En general, los edificios están asegurados mediante unos sistemas de control de acceso (por ejemplo, sistema de acceso con tarjetas inteligentes).
- Como requisito mínimo, los puntos de entrada más alejados del edificio deben estar equipados con un sistema de llaves certificado que incluya una gestión de llaves activa y moderna.
- En función de la clasificación de seguridad, los edificios, las áreas individuales y las instalaciones de los alrededores estarán además protegidas con medidas adicionales. Estas medidas incluyen: perfiles de acceso específicos, vídeovigilancia, sistemas de alarma contra intrusos y sistemas de control de acceso biométrico.
- Se conceden derechos de acceso a las personas autorizadas de forma individual de conformidad con las medidas de Control de Acceso a los Datos y al Sistema (véanse las secciones 1.2 y 1.3 siguientes). Esto también se aplica al acceso de los visitantes. Los invitados y visitantes de los edificios de SAP tienen que registrar sus nombres en recepción, y deben ir acompañados por personal autorizado de SAP.
- Los empleados de SAP y el personal externo deben llevar sus tarjetas de identificación en todas las ubicaciones de SAP.

Medidas adicionales para Centros de Datos:

- Todos los Centros de Datos siguen estrictos procedimientos de seguridad reforzados por guardias, cámaras de vigilancia, detectores de movimiento, mecanismos de control del acceso y otras medidas para evitar comprometer los equipos y las instalaciones del Centro de Datos. Los únicos que tienen acceso a los sistemas y a la infraestructura dentro de las instalaciones del Centro de Datos son los representantes autorizados. Para proteger el correcto funcionamiento, periódicamente se efectúa el mantenimiento de los equipos de seguridad físicos (por ejemplo, sensores de movimiento, cámaras, etc.).
- SAP y todos los terceros proveedores de Centros de Datos registran los nombres y las horas del personal autorizado que accede a áreas privadas de SAP dentro de los Centros de Datos.

1.2 Control de Acceso al Sistema. Es necesario impedir que los sistemas de tratamiento de datos que se utilizan para prestar el Servicio Cloud se puedan usar sin autorización.

Medidas:

- Se utilizan varios niveles de autorización para garantizar el acceso a sistemas sensibles, incluidos aquellos que almacenan y tratan Datos Personales. Las autorizaciones se gestionan mediante procesos definidos conforme a la Política de Seguridad de SAP.
- Todo el personal accede a los sistemas de SAP con un identificador único (ID de usuario).
- SAP dispone de procedimientos para que los cambios de autorización solicitados se implementen solamente de acuerdo con la Política de Seguridad de SAP (por ejemplo, no se otorgan derechos sin autorización). En caso de que el personal deje la empresa, sus derechos de acceso quedarán revocados.

- SAP ha establecido una política de contraseñas que prohíbe compartirlas, especifica qué debe hacerse en caso de que se divulgue una contraseña y exige que se cambien periódicamente y que se modifiquen las contraseñas predeterminadas. Se asignan identificadores de usuario personalizados para la autenticación. Todas las contraseñas deben cumplir unos requisitos mínimos definidos y se almacenan de forma encriptada. En el caso de las contraseñas de dominios, el sistema obliga a cambiar la contraseña cada seis meses para cumplir con los requisitos para contraseñas complejas. Cada ordenador tiene un protector de pantalla protegido mediante contraseña.
- La red de la empresa está protegida de la red pública mediante cortafuegos.
- SAP utiliza un software de antivirus actualizado en los puntos de acceso ala red de la empresa (para cuentas de correo electrónico) y en todos los servidores de archivo y centros de trabajo. Se ha implementado la gestión de parches de seguridad para proporcionar implementaciones regulares y periódicas de las actualizaciones de seguridad pertinentes. El acceso remoto total a la red corporativa de SAP y a la infraestructura crítica está protegido mediante una autenticación sólida.

1.3 Control de Acceso a los Datos. Aquellas personas que estén autorizadas para utilizar sistemas de tratamiento de datos únicamente deberán tener acceso a los Datos Personales para los que tengan derecho de acceso, y los Datos Personales no podrán leerse, copiarse, modificarse o eliminarse sin autorización durante el tratamiento, el uso y el almacenamiento.

