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

1. ANTECEDENTES

1.1 Finalidad.

Este documento es un contrato de tratamiento de datos ("**DPA**") entre SAP y el Cliente y se aplica a los Datos Personales proporcionados por el Cliente y a cada Controlador de Datos en relación con el uso que hacen del Servicio Cloud. Establece las medidas organizativas y técnicas que SAP utiliza para proteger los Datos Personales almacenados en el sistema de producción del Servicio Cloud.

1.2 Aplicación del Documento de las Cláusulas Contractuales Tipo

Si el tratamiento de Datos Personales incluye una Transferencia Internacional, las Cláusulas Contractuales Tipo se aplicarán como está estipulado en la Sección 5 y se incorporarán como referencia.

1.3 Gobernanza.

Salvo que esté especificado en la Sección 5.2, el Cliente será el único responsable de la administración de todas las solicitudes de otros Controladores de Datos. El Cliente vinculará a cualquier otro Controlador de Datos el permiso para utilizar el Servicio Cloud de acuerdo con las condiciones de este DPA.

2. APÉNDICES

El Cliente y sus Controladores de Datos deberán determinar las finalidades de recopilación y tratamiento de los Datos Personales en el Servicio Cloud. El Apéndice 1 expone los detalles del tratamiento que SAP proporcionará mediante el Servicio Cloud. El Apéndice 2 expone las medidas técnicas y organizativas que SAP aplicará al Servicio Cloud, salvo que el Contrato especifique lo contrario.

3. OBLIGACIONES DE SAP

3.1 Instrucciones del Cliente

SAP seguirá las instrucciones que reciba del Cliente (en su nombre o en nombre de sus Controladores de Datos) con respecto a los Datos Personales, a menos que estén (i) legalmente prohibidas o (ii) requieran cambios materiales en el Servicio Cloud. SAP podrá corregir o eliminar Datos Personales de conformidad con las instrucciones del Cliente. En caso de que SAP no pueda cumplir una instrucción, deberá notificar al Cliente inmediatamente (se acepta por correo electrónico).

3.2 Confidencialidad de los Datos.

Para tratar Datos Personales, SAP y sus Subprocesadores solo emplearán personal que esté sujeto a una obligación vinculante de cumplimiento de la confidencialidad de los datos o de las telecomunicaciones, conforme a la Ley de Protección de Datos. SAP y sus Subprocesadores deberán formar periódicamente en seguridad y privacidad de los datos a las personas a las que conceda acceso a los Datos Personales.

3.3 Medidas Técnicas y Organizativas.

(a) SAP utilizará las medidas técnicas y organizativas apropiadas estipuladas en el Apéndice 2.

(b) El Apéndice 2 se aplicará al sistema de producción del Servicio Cloud. El Cliente no deberá almacenar Datos Personales en entornos que no sean de producción.

(c) SAP proporciona el Servicio Cloud a toda la base de clientes de SAP alojados en el mismo centro de datos y suscritos al mismo Servicio Cloud. El Cliente acepta que SAP podrá mejorar las medidas estipuladas en el Apéndice 2 sobre la protección de Datos Personales siempre y cuando no se reduzca el nivel de protección de datos.

3.4 Notificación de Incumplimiento de Seguridad.

SAP deberá informar inmediatamente al Cliente si tiene conocimiento de cualquier Incumplimiento de Seguridad

3.5 Cooperación.

A petición del Cliente, SAP ayudará de forma razonable al Cliente o a cualquier Controlador de Datos a atender las solicitudes de Sujetos de Datos o de autoridades supervisoras con respecto al tratamiento de Datos Personales por parte de SAP.

4. SUBPROCESADORES DE DATOS

4.1 Uso Permitido.

(a) El Cliente y los Controladores de Datos autorizan a SAP a subcontratar el tratamiento de Datos Personales a Subprocesadores. SAP es responsable de cualquier incumplimiento del Contrato por parte de sus Subprocesadores.

(b) Los Subprocesadores tendrán las mismas obligaciones que SAP como Responsables del Tratamiento de Datos (o Subprocesadores) en relación al tratamiento de Datos Personales.

