CONTRATO DE PROTECCIÓN DE DATOS (DPA)

Este Contrato de Protección de Datos ("DPA") es parte de un acuerdo para ciertos servicios SINCH ("Acuerdo") entre SINCH y el Cliente. El Cliente deberá poner a disposición de SINCH y el Cliente autoriza a SINCH a procesar información, incluidos los datos personales para la prestación de los Servicios en virtud del Acuerdo firmado. Las partes han acordado celebrar este Contrato de Protección de Datos, en lo sucesivo denominado simplemente "DPA", para confirmar las normas de protección de datos relacionadas con su relación, así como para cumplir con los requisitos de la Legislación de Protección de Datos aplicable.

1. DEFINICIONES

1.1 Para los efectos del presente DPA:

"Legislación de Protección de Datos" significa legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la privacidad con respecto al tratamiento de datos personales por parte del Cliente como responsable de datos, incluidas, entre otras, todas las leyes (inter)nacionales vinculantes y otras directivas vinculantes de protección de datos o seguridad de datos, leyes, reglamentos y decisiones válidos en cada momento, incluidas las directrices y códigos de práctica emitidos por la autoridad supervisora correspondiente;

"Datos Personales" significa cualquier información relacionada con una persona física identificada o identificable ("**sujeto de datos**"); una persona identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador, como un nombre, número de identificación, datos de ubicación, identificador en línea, o a uno o más factores específicos de naturaleza física, fisiológica, genética, mental, económica, cultural o social específica;

"Tratamiento de (Datos)" significa cualquier operación o conjunto de operaciones realizadas sobre Datos Personales o conjuntos de Datos Personales, ya sea por medios automatizados o no, como la recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, extracción, consulta, uso, divulgación por transmisión, difusión o disponibilidad, alineación o combinación, restricción, eliminación o destrucción;

"Datos Personales Sensibles": Datos Personales relacionados con el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos de salud, datos relativos a la vida u orientación sexuales de una persona física o cualquier otra categoría especial de datos, tal como se indica en el Anexo 2 Cambios específicos basados en la legislación nacional aplicable. o en la Orden de Servicio o Especificación de Servicio;

"Medidas técnicas y organizativas" o "**TOMs**" significa medidas diseñadas para proteger los Datos Personales de la destrucción accidental o ilegal o la pérdida accidental, alteración, divulgación o acceso no autorizado. Esto incluye los requisitos de seguridad aplicables acordados, las instrucciones de seguridad y sus actualizaciones aplicables en un momento dado, descritas en el Anexo 1 Medidas técnicas y organizativas de este DPA o en la Orden de Servicio o Especificación de servicio;

Los términos **"responsable de datos" o "controlador de datos" y "encargado de datos" o "operador de datos"** tendrán los significados asignados a ellos en el Reglamento General de Protección de Datos o GDPR.

1.2 Los términos en mayúscula utilizados y no definidos en este DPA tienen los significados asignados en el Acuerdo.

2. RESPONSABILIDAD DE LAS PARTES

Las partes entienden que para la prestación de los Servicios se hace una distinción entre dos tipos de tratamiento de Datos Personales: (i) la prestación de los servicios (es decir, la base de datos de registros y registros de datos de llamadas creados y administrados por SINCH en nombre y bajo la supervisión del Cliente) para los cuales SINCH actuará como responsable de datos y se compromete a cumplir con las obligaciones respectivas establecidas en este DPA, y (ii) la transmisión de mensajes (por ejemplo, A2P, SMS) por SINCH y otros Proveedores de Servicios para los cuales SINCH actuará como responsable de datos.

3. OBJETO, NATURALEZA Y FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE SINCH

3.1 El objeto, la naturaleza y el propósito del tratamiento de Datos Personales de conformidad con este DPA es la prestación de los Servicios por parte de SINCH de conformidad con el Acuerdo y según lo indique el Cliente en su uso de los Servicios ("Instrucciones"), a menos que sea necesario hacerlo de una manera distinta a la establecida y en la medida permitida por la Legislación de Protección de Datos y / o las leyes relevantes.

3.2 Las instrucciones del Cliente deben ser por escrito (incluyendo, pero no limitado a, correo electrónico) o pueden ser proporcionadas a través de configuraciones y uso del portal y/o software de sinch. En casos excepcionales, las Instrucciones pueden ser proporcionadas oralmente por el Cliente. Estas Instrucciones Orales serán confirmadas por la persona autorizada del Cliente por escrito o por correo electrónico (en formato de texto).

4. DURACIÓN

4.1 SINCH solo recopilará o tratará Datos Personales durante la vigencia del Acuerdo en la medida y según sea necesario para la prestación de los Servicios y de acuerdo con el DPA y la Legislación de Protección de Datos aplicable a SINCH de acuerdo con su función en el tratamiento de Datos Personales.

4.2 El tratamiento de los Datos Personales se llevará a cabo por SINCH tras la resolución del Acuerdo siempre que sea necesario para cumplir con las obligaciones de este DPA o cuando sea necesario por la obligación legal, salvo acuerdo expreso de las partes de forma diferente.

5. TIPO DE DATOS PERSONALES TRATADOS

Las siguientes categorías de Datos personales pueden procesarse para proporcionar los Servicios, cuyo alcance es determinado y controlado por el Cliente a su entera discreción y puede incluir, entre otras, las siguientes categorías de Datos personales:

- Información de contacto (empresa, correo electrónico, teléfono, dirección física)
- Nombre y apellido
- Datos identificativos
- Posición
- Función
- Empleador
- Datos de conexión
- Datos de ubicación
- Otros datos, tal como se definen en el Acuerdo, según lo acordado entre las partes.