Medidas:

- Como parte de la Política de Seguridad de SAP, los Datos Personales requieren al menos el mismo nivel de protección que la información "confidencial" de acuerdo con el estándar de Clasificación de la Información de SAP.
- El acceso a los Datos Personales se otorga en función de la necesidad de conocerlos. El personal tiene acceso a la información que necesita para cumplir sus obligaciones. SAP utiliza conceptos de autorización que documentan los procesos otorgados y los roles asignados por cuenta (ID de usuario). Todos los Datos del Cliente están protegidos de conformidad con la Política de Seguridad de SAP.
- Todos los servidores de producción funcionan en los Centros de Datos o en salas de servidores seguras. Las medidas de seguridad que protegen las aplicaciones que tratan Datos Personales se verifican periódicamente. Con este objetivo, SAP lleva a cabo verificaciones de seguridad internas y externas y pruebas de entrada en sus sistemas de TI.
- SAP no permite la instalación de software que no haya sido autorizado por SAP.
- Un estándar de seguridad de SAP rige cómo se eliminan o destruyen los datos y los soportes de datos una vez que ya no son necesarios.

1.4 Control de Transmisión de Datos. Excepto en la medida en que sea necesario para la prestación de los Servicios Cloud de acuerdo con el Contrato, los Datos Personales no se podrán leer, copiar, modificar o eliminar sin autorización durante la transferencia. Cuando los soportes de datos se transportan físicamente, se implementan medidas adecuadas en SAP para proporcionar los niveles de servicio acordados (por ejemplo, encriptación y contenedores con blindaje de plomo).

Medidas:

- Los Datos Personales que se transfieren a través de redes internas de SAP están protegidos conforme a la Política de Seguridad de SAP.
- Cuando los datos se transfieren entre SAP y sus clientes, las medidas de protección para los Datos Personales transferidos se acuerdan mutuamente y forman parte del contrato relevante. Esto se aplica a la transferencia de datos a través de una red como a la transferencia física. En cualquier caso, el Cliente asume la responsabilidad de cualquier transferencia de datos si se encuentra fuera de los sistemas controlados por SAP (por ejemplo, datos transferidos fuera del *firewall* del Centro de Datos de SAP).

1.5 Control de Entrada de Datos. Será posible examinar de forma retrospectiva y establecer si, y por quién se introdujeron, modificaron o eliminaron Datos Personales de los sistemas de tratamiento de SAP.

Medidas:

- SAP solamente permite que el personal autorizado acceda a los Datos Personales que necesitan, durante el transcurso de su trabajo.
- SAP ha implementado un sistema de registro para la entrada, la modificación, la eliminación o el bloqueo de Datos Personales por parte de SAP o sus subencargados del tratamiento de datos en el Servicio Cloud en la mayor medida técnica posible.

1.6 Control de Funciones. Los Datos Personales tratados por encargo (por ejemplo, los Datos Personales tratados en nombre de un cliente) se tratarán únicamente de conformidad con el Contrato y según las instrucciones del cliente.

Medidas:

- SAP utiliza controles y procesos para supervisar el cumplimiento de los contratos entre SAP y sus clientes, subencargados del tratamiento de datos u otros proveedores de servicios.
- Como parte de la Política de Seguridad de SAP, los Datos Personales requieren, como mínimo, el mismo nivel de protección que la información "confidencial" de acuerdo con el estándar de Clasificación de la Información de SAP.
- Todos los empleados de SAP, los subprocesadores contractuales u otros proveedores de servicios están vinculados mediante contrato al respeto de la confidencialidad de toda la información sensible, incluidos los secretos comerciales de los clientes y socios de SAP.

1.7 Control de Disponibilidad. Los Datos Personales deberán protegerse de posibles pérdidas o destrucciones accidentales o no autorizadas.