(c) SAP evaluará las prácticas de seguridad, privacidad y confidencialidad del Subprocesador antes de ser seleccionado. Los Subprocesadores podrán disponer de certificaciones de seguridad que demuestren que están utilizando las medidas de seguridad adecuadas. De no ser así, SAP evaluará periódicamente las prácticas de seguridad de todos los Subprocesadores relacionadas con la manipulación de datos.

(d) Si el Cliente lo solicita, SAP informará al Cliente del nombre, la dirección y el rol de cada Subprocesador de Datos al que recurra para prestar el Servicio Cloud.

4.2 Nuevos Subprocesadores de Datos.

El uso de Subprocesadores por parte de SAP se realizará a decisión exclusiva de SAP, siempre y cuando:

(a) SAP notifique al Cliente por adelantado (mediante correo electrónico o publicación en el Portal de Soporte) de cualquier cambio efectuado en la lista de Subprocesadores efectivo en la Fecha de Entrada en Vigor (salvo en el caso de las Sustituciones de Urgencia o las eliminaciones de Subprocesadores sin sustitución).

(b) En caso de que el Cliente disponga de un motivo legítimo relacionado con el tratamiento de Datos Personales de los Subprocesadores, el Cliente podrá oponerse al uso de un Subprocesador por parte de SAP notificando a SAP por escrito en un plazo de treinta días tras la recepción de la notificación de SAP. En caso de que Cliente se oponga al uso del Subprocesador, las partes se reunirán de buena fe para debatir una resolución. SAP podrá elegir: (i) no emplear al Subprocesador o (ii) tomar las medidas correctivas que solicite el Cliente en su oposición y emplear al Subprocesador. Si ninguna de estas opciones es razonablemente viable y el Cliente sigue oponiendo un motivo legítimo, cualquier parte podrá finalizar el Contrato mediante una notificación escrita en un plazo de 30 días. En caso de que el Cliente no se oponga dentro de los treinta días posteriores a la recepción de dicha notificación, se entenderá que el Cliente acepta al nuevo Subprocesador.

(c) En caso de que la objeción del Cliente siga pendiente sesenta días después de ser formulada y SAP no haya recibido ninguna notificación de finalización, se entenderá que el Cliente acepta al Subprocesador.

4.3 Sustitución de Urgencia.

SAP podrá reemplazar un Subprocesador si el motivo de la sustitución está fuera del control razonable de SAP. En este caso, SAP informará al Cliente sobre la sustitución del Subprocesador lo antes posible. El Cliente conserva el derecho a oponerse a esta sustitución del Subprocesador de conformidad con la Sección 4.2(b).

5. TRANSFERENCIAS INTERNACIONALES

5.1 Limitaciones de la Transferencia Internacional.

Únicamente SAP o sus Subprocesadores fuera del EEE o de Suiza podrán acceder o exportar Datos Personales del EEE o del Controlador de Datos Suizos (**"Transferencia Internacional"**):

(a) Si el destinatario, el país o el territorio en el que se procesa o accede a los Datos Personales garantiza un nivel de protección adecuado para los derechos y libertades de los

Sujetos de Datos en relación con el tratamiento de Datos Personales, tal como determina la Unión Europea; o

(b) de acuerdo con la Sección 5.2.

5.2 Cláusulas Contractuales Tipo y Marco de Múltiples Niveles

(a) Las Cláusulas Contractuales Tipo se aplican cuando existen Transferencias Internacionales a un país que no garantiza un nivel de protección adecuado para los derechos y libertades de los Sujetos de Datos en relación con el tratamiento de Datos Personales, tal como determina la Unión Europea.

(b) Para los Subprocesadores de un País Tercero, SAP ha formalizado la versión no modificada de las Cláusulas Contractuales Tipo anterior al tratamiento de Datos Personales por parte del Subprocesador. Por el presente, el Cliente (en nombre propio y en nombre de cada Controlador de Datos) accede a las Cláusulas Contractuales Tipo entre SAP y el Subprocesador de un País Tercero. SAP deberá hacer que dicho Subprocesador aplique las Cláusulas Contractuales Tipo en nombre del Controlador de Datos si el derecho directo de aplicación no se encuentra disponible en la Ley de Protección de Datos.