6. TIPO DE TITULAR

El Cliente puede enviar Datos Personales a través del uso de los Servicios, cuyo alcance es determinado y controlado por el Cliente a su entera discreción, y que puede incluir, entre otros, Datos Personales relacionados con las siguientes categorías de titulares de datos:

- Clientes, socios comerciales y proveedores (que son individuos)
- Empleados de personas de contacto con clientes, socios comerciales y proveedores de clientes
- Empleados, agentes, consultores, autónomos (que son individuos)
- Usuario de los Servicios del Cliente, incluido cualquier usuario de los Servicios, que el Cliente permite utilizar los Servicios

7. SUBENCARGADOS

7.1 El Cliente acepta que SINCH puede involucrar a un Afiliado de Sinch o a terceros para tratar Datos Personales con el fin de ayudar a SINCH a proporcionar los Servicios en nombre del Cliente **("Subencargados" o "Suboperadores").** SINCH tiene o celebrará un acuerdo por escrito con cada Subencargado que contenga obligaciones de protección de datos que no sean menos estrictas que las contenidas en este DPA, en la medida en que sea aplicable a la naturaleza de los Servicios proporcionados por dicho Subencargado.

7.2 Cuando lo exija la ley, SINCH celebrará acuerdos adicionales (por ejemplo, entre otros, Contratos de Asociado Comercial según lo requerido por la Ley de Portabilidad y Responsabilidad del Seguro Médico

de 1996 ("HIPAA") y / o Tecnología de la Información de Salud para la Economía y la Ley de Salud Clínica ("HITECH").

7.3 Los Subencargados actuales de los Servicios se definen en https://www.sinch.com/data-protection-agreement/sub-processors/ ("Lista de Subencargados") y el Cliente acepta y aprueba a los Subencargados para tratar los Datos Personales que el Cliente pueda encontrar en https://www.sinch.com/data-protection-agreement/sub-processors/ un mecanismo a través del cual recibe notificaciones sobre nuevos Subencargados para cada Servicio aplicable y siempre que esté suscrito, SINCH proporcionará una notificación de los nuevos Subencargados antes de autorizar a cualquier nuevo Subencargado (s) a tratar Datos Personales en relación con la prestación del Servicio aplicable.

7.4 SINCH notificará al Cliente con 30 días de anticipación, de cualquier cambio previsto relacionado con la adición o reemplazo de cualquier Subencargado durante el cual el Cliente pueda objetar el nombramiento del Subencargado. Cualquier objeción debe hacerse inmediatamente (y en cualquier caso, a más tardar catorce (14) días después de que SINCH sea notificado de los cambios previstos). Si SINCH decide evitar que el Subencargado se oponga, SINCH le notificará al menos catorce (14) días antes de autorizar al Subencargado a tratar Datos Personales, y luego el Cliente puede interrumpir inmediatamente el uso de de los Servicios y puede terminar el Acuerdo. Cuando corresponda, SINCH le reembolsará cualquier tarifa prepagada que cubra el resto del plazo de dicha parte relevante del Servicio después de la fecha efectiva de terminación, y no hay penalización para ninguna de las partes.

7.5 SINCH puede reemplazar a un Subencargado sin previo aviso cuando la razón del cambio está fuera del control razonable de SINCH y el reemplazo inmediato es necesario por razones de seguridad u otras razones urgentes, incluidos, entre otros, el incumplimiento de un Subencargado con la Ley de Protección de Datos o DPA entre SINCH y el Subencargado. En este caso, SINCH informará al Cliente (responsable del tratamiento) sobre la sustitución del Subencargado tan pronto como sea posible tras su nombramiento. Por lo tanto, se aplica la sección 7.4.

7.6 Para evitar dudas, cuando cualquier Subencargado deje de cumplir con sus obligaciones en virtud de cualquier acuerdo de subtratamiento o bajo la ley aplicable, SINCH seguirá siendo totalmente responsable ante el Cliente por el cumplimiento de sus obligaciones en virtud de este DPA.

8. TRANSFERENCIA INTERNACIONAL

8.1 Siempre que SINCH (o sus Subencargado) traten Datos Personales en países distintos del país en el que SINCH está establecido, SINCH garantizará un nivel adecuado de protección de Datos Personales a través de medidas organizativas, técnicas y contractuales según lo exija la Legislación de Protección de Datos aplicable y este DPA.

8.2 Cuando (i) los Datos Personales de otro responsable de datos se procesan internacionalmente y dicho tratamiento internacional requiere un medio de adecuación de acuerdo con las leyes del país del responsable de datos, que incluye, entre otros, la idoneidad y el cumplimiento de las Cláusulas Contractuales Estándar Europeas aprobadas por la Comisión Europea para la transferencia de Datos Personales. El Cliente proporciona un poder notarial para que SINCH celebre cualquier Cláusula Contractual Estándar Europea aprobada por la Comisión Europea con un Subencargado aprobado según lo establecido en la cláusula 7 en nombre del Cliente, o cuando (ii) los Datos Personales de un encargado de Datos con sede en el Espacio Económico Europeo (EEE) o Suiza se procesan en un país fuera del EEE, Suiza y cualquier país, organización o territorio reconocido por la Unión Europea como un país seguro con un nivel adecuado de protección de datos en virtud del art. 45 del GDPR y ningún otro mecanismo de transferencia legal, como las Normas Corporativas Vinculantes (art. 47 del GDPR o el Código de Conducta (art. 40 del GDPR).

8.3 Cuando la Comisión Europea apruebe las Cláusulas Contractuales Tipo Europeas celebradas entre SINCH y el Cliente, sus cláusulas se aplicarán hasta que una autoridad de control competente de un Estado miembro, o un tribunal de la Unión Europea o un Estado miembro competente apruebe un nuevo mecanismo de transferencia legal aplicable a las transferencias de datos cubiertas por las Cláusulas Contractuales Tipo Europeas (en el caso de que dicho mecanismo se aplique solo a algunas de las transferencias de Las cláusulas contractuales tipo europeas seguirán siendo aplicables a las transferencias que no puedan ser cubiertas por el nuevo mecanismo de transferencia legal):

(i) Los derechos otorgados a los titulares en virtud de este DPA y las Cláusulas Contractuales Tipo Europeas pueden ser aplicados por el titular contra SINCH, independientemente de cualquier restricción en las Cláusulas 3 o 6 de las Cláusulas Contractuales Estándar Europeas. Sus derechos son personales y no pueden ser atribuidos a terceros. El titular solo puede presentar una reclamación en

virtud de este DPA y las Cláusulas Contractuales Estándar Europeas individualmente, y no como parte de una demanda colectiva, grupo o representante.