Medidas:

- SAP realiza procesos de copia de seguridad periódicos para garantizar la restauración de los sistemas críticos para las actividades empresariales siempre que sea necesario.
- SAP utiliza un suministro eléctrico ininterrumpido (p. ej.: UPS, baterías, generadores, etc.) para proteger el suministro de electricidad a los Centros de Datos.
- SAP ha definido planes de contingencia empresarial para los procesos críticos para la actividad empresarial y puede ofrecer estrategias de recuperación en caso de desastre para los Servicios críticos para la empresa, según lo especificado en la Documentación o lo incluido en el Formulario de Pedido para el Servicio Cloud relevante.
- Los procesos y sistemas de emergencia se prueban periódicamente.

1.8 Control de Separación de Datos. Los Datos Personales recopilados para diferentes finalidades pueden tratarse por separado.

Medidas:

- SAP utiliza funcionalidades técnicas del software implementado (por ejemplo para múltiples arrendatarios o ambientes de sistema independientes) para lograr la separación de datos entre los Datos Personales originados desde varios clientes.
- El Cliente (incluidos sus Responsables del Tratamiento de Datos) solo tiene acceso a sus propios datos.
- En caso de que se necesiten Datos Personales para procesar una incidencia de soporte del Cliente, los datos se asignarán a este mensaje específico y se utilizarán únicamente para procesar dicho mensaje; no se accederá a ellos para procesar ninguno otro. Dichos datos se almacenarán en sistemas de soporte exclusivos.

1.9 Control de la Integridad de los Datos. Los Datos Personales permanecerán intactos, completos y actualizados durante las actividades de tratamiento.

Medidas:

SAP ha implementado una estrategia de defensa basada en varias capas como método de protección contra modificaciones no autorizadas.

En concreto, SAP utiliza los siguientes elementos para implementar las secciones de control y medidas descritas anteriormente. En concreto:

- Cortafuegos (*Firewalls*)
- Centro de Control de la Seguridad
- Software antivirus
- Copias de seguridad y recuperación
- Pruebas de vulnerabilidad internas y externas
- Auditorías externas periódicas para probar las medidas de seguridad

Apéndice 3 al DPA y, si aplica, a las Cláusulas Contractuales Tipo

La siguiente tabla especifica los Artículos del GDPR relevantes y las condiciones correspondientes del DPA únicamente a modo de ejemplo.

Artículo del GDPR	**Sección del DPA**	**Haga clic en el enlace para ver la Sección**
28(1)	2 y el Apéndice 2	Seguridad del Tratamiento y el Apéndice 2, Medidas Técnicas y Organizativas.
28(2), 28(3) (d) y 28 (4)	6	SUBENCARGADOS DEL TRATAMIENTO DE DATOS
28 (3) frase 1	1.1 y el Apéndice 1, 1.2	Finalidad y Aplicación. Estructura.
28(3) (a) y 29	3.1 y 3.2	Instrucciones del Cliente. Tratamiento de Requisitos Legales.
28(3) (b)	3.3	Personal.
28(3) (c) y 32	2 y el Apéndice 2	Seguridad del Tratamiento y el Apéndice 2, Medidas Técnicas y Organizativas.
28(3) (e)	3.4	Cooperación.
28(3) (f) y 32-36	2 y el Apéndice 2, 3.5, 3.6	Seguridad del Tratamiento y el Apéndice 2, Medidas Técnicas y Organizativas. Notificación de Incumplimiento de los Datos Personales. Evaluación del Impacto de la Protección de Datos.
28(3) (g)	4	Exportación y Eliminación de Datos
28(3) (h)	5	CERTIFICACIONES Y AUDITORÍAS
28 (4)	6	SUBENCARGADOS DEL TRATAMIENTO DE DATOS
30	8	Documentación; Registros del tratamiento
46(2) (c)	7.2	Cláusulas Contractuales Tipo.

Apéndice 4

CLÁUSULAS CONTRACTUALES TIPO (ENCARGADOS DEL TRATAMIENTO DE DATOS)[1]

Las Cláusulas Contractuales Tipo estándar a las que se hace referencia en este DPA se encuentran en el siguiente enlace:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087

---------- el resto de la página intencionalmente en blanco ----------

[1] Conforme a la Decisión de la Comisión del 5 de febrero de 2010 (2010/87/UE)