(c) Nada de lo dispuesto en este DPA prevalecerá ante cualquier cláusula en conflicto de las Cláusulas Contractuales Tipo.

6. CERTIFICACIONES Y AUDITORÍAS

6.1 Auditorías del Cliente.

El Cliente o sus auditores externos independientes podrán auditar las prácticas de seguridad y el entorno de control de SAP relevantes para los Datos Personales tratados por SAP solo si:

(a) SAP no ha proporcionado pruebas suficientes del cumplimiento con 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. Previa solicitud del Cliente, los informes de auditoría SOC o las certificaciones ISO están disponibles mediante el auditor externo o SAP;

(b) Se ha producido un Incumplimiento de Seguridad;

(c) El Cliente u otro Controlador de Datos posee fundamentos razonables para sospechar que SAP no cumple con las obligaciones que le corresponden en virtud de este DPA;

(d) El Cliente u otra autoridad de protección de datos del Controlador de Datos solicita formalmente una auditoría; o

(e) La Ley de Protección de Datos obligatoria proporciona al Cliente un derecho directo de auditoría.

Si el Cliente audita el entorno de SAP, SAP ayudará de forma razonable al Cliente en su proceso de auditoría.

6.2 Restricciones de la Auditoría.

La auditoría del Cliente se limitará a una dentro de un período de doce meses y a un máximo de tiempo de 3 días laborables, y su alcance será el acordado previamente de forma razonable entre las dos partes. Se deberá informar con una antelación razonable de al menos sesenta días, salvo que la Ley de Protección de Datos requiera una auditoría antes. SAP y el Cliente utilizarán certificaciones u otros informes de auditoría vigentes con el fin de minimizar auditorías repetitivas. El Cliente y SAP se harán cargo de sus propios costes de auditoría, a menos que el Cliente sea auditado de conformidad con la Sección 6.1 (c) (salvo que dicha auditoría revele un incumplimiento por parte de SAP, en cuyo caso SAP se hará cargo de sus propios gastos de auditoría), 6.1 (d) o 6.1 (e). En dichos casos, el Cliente se hará cargo de sus propios gastos y del coste de los recursos internos de SAP necesarios para realizar la auditoría. Si una auditoría determina que SAP ha incumplido sus obligaciones de conformidad con el Contrato, SAP deberá solventar dicho incumplimiento de inmediato asumiendo todos los costes.

7. ACCESO UE

7.1 Servicio opcional.

Si se incluye en el Formulario de Pedido, SAP acuerda proporcionar Acceso UE para el Servicio Cloud elegible, de conformidad con la Sección 7.

7.2 Acceso UE.

SAP solo utilizará Subprocesadores europeos para proporcionar un soporte que requiera acceso a los Datos Personales en el Servicio Cloud.

7.3 Ubicación del Centro de Datos.

A partir de la Fecha de Entrada en Vigor del Formulario de Pedido, los Centros de Datos utilizados 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 deberá notificar 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.

7.4 Exclusiones.

Los siguientes Datos Personales no estarán sujetos a los requisitos en las secciones 7.2 y 7.3:

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

(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;

(c) Datos Personales en sistemas de no producción.

8. DEFINICIONES

Los términos en mayúscula que no se definan en el presente documento tendrán el significado que se les haya atribuido en el Contrato. **"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 , notificado al Cliente o acordado de otra forma en un Formulario de Pedido.

8.2 "Controlador de Datos" es la persona física o jurídica, autoridad pública, agencia u otro organismo que, sola o conjuntamente con otros, determina los objetivos y los medios del tratamiento de los Datos Personales.

8.3 "Responsable del Tratamiento de Datos" es la persona física o jurídica, autoridad pública, agencia u otro organismo que procesa los datos personales en nombre del controlador.

8.4 "Ley de Protección de Datos" es la legislación aplicable que protege los derechos y libertades fundamentales de las personas y su derecho a la privacidad con relación al tratamiento de los Datos Personales en virtud del Contrato.

8.5 "Sujeto de Datos" es una persona natural identificada o identificable.