(ii) Además de la Cláusula 5 (b) de las Cláusulas Contractuales Tipo Europeas, SINCH acepta que, en el momento de la celebración de este DPA, no tiene ninguna razón para creer que la legislación aplicable a SINCH o su Subencargado, incluso en cualquier país donde los Datos Personales sean transferidos por SINCH o a través de un Subencargado, le impide cumplir con las instrucciones recibidas del Cliente y sus obligaciones en virtud de las Cláusulas Contractuales Estándar Europeas y que, en caso de un cambio en esta legislación, que pueda tener un efecto adverso en las garantías y obligaciones previstas en las Cláusulas Contractuales Tipo Europeas, notificará al Cliente el cambio tan pronto como tenga conocimiento, en cuyo caso tiene derecho a suspender la transferencia de datos y / o rescindir el DPA.

(iii) A los efectos de esta sección, los esfuerzos legales no incluyen acciones que resultarían en sanciones civiles o penales, como el desacato al tribunal bajo las leyes de la jurisdicción pertinente:

- Si SINCH recibe una solicitud de terceros para la divulgación forzosa de cualquier Dato Personal que haya sido transferido de acuerdo con las Cláusulas Contractuales Estándar Europeas, SINCH redirigirá, cuando sea posible, al tercero para que solicite datos directamente al Cliente.

- Si SINCH recibe una solicitud de cualquier tercero para la divulgación forzada de cualquier Dato Personal que haya sido transferido de acuerdo con las Cláusulas Contractuales Tipo Europeas, SINCH hará todos los esfuerzos legales para impugnar la solicitud de divulgación basada en cualquier deficiencia legal bajo las leyes de la Parte solicitante o cualquier conflicto relevante con la ley de la Unión Europea o las leyes aplicables de los Estados miembros.

9. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

SINCH ha implementado y mantiene medidas técnicas y organizativas apropiadas para proteger los Datos Personales procesados contra el tratamiento no autorizado o ilegal y contra la pérdida, destrucción, daño, alteración o divulgación accidentales. Estas medidas se describen en el Anexo 1 *Medidas técnicas y organizativas.*

10. GARANTÍAS DE CALIDAD SINCH Y OTRAS FUNCIONES

10.1 SINCH debe cumplir con los siguientes requisitos, entre ellos:

- no realizar ningún tratamiento de Datos Personales, excepto por instrucciones del responsable de Datos y / o cuando lo exija una autoridad bajo la ley;
- implementar un registro de tratamiento de datos
- implementar medidas técnicas y organizativas para garantizar un nivel de seguridad de los datos adecuado al nivel de riesgo que presenta el tratamiento de los Datos personales;
- cooperar con la autoridad de control de la protección de datos en el desempeño de sus funciones
- notificar, cuando resulte procedente, la violación de los Datos Personales a la autoridad supervisora y al titular;
- realizar una evaluación de impacto de la protección de datos cuando sea necesario de conformidad con la ley y consultar con la autoridad de control antes del tratamiento de datos, cuando la evaluación de impacto de la protección de datos indique que el tratamiento daría lugar a un alto riesgo en ausencia de medidas adoptadas por el responsable de datos para mitigar el riesgo.

y garantiza, en particular, el cumplimiento de los siguientes requisitos:

a) Designar a un oficial de protección de datos, que desempeñará sus funciones de conformidad con la legislación de protección de datos. Los datos de contacto del oficial de protección de datos (DPO) están disponibles en la página web oficial de SINCH. Si la parte contratada de SINCH no está establecida en la Unión Europea, SINCH designará a una persona de contacto responsable en la Unión Europea y/o a un delegado de protección de datos de conformidad con la legislación de protección de datos aplicable.

b) Confidencialidad de acuerdo con la legislación de protección de datos. SINCH confía el tratamiento de datos descrito en este DPA solo a empleados que están sujetos a confidencialidad y que han estado previamente familiarizados con las disposiciones de protección de datos relevantes para su trabajo. SINCH y cualquier persona que actúe bajo su autoridad y que tenga acceso a los Datos Personales no tratarán dichos datos a menos que se mediante las instrucciones del Cliente (que incluyen los poderes otorgados en este DPA), y / o a menos que lo exija la Legislación de Protección de Datos.

c) A expensas y gastos del Cliente y teniendo en cuenta la naturaleza del tratamiento y la información disponible para SINCH, proporcionar la información y la asistencia que el Cliente pueda requerir razonablemente y dentro de los límites de tiempo razonablemente especificados por el Cliente para ayudar al Cliente a cumplir con sus obligaciones en virtud de la Legislación de Protección de Datos aplicable, lo

que puede incluir ayudar al Cliente a:

i) notificar al Cliente de cualquier solicitud que SINCH reciba a un titular en relación con los Datos Personales tratados y notificar al titular para que se ponga en contacto con el Cliente si desea utilizar sus derechos;
ii) cumplir con sus obligaciones de seguridad;
iii) cumplir con sus obligaciones de responder a las solicitudes relacionadas con el ejercicio de los derechos del titular, incluido el derecho de acceso, el derecho de rectificación, el derecho de pago ("derecho al olvido") el derecho de restricción del tratamiento (en la medida en que los datos personales no sean accesibles para el Cliente a través de los Servicios); llevar a cabo la evaluación de impacto de la protección de datos y auditar el cumplimiento de la evaluación de impacto de la protección de datos y consultar con la autoridad de control;
iv) seguir la Evaluación de Impacto de Protección de Datos.

d) Para efectos de esta sección, los esfuerzos legales no incluyen acciones que resultarían en sanciones civiles o penales, como el desacato al tribunal bajo las leyes de la jurisdicción pertinente:

i) A menos que lo prohíba la ley aplicable o una solicitud de aplicación de la ley vinculante, SINCH notificará inmediatamente al cliente de cualquier solicitud de cualquier funcionario gubernamental, autoridad supervisora de protección de datos o autoridad policial en relación con cualquier dato personal y, si se le prohíbe notificar al cliente, SINCH hará todos los esfuerzos legales para obtener el derecho a renunciar a la prohibición con el fin de comunicar tanto como sea posible. información al Cliente lo antes posible;

e) SINCH supervisará periódicamente los procesos internos y los TOMs para garantizar que el tratamiento dentro del área de responsabilidad de SINCH esté de acuerdo con los requisitos de la Legislación de Protección de Datos y la protección de los derechos del titular.