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

8.7 "Subprocesador de Datos Europeo" es un Subprocesador de Datos que trata físicamente los Datos Personales en el EEE o en Suiza.

8.8 "Datos Personales" es cualquier información relacionada con un Sujeto de Datos para la finalidad de este DPA. Incluye únicamente los datos personales registrados por el Cliente o sus Usuarios Autorizados dentro o derivados del uso que hacen del Servicio Cloud. Asimismo, incluye los datos personales proporcionados a SAP o a los que SAP, o sus Subprocesadores de Datos, acceden para prestar soporte de acuerdo con el Contrato Los Datos Personales son un subconjunto de Datos del Cliente.

8.9 "Incumplimiento de Seguridad" es (1) la destrucción accidental o ilícita, pérdida, alteración o divulgación confirmada de Datos Personales del Cliente o Datos Confidenciales, o (2)

cualquier situación similar relacionada con Datos Personales para la que se requiera un Responsable de Tratamiento de Datos en virtud de la ley vigente para notificar al Controlador de Datos.

8.10 "Cláusulas Contractuales Tipo", también denominadas "Cláusulas Modelo de la UE", son las Cláusulas Contractuales Tipo (Procesador de Datos) o cualquier versión posterior de estas publicadas por la Comisión (que se aplicarán automáticamente). Las Cláusulas Contractuales Tipo vigentes se encuentran en http://ec.europa.eu/justice/data-protection/international-transfers/files/clauses_for_personal_data_transfer_processors_c2010-593.doc. Incluyen los Apéndices 1 y 2 adjuntos a este DPA.

8.11 "Subprocesador" son Filiales de SAP y terceros contratados por SAP o por Filiales de SAP para tratar datos personales.

8.12 "Subprocesador de un País Tercero" es cualquier Subprocesador constituido fuera del EEE y de cualquier país para el cual la Comisión Europea haya publicado una decisión de adecuación, tal como se indica en http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Anexo 1 del Contrato de Tratamiento de Datos y Cláusulas Contractuales Tipo

Exportador de Datos
El Exportador de Datos suscrito a un Servicio Cloud que permite a los Usuarios Autorizados grabar, modificar, utilizar, eliminar o de otra forma tratar los Datos Personales.

Importador de Datos
SAP y sus Subprocesadores proporcionan el Servicio Cloud, que incluye el siguiente soporte:
Las Filiales de SAP 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, administración y solución de problemas de la infraestructura y la base de datos subyacente del Servicio Cloud
- Control de la seguridad, soporte para la detección de intrusiones en la red, realización de pruebas de penetración

Las Filiales de SAP 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.

Sujetos de Datos
Salvo que el Exportador de Datos lo establezca de otra forma, los Datos Personales transferidos se relacionan con la siguientes categorías de sujetos de datos: 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 de Datos Especiales (si procede)
Los Datos Personales transferidos afectan a las siguientes categorías especiales de datos: las que se especifican en el Formulario de Pedido, de haberlas.

Operaciones de Tratamiento
Los Datos Personales transferidos están sujetos a las siguientes actividades de tratamiento básico:

- Uso de los Datos Personales para configurar, utilizar, 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 este Contrato

Apéndice 2 – Medidas Técnicas y Organizativas

1. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

Las siguientes secciones definen las medidas de seguridad vigentes de SAP. SAP podrá modificarlas en cualquier momento, sin previo aviso, siempre que mantenga un nivel de seguridad comparable o mejor. Esto puede significar que las medidas concretas se sustituyan por medidas nuevas con la misma finalidad sin reducir el nivel de seguridad.

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 utilizando los medios adecuados en función de la clasificación de seguridad llevada a cabo por un departamento de seguridad interno.
- 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, videovigilancia, 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 garantizar un funcionamiento adecuado, periódicamente se efectúa el mantenimiento de los equipos de seguridad (por ejemplo, sensores de movimiento, cámaras, etc.).
- SAP y todos los terceros proveedores de Centros de Datos registran los nombres y las horas de las personas que acceden 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 utilizados para prestar los Servicios de SAP puedan utilizarse sin autorización.

Medidas:

- Se utilizan varios niveles de autorización para garantizar el acceso a sistemas sensibles, incluidos aquellos que almacenan y tratan Datos Personales. Los procesos se implementan para garantizar que los usuarios autorizados tienen el permiso adecuado para añadir, eliminar o modificar usuarios.
- Todos los usuarios acceden a los sistemas de SAP con un identificador único (Id del usuario).

- SAP dispone de procedimientos para garantizar que los cambios de autorización solicitados se implementan solamente de acuerdo con las directrices (por ejemplo, no se otorgan derechos sin autorización). Si un usuario deja la empresa, sus derechos de acceso quedan 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 garantizar la implementación regular y periódica 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 la información personal, confidencial o sensible se garantiza en función de la necesidad de conocerla. En otras palabras, los empleados o terceros externos tienen acceso a la información relevante para poder llevar a cabo su trabajo. SAP utiliza conceptos de autorización que documentan cómo se asignan las autorizaciones, qué autorizaciones se asignan y a quién. Todos los datos personales, confidenciales o sensibles están protegidos de acuerdo con los estándares de seguridad de SAP. La información confidencial debe procesarse de forma confidencial.
- 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, confidenciales o sensibles 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 personal, ni de cualquier otro software que no haya sido autorizado por SAP.
- Un estándar de seguridad de SAP rige cómo se eliminan o destruyen los datos y los transportadores 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 de acuerdo con el contrato de servicio relevante, 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 garantizar los niveles de servicio acordados (por ejemplo, encriptación y contenedores con blindaje de plomo).

- Las transferencias de Datos Personales mediante las redes internas de SAP están protegidas de la misma forma que cualquier otro dato confidencial de acuerdo con 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 tanto a la transferencia de datos en red como 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 transmitidos fuera del cortafuegos del Centro de Datos de SAP).

1.5 Control de Entrada de Datos.

Será posible examinar de forma retrospectiva y establecer si y quién ha introducido, modificado o eliminado Datos Personales de los sistemas de tratamiento de SAP.

Medidas:

- SAP solamente permite que las personas autorizadas accedan 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 subprocesadores en los Productos y Servicios de SAP en la mayor medida 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 relevante y según las instrucciones del cliente.

Medidas:

- SAP utiliza controles y procesos para garantizar el cumplimiento con los contratos entre SAP y sus clientes, subprocesadores u otros proveedores de servicios.
- 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.
- 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.
- Para los servicios de soporte on-premise, SAP proporciona una instalación de tickets de soporte segura y diseñada específicamente en la que SAP proporciona un área de seguridad con acceso restringido y controlado para transferir los datos de acceso y las contraseñas. Los clientes de SAP tienen en todo momento control sobre sus conexiones de soporte remoto. Los empleados de SAP no pueden acceder al sistema del cliente sin el conocimiento o la participación activa completa del cliente.

1.7 Control de Disponibilidad.

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

Medidas:

- SAP utiliza procesos de copia de seguridad y otras medidas que garantizan la restauración rápida de los sistemas empresariales críticos cuando sea necesario.
- SAP utiliza un suministro eléctrico ininterrumpido (p. ej.: UPS, baterías, generadores, etc.) para garantizar el suministro de electricidad a los Centros de Datos.
- SAP ha definido planes de contingencia así como estrategias empresariales y de recuperación de desastres para los Servicios prestados.
- Los procesos y sistemas de emergencia se prueban periódicamente.

1.8 Control de Separación de Datos.

Los Datos Personales recopilados para finalidades diferentes pueden tratarse por separado.

Medidas:

- SAP utiliza funcionalidades técnicas del software implementado (por ejemplo para múltiples arrendatarios o entornos de sistema independientes) para lograr la separación de datos entre los Datos Personales originados desde varios clientes.
- Los Clientes (incluidas sus Filiales) tienen acceso solamente a sus propios datos.
- En caso de que sean necesarios Datos Personales para procesar la incidencia de soporte de un cliente específico, los datos se asignarán a este mensaje 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
- Centro de Control de la Seguridad
- Software antivirus
- Copias de seguridad y recuperación
- Pruebas de entrada internas y externas
- Auditorías externas periódicas para probar las medidas de seguridad