11. AUDITORÍAS E INSPECCIONES

11.1 En el caso de que el Cliente, un Regulador o autoridad de protección de datos requiera información adicional o una auditoría relacionada con los Servicios, SINCH acepta otorgar acceso a sus instalaciones de procesamiento de datos, archivos de datos y documentación necesaria para el procesamiento de Datos Personales. SINCH se compromete a proporcionar una cooperación razonable durante dichas operaciones, incluida la provisión de toda la información relevante y el acceso a todos los equipos, software, datos, archivos, sistemas de información, etc., utilizados para el desempeño de los Servicios, incluido el tratamiento de Datos Personales.

11.2 El derecho de auditoría, tal como se describe en la cláusula 11.1, se aplicará al Cliente si SINCH no ha proporcionado pruebas suficientes de su cumplimiento de las medidas técnicas y organizativas. La evidencia suficiente incluye proporcionar: (i) una certificación para el CUMPLIMIENTO DE LA NORMA ISO 27001 u otras normas implementadas por EL SINCH (alcance según se define en el certificado); o (ii) un informe de auditoría o certificación de un tercero independiente. Una auditoría como se describe en la cláusula 11.1 se llevará a cabo a cargo del Cliente. El Cliente o cualquier tercero puede realizar una auditoría razonablemente aceptable para SINCH (que no incluirá a ningún auditor externo que sea competidor de SINCH o no esté debidamente calificado o independiente) para verificar el cumplimiento de este DPA, así como el cumplimiento de las medidas técnicas y organizativas de SINCH, siempre que con un aviso razonable de al menos treinta (30) días y la conclusión de un acuerdo de no divulgación directamente entre SINCH y el auditor externo.

12. NOTIFICACIÓN DE VIOLACIÓN DE DATOS

12.1 Si SINCH tiene conocimiento de cualquier violación de seguridad que resulte en la destrucción accidental, no autorizada o ilegal ola divulgación no autorizada de usted en el acceso a los Datos personales, SINCH deberá, entre otras cosas:

a) Notificar al Cliente por escrito inmediatamente, pero no después de 72 horas después de tener conocimiento de la violación de los Datos Personales;

b) Asistir al Cliente con respecto a la obligación del Cliente de proporcionar información al titular y de proporcionar al Cliente información relevante a este respecto;

c) Apoyar al Cliente en consultas (Q&A) con la autoridad de protección de datos.

12.2 En la medida de lo legalmente posible, SINCH puede reclamar una compensación por los servicios de soporte en virtud de esta cláusula 12 que no sean atribuibles a violaciones de Datos Personales causadas por SINCH.

13. ELIMINACIÓN DE DATOS PERSONALES

13.1 SINCH está obligado a eliminar los Datos Personales según lo estipulado en el Acuerdo y de acuerdo con la Legislación de Protección de Datos y / o las leyes relevantes.

13.2 El Cliente tiene derecho a solicitar el cumplimiento de los derechos y obligaciones descritos en la cláusula 13.1 durante la duración de todo el DPA.

13.3 Las obligaciones legales de retención u obligaciones contractuales con los Proveedores de Servicios de SINCH (por ejemplo, pero no limitados a los operadores) permanecerán inalterados por las disposiciones anteriores. La documentación que sirva como evidencia para un procesamiento ordenado de datos de acuerdo con las disposiciones del DPA será retenida por SINCH al finalizar el DPA de acuerdo con la Legislación de Protección de Datos y / o las leyes relevantes.

14. OBLIGACIONES DE SINCH COMO RESPONSABLE DEL TRATAMIENTO

En situaciones en las que SINCH actuará como responsable de datos, se compromete a cumplir con sus obligaciones en virtud de la Legislación de Protección de Datos aplicable en relación con cualquier dato personal tratado en relación con el Acuerdo y los Servicios. SINCH procesará dichos datos personales en relación con la transmisión de mensajes y para cumplir con sus obligaciones asociadas en virtud del Acuerdo o según lo exija la ley, una orden judicial o cualquier autoridad gubernamental o reguladora y de acuerdo con su política de privacidad, que está disponible en https://www.sinch.com/privacy-policy/ según se modifique de vez en cuando, si es necesario.

15. OBLIGACIONES DEL CLIENTE

El Cliente deberá cumplir en todo momento con la Legislación de Protección de Datos en relación con el tratamiento de Datos Personales en relación con el Acuerdo y los Servicios. El Cliente deberá informar a SINCH por escrito si se aplica legislación adicional al Tratamiento de Datos Personales que no sea la ley del país donde el Cliente está establecido.

16. LIMITACIÓN DE RESPONSABILIDAD

16.1 La responsabilidad de cada parte y todos sus Afiliados, que surja de o esté relacionada con este DPA, ya sea por contrato, agravio o bajo cualquier otra teoría de responsabilidad, está sujeta a la sección de Limitación de Responsabilidad del Acuerdo, y cualquier referencia en dicha sección a la responsabilidad de una parte significa la responsabilidad agregada de esa parte y todos sus Afiliados en virtud del Acuerdo y ese DPA.

16.2 La cláusula 16.1 no se aplica si el daño fue causado por la implementación incorrecta del servicio pedido realizado por el cliente o por una instrucción dada por el Cliente. En este caso, el Cliente será responsable de dichos daños.

17. DISPOSICIONES DIVERSAS

17.1 DPA es una parte integral del Acuerdo entre el Cliente y SINCH. En caso de conflicto entre las disposiciones obligatorias de las Cláusulas Contractuales Tipo Europeas y este DPA, prevalecerán las Cláusulas Contractuales Tipo Europeas. En caso de otros conflictos entre otros documentos (incluso en el caso de un conflicto entre el Acuerdo y este DPA), prevalecerá el DPA.

17.2 Si alguna disposición de este DPA es o se vuelve inválida o contiene una laguna, las disposiciones restantes no se verán afectadas. El Cliente y SINCH se comprometen a reemplazar la disposición inválida con disposiciones legalmente válidas que estén más cerca del interés de la disposición inválida, respectivamente, lo que llena el vacío.

ANEXO 1 del Acuerdo de Protección de Datos - Medidas técnicas y organizativas

SINCH implementará las medidas descritas en este Anexo 1, siempre que las medidas contribuyan directa o indirectamente o puedan contribuir a la protección de Datos Personales en virtud del Acuerdo celebrado entre las partes para el tratamiento de datos.

Las medidas técnicas y organizativas que se implementan por EL SINCH se basan en el estado actual de la tecnología, los costos de implementación y la naturaleza, alcance, circunstancias y propósitos del tratamiento, y la probabilidad y gravedad del riesgo para los derechos y libertades de las personas son ciertos. Las medidas técnicas y organizativas están sujetas al progreso técnico y al desarrollo. En este sentido, el SINCH está autorizado a implementar medidas alternativas apropiadas. El nivel de seguridad debe estar alineado con las mejores prácticas de seguridad del sector y no menos que las medidas aquí establecidas. Todos los cambios importantes deben ser acordados con el Cliente y documentados.

Las Medidas Técnicas y Organizativas incluidas en este Anexo 1 son medidas aplicables a los Servicios prestados por el SINCH. Si es necesario, para el Servicio, SINCH puede incluir otras medidas técnicas y organizativas en la Orden de Servicio o especificación del Servicio.

1 Gestión de riesgos y procedimientos de validación, revisión y evaluación

i. El SINCH identificará y evaluará los riesgos de seguridad relacionados con la confidencialidad, la integridad y la disponibilidad y, sobre la base de esta evaluación, implementará las medidas técnicas y organizativas adecuadas para garantizar un nivel adecuado de seguridad para el riesgo.

ii. SINCH deberá tener procesos y rutinas documentadas para abordar los riesgos en sus operaciones y mediante el tratamiento de datos personales en nombre del Cliente.

iii. El SINCH debe evaluar periódicamente los riesgos relacionados con los sistemas de información y el tratamiento, almacenamiento y transmisión de información.

iv. SINCH identificará y evaluará los riesgos de seguridad relacionados con la confidencialidad, integridad y disponibilidad y, sobre la base de dicha evaluación, implementará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de los tipos y propósitos específicos de Datos Personales que sean procesados por SINCH, incluyendo pero no limitado a:

   a) La pseudonimización y el cifrado de Datos Personales;
   b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas y servicios de tratamiento;
   c) La capacidad de restaurar la disponibilidad y el acceso a los Datos del Cliente de manera oportuna en caso de un incidente físico o técnico;

v. Un proceso para probar, evaluar y evaluar regularmente la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

vi. El SINCH debe evaluar periódicamente los riesgos relacionados con los sistemas de información y el tratamiento de datos personales (por ejemplo, al almacenar y transmitir datos personales).

vii. SINCH supervisará, revisará y auditará regularmente el cumplimiento del Subencargado con las Medidas Técnicas y Organizativas y SINCH, a petición del Cliente, proporcionará al Cliente evidencia del cumplimiento del Subencargado con las medidas técnicas y organizativas.

viii. SINCH operará de acuerdo con los principios de protección de datos desde el diseño y por defecto y debe proporcionar documentación suficiente de la implementación de la protección de datos desde el diseño y por defecto.

2 Medidas organizativas

La organización interna del operador de datos debe cumplir con requisitos específicos de protección de datos.

A. Políticas y gestión de políticas

i. SinCH debe tener un sistema de gestión de seguridad de la información (SGSI) definido y documentado, que incluya una política y procedimientos de seguridad de la información existentes, que deben ser aprobados por la administración de SINCH. Deben publicarse dentro de la organización SINCH y comunicarse a las personas relevantes de SINCH.

ii. Sinch revisará periódicamente las políticas y procedimientos de protección de datos y seguridad de la información de SINCH y los actualizará, si es necesario, para garantizar el cumplimiento de las Medidas Técnicas y Organizativas y DPA.

B. Organización de Protección de Datos y Seguridad de la Información

i. SINCH designará al menos a una persona responsable del tratamiento de los datos personales con las competencias adecuadas y que actúe como principal contacto de protección de datos. Si así lo exige la ley, SINCH nombrará un oficial de protección de datos a nivel de empresa.

ii. SINCH debe tener definidas las funciones y responsabilidades de seguridad y documentación en su organización.

C. Requisitos organizativos

i. SINCH se asegurará de que el personal de SINCH trate la información de acuerdo con el nivel de confidencialidad requerido por el DPA y que tenga el compromiso por escrito de los empleados de mantener la confidencialidad.

ii. SINCH se asegurará de que las personas relevantes de SINCH conozcan el uso aprobado (incluidas las restricciones de uso, según sea el caso) de la información, las instalaciones y los sistemas bajo el DPA.

iii. SINCH se asegurará de que cualquier personal de SINCH que realice tareas bajo el DPA sea de confianza, cumpla con los criterios de seguridad establecidos y haya sido, y durante el período de asignación, sujeto a la selección y verificación de antecedentes apropiadas (si lo permite la ley aplicable).

iv. SINCH debe asegurarse de que el personal de SINCH con responsabilidades de seguridad esté debidamente capacitado para realizar tareas relacionadas con la seguridad.

v. SINCH proporcionará o garantizará la capacitación periódica de sensibilización para el personal pertinente del SINCH. Esta capacitación debe incluir, sin limitación:

a) Cómo lidiar con la seguridad de la información del Cliente (es decir, la protección de la confidencialidad, integridad y disponibilidad de la información);
b) Porqué la seguridad de la información es necesaria para proteger la información y los sistemas de los clientes;
c) Los tipos comunes de amenazas de seguridad (como robo de identidad, malware, *piratería,*fuga de información y amenazas internas);
d) La importancia de cumplir con las políticas de seguridad de la información y aplicar los estándares/procedimientos asociados;
e) Responsabilidad personal por la seguridad de la información (como proteger la información relacionada con la privacidad del Cliente y reportar violaciones de datos reales y sospechosas).

3 Confidencialidad

A. Control de Acceso (Seguridad Física y Ambiental)

i. SINCH debe proteger las instalaciones de tratamiento de información de amenazas y riesgos externos y ambientales, incluidas las fallas de energía / cableado y otras interrupciones causadas por fallas en apoyo de los servicios públicos. Esto incluye el perímetro físico y la protección de acceso.
ii. SINCH protegerá la propiedad del robo, la manipulación y la destrucción.
iii. SINCH especificará las personas autorizadas permitidas en sus instalaciones de tratamiento y tendrá un proceso de control de acceso.
iv. Medidas adicionales para centros de datos:
a) Todos los centros de datos admiten procedimientos de seguridad estrictos respaldados por guardias, cámaras de vigilancia, detectores de movimiento, mecanismos de control de acceso y otras medidas para evitar que los equipos e instalaciones del centro de datos se vean comprometidos.
b) Solo los representantes autorizados tienen acceso a los sistemas y la infraestructura dentro de las instalaciones del Centro de Datos.
c) Para proteger la funcionalidad adecuada, el equipo de seguridad física (por ejemplo, sensores de movimiento, cámaras, etc.) se somete a un mantenimiento regular.
d) SINCH y todos los proveedores de centros de datos de terceros registran los nombres y las horas del personal autorizado que ingresa a las áreas privadas de SINCH dentro de los centros de datos.

B. Control de acceso (Lógico)

i. SINCH debe tener una política de control de acceso definida y documentada para instalaciones, sitios, red, sistema, aplicación y acceso a información/datos (incluidos los controles de acceso físicos, lógicos y remotos), un proceso de autorización para el acceso y los privilegios de los usuarios, procedimientos para revocar los derechos de acceso y un uso aceptable de los privilegios de acceso para el personal local de SINCH.
ii. SINCH debe tener un registro de usuario formal y documentado y un proceso de cancelación de registro implementado para permitir la asignación de derechos de acceso.
iii. SINCH debe tener un *proceso de joiner-mover-leaver* para sus empleados.
iv. SINCH asignará todos los privilegios de acceso basados en el principio de la necesidad de tomar conciencia y el principio del privilegio mínimo.
v. SINCH debe utilizar una autenticación fuerte (multifactorial) para los usuarios de acceso remoto y los usuarios que se conectan desde una red que no es de confianza.

vi. SINCH se asegurará de que el personal del SINCH disponga de un identificador único y personal (ID de usuario) y utilice una técnica de autenticación adecuada que confirme y garantice la identidad de los usuarios.

C. Cifrado/Pseudonimización/Anonimización

i. SINCH garantizará el uso adecuado y efectivo del cifrado en la información clasificada como confidencial y secreta (como los datos personales).
ii. SINCH debe proteger las claves criptográficas y almacenarlas de acuerdo con la ley aplicable.
iii. SINCH implementará las medidas apropiadas para la pseudonimización (reemplazando los identificadores personales con información no personal) cuando corresponda.
iv. SINCH implementará las medidas apropiadas para el anonimato (desidentificación de identificadores personales con información no personal) cuando corresponda.

D. Directrices sobre la admisión a las instalaciones del Cliente y/o a las instalaciones del SINCH.

La autorización para el acceso a instalaciones y propiedades (como edificios de centros de datos, edificios de oficinas, ubicaciones técnicas) está sujeta a lo siguiente:

i. SINCH cumplirá con las regulaciones locales (como las regulaciones para "áreas restringidas") para las instalaciones del Cliente al hacer la cesión bajo el Acuerdo.
ii. El personal del SINCH debe llevar una tarjeta de identificación o, en el caso de los visitantes, una credencial de visitante, visible todo el tiempo durante el trabajo.
iii. Al finalizar la tarea, o cuando el personal del SINCH sea transferido a otras tareas, el personal debe, sin demora, informar al personal autorizado del cambio y devolver las llaves, tarjetas clave, certificados, credenciales de visitante y artículos similares.
iv. Las llaves o tarjetas de acceso deben ser firmadas personalmente por el personal de SINCH y deben manejarse de acuerdo con las reglas escritas dadas al momento de la recepción.
v. La pérdida de la llave o tarjeta de acceso debe ser comunicada sin demora al personal autorizado.
vi. Está prohibido disparar dentro de las instalaciones sin permiso.
vii. Las mercancías no deben retirarse de las instalaciones sin permiso.
viii. El personal del SINCH no debe permitir el acceso de personas no autorizadas a las instalaciones.

4 Seguridad de las operaciones

i. SinCH debe contar con un sistema de gestión de cambios para realizar cambios en los procesos comerciales, las instalaciones y los sistemas de tratamiento de información. El sistema de gestión de cambios debe incluir pruebas y revisiones antes de que se implementen los cambios, como procedimientos para tratar los cambios urgentes, procedimientos de reversión para recuperarse de cambios fallidos, registros que muestren qué ha cambiado, cuándo y por quién.
ii. SINCH implementará protección contra malware para garantizar que cualquier software utilizado para proporcionar los Servicios SINCH al cliente esté protegido contra el malware.
iii. La red SINCH está protegida de la red pública por firewall.
iv. SINCH realizará copias de seguridad de la información crítica y probará copias de seguridad para garantizar que la información se pueda restaurar según lo acordado con el Cliente.
v. SINCH registrará y supervisará actividades como la creación, lectura, copia, alteración y eliminación de los datos tratados, así como las excepciones, fallos y eventos de seguridad de la información y los revisará periódicamente. Además, SINCH protegerá y almacenará (durante al menos 6 meses o durante el período (s) definido por la Legislación de Protección de Datos) la información de registro y, previa solicitud, proporcionará datos de monitoreo del cliente. Las anomalías/incidentes/indicadores de compromiso deben notificarse de conformidad con los requisitos de gestión de la violación de datos que se establecen a continuación.
vi. SINCH debe gestionar las vulnerabilidades de todas las tecnologías relevantes, como sistemas operativos, bases de datos, aplicaciones de manera proactiva y oportuna.
vii. SINCH debe establecer líneas de base de seguridad (refuerzo) para todas las tecnologías relevantes, como sistemas operativos, bases de datos, aplicaciones.
viii. SINCH debe garantizar que el desarrollo esté separado del entorno de prueba y producción.

5 Integridad

i. SINCH debe implementar controles de seguridad de red como el nivel de servicio, el firewall y la segregación para proteger los sistemas de información.
ii. SINCH opera un sistema de detección de phishing y SPAM para proteger a sus clientes y a SINCH (y los Datos Personales de los cuales las partes son el Controlador) del contenido no deseado y la propagación de SPAM / phishing y cumplir con los requisitos del operador y la legislación aplicable. El sistema recupera las URL del cuerpo del mensaje de solicitud terminado por el dispositivo móvil y, a continuación, habilita la validación de URL emitiendo una solicitud de método GET a la URL y expandiéndola a la URL completa como si estuviera en la barra de direcciones del navegador. Si es necesario, debido a información insuficiente o contenido sospechoso de no conformidad, toda la página puede cargarse y

analizarse, incluido el contenido de esa página. Se trata de un *algoritmo de machine learning* (con validación humana) diseñado para aprender del phishing confirmado y la detección de SPAM y que los datos se utilizarán para este fin dentro del grupo SINCH. SINCH no proporcionará ni enviará datos personales de los que el cliente sea el controlador a terceros fuera del Grupo SINCH, excepto a los Suboperadores necesarios para proporcionar esta funcionalidad.

iii. Los Datos Personales tratados en nombre del Cliente se procesarán exclusivamente de acuerdo con el DPA y las instrucciones del responsable de datos.

iv. SINCH trabajará de acuerdo con instrucciones escritas o acuerdos y documentos relacionados con este DPA.

6 Gestión de brechas de datos

i. SINCH debe tener procedimientos establecidos para la gestión de violaciones de datos.

ii. SINCH le informará de cualquier violación de datos (incluidos, entre otros, incidentes relacionados con el tratamiento de datos personales) lo antes posible, pero a más tardar 72 horas después de que se haya identificado la violación de datos.

iii. Todos los informes de incidentes relacionados con la seguridad deben tratarse como información confidencial y cifrada, utilizando métodos de cifrado estándar de la industria.

iv. El informe de violación de datos debe contener al menos la siguiente información:

a) La naturaleza de la violación de datos,
b) La naturaleza de los datos personales afectados,
c) Las categorías y el número de titulares afectados,
d) El número de registros de datos personales en cuestión,
e) Las medidas adoptadas para hacer frente a la violación de datos,
f) Las posibles consecuencias y efectos adversos de la violación de datos, y
g) Cualquier otra información que el Cliente deba informar al regulador o al titular correspondiente.

En la medida de lo legalmente posible, SINCH puede reclamar una compensación por los servicios de soporte bajo esta cláusula que no son atribuibles a fallas por parte de SINCH.

7 Gestión de la continuidad del negocio

i. SINCH debe identificar los riesgos de continuidad del negocio y tomar las medidas necesarias para controlar y mitigar esos riesgos.

ii. SINCH debe tener procesos y rutinas documentados para manejar la continuidad del negocio.

iii. SINCH debe garantizar que la seguridad de la información se incorpore en los planes de continuidad del negocio.

iv. SINCH debe evaluar periódicamente la eficiencia de su gestión de la continuidad del negocio y el cumplimiento de los requisitos de disponibilidad (si los hubiera).

8 Desarrollo y mantenimiento de sistemas/software (cuando el desarrollo de software o el desarrollo de sistemas es proporcionado al Cliente por SINCH)

i. SINCH debe implementar reglas para el ciclo de vida de desarrollo de software y sistemas, incluidos los procedimientos de cambio y revisión.

ii. SINCH debe probar la funcionalidad de seguridad durante el desarrollo en un entorno controlado.

iii. La administración de parches de seguridad se implementa para proporcionar una implementación regular y periódica de las actualizaciones de seguridad relevantes.

iv. SINCH trabajará de acuerdo con los principios de protección de datos*"por diseño y por* defecto" y proporcionará documentación suficiente de la implementación de la protección de datos *"por diseño y por defecto".*

Anexo 2 del Acuerdo de protección de datos - NORMAS ESPECÍFICAS sobre la base de la legislación nacional aplicable

1. España

Si el Controlador / Operador se encuentra en España, las medidas técnicas y organizativas que debe tomar el Operador están sujetas a las leyes de protección de datos de España. En este caso, el preámbulo del anexo 1 del presente Acuerdo de Acción de Las Comunicaciones debe completarse como sigue:

"El Operador velará por que las siguientes medidas técnicas y organizativas cumplan con las medidas de "seguridad de alto nivel" de conformidad con el Real Decreto 1720/2007 Título VIII, Art. 80 y ss. El operador aplicará, en particular, los requisitos del apartado tres (art. 89 y siguientes) del Real Decreto 1720/2007, si los requisitos del presente anexo 1 no cumplen dichos requisitos. En este caso, el Operador informará al Controlador y presentará cualquier cambio o desviación de este Anexo 1 que considere necesario para la aprobación previa del Controlador".

2. Canadá

La definición de "Datos Personales Sensibles" en la Cláusula 1 de este DPA se considerará de la siguiente manera:

"Datos personales sensibles" significa información sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual, o cualquier otro personal que pueda considerarse datos confidenciales según la ley aplicable".

Además de lo acordado en este DPA, se aplicará en relación con la transferencia de datos:

"El Controlador reconoce que el Operador puede transferir, almacenar y procesar Datos Personales a territorios fuera de Canadá, donde estarán sujetos a las leyes de las jurisdicciones extranjeras en las que se mantienen. El Operador no deberá, y deberá, estar seguro de que cualquier Afiliado o cualquier tercero con el que contrate para Procesar Datos Personales en su nombre en relación con los Servicios relevantes, no:

- transferir Datos personales a un territorio fuera de Canadá, excepto en términos sustancialmente similares a los términos del presente documento, que se acuerdan antes de dicha transferencia; o
- operar en relación con dichos Datos personales de cualquier manera que incumpla al Controlador sus obligaciones de acuerdo con las leyes de privacidad aplicables".

Además de lo acordado en este DPA:

"El Controlador reconoce que tiene todos los consentimientos necesarios y la autoridad legal de los titulares que permitirían al Operador procesar los datos".

Además de lo acordado en la Sección 7 de este DPA:

"Las partes también cooperarán con respecto a cualquier aviso de violación de datos a las autoridades reguladoras canadienses, individuos y otras organizaciones que sean requeridos por la ley o aconsejables a la entera discreción del Controlador".

Sin limitar los términos y condiciones del DPA a Canadá y el Acuerdo, en la medida en que sea aplicable en Canadá, se aplica lo siguiente:

"El Operador deberá cumplir con todas las leyes canadienses de privacidad y antispam federales y provinciales aplicables al Controlador y al Operador en el curso del tratamiento de cualquier Dato en relación con los Servicios, incluidos todos los requisitos aplicables para la notificación, el consentimiento, el contenido y la cancelación de suscripción con respecto al envío de mensajes electrónicos y la instalación de programas informáticos en el dispositivo de otra persona.

El Operador dispondrá que el acceso a los Datos se limite solo a los empleados y agentes autorizados del Operador que necesiten acceso a los Datos Personales únicamente con el fin de procesar los Servicios por parte del Operador".

3. Australia

Siguiendo las directrices australianas de protección de datos (Principios de privacidad australianos; APP) del Anexo 1 de la "Ley de Enmienda de Privacidad (Mejora de la Protección de la Privacidad) de 2012", que es un complemento de la "Ley de Privacidad de 1988", lo siguiente se aplica al tratamiento de Datos Personales:

(i) "Controlador" significa una persona que, sola o en conjunto con otras personas, establece los objetivos y la forma de tratamiento de datos personales; y "Operador" significa cualquier persona (que no sea un empleado del Controlador) que, en nombre del Controlador, trate datos personales.

(ii) Cuando un Controlador o sus Usuarios Autorizados en Australia tengan la intención de recopilar Datos Personales en el Servicio en la Nube, el Controlador se compromete a obtener el consentimiento previo de cada Sujeto de Datos a una Transferencia Internacional de acuerdo con este Programa si, y en la medida necesaria de acuerdo con la Ley de Privacidad. El Controlador confirma que ha recibido los datos personales e informado a las partes interesadas sobre la divulgación de datos personales de acuerdo con la APP y la Ley de Privacidad de 1988. En base a esto, el requisito de "Consentimiento Libre e Informado" en el punto 8.1 de la APP se considera cumplido debido a la excepción de "Consentimiento Libre e Informado". Mientras no se aplique el consentimiento informado, este Cronograma proporciona el marco para la protección de los Datos Personales de los afectados en Australia, en la medida en que proporcione al menos esencialmente la misma privacidad que la APP, y el Operador y sus Suboperadores se comprometan a un nivel de protección de datos que sea el mismo que el establecido en las Secciones 2, 3 y 6 del presente anexo (excepción a la "Ley sustancialmente similar" en virtud del apartado a) del punto 8.2 de la APP). Para ello se cumple el requisito establecido en la APP 8.1 de "Ley Sustancialmente Similar" a tal efecto.

4. Reino Unido

En la medida en que una Ley de Protección de Datos (incluido el nuevo Reglamento Básico de Protección de Datos de la Unión Europea o su sucesor después de que Gran Bretaña abandone la Unión Europea) entre en vigor después de la fecha de entrada en vigor de este DPA y sea contraria a los términos de este DPA o requiera una enmienda a este DPA, una de las partes podrá notificar a la otra parte para comenzar a negociar los cambios necesarios en este DPA de conformidad con el principio de buena fe.

5. Suiza

De acuerdo con el art. 3 lit. (b) de la Ley Federal Suiza de 19 de junio de 1992 sobre Protección de Datos (FADP), las definiciones de la cláusula 1 de este DPA se considerarán de la siguiente manera:
"Sujeto de datos"**:** personas físicas o jurídicas cuyos datos son tratados.

6. Italia

De conformidad con el artículo 29 del Código italiano de protección de datos personales, es necesario indicar el operador de datos de conformidad con la legislación italiana y describir las tareas específicas que tienen de conformidad con el Código de protección de datos italiano. Cuando firma este DPA, el Controlador indica al Operador como Operador de Datos. El Operador de Datos tratará los datos de acuerdo con la normativa y medidas de seguridad previstas en el Decreto Legislativo Nº 196/2003 e identificados en el Anexo B de las mismas "Especificaciones técnicas relativas a las medidas mínimas de seguridad" y las normas y medidas de seguridad que se proporcionarán como actualizaciones de las aquí contenidas. Las medidas que deben adoptarse se describen en el presente DPA y en sus anexos.

Específicamente, el Operador de Datos se compromete a realizar sus funciones estrictamente de acuerdo con las Instrucciones que le proporcione el Controlador de Datos, y deberá, de conformidad con el Art. 29, párrafo 5 del Decreto Legislativo No. 196/2003, supervisar el cumplimiento oportuno de las tareas asignadas al Operador de Datos.

El Operador de Datos se compromete a:

- proporcionar los servicios de tratamiento de datos descritos en el DPA, en particular comprometiéndose a completar cualquier operación de tratamiento o conjunto de operaciones, con o sin la ayuda de medios electrónicos, con respecto a la recopilación, registro, organización, almacenamiento, consulta, tratamiento, modificación, selección, extracción, comparación, uso, interconexión, bloqueo, comunicación, difusión, cancelación y destrucción de datos, incluso si no están registrados en una base de datos;
- realizar los Servicios de acuerdo con los requisitos de protección de datos y solo para los fines previstos como se describe en el DPA. El Operador de Datos está obligado a salvaguardar la confidencialidad de los datos de acuerdo con la legislación de protección de datos, en particular el Operador de Datos se compromete a completar las operaciones de tratamiento de datos a las que se hace referencia en este documento de una manera legal y adecuada, que proporcione la máxima confidencialidad y también proporcione de manera oportuna y pleno cumplimiento de las leyes y regulaciones aplicables;

- aplicar medidas para que todo el personal a cargo del manejo de datos lo haga de acuerdo con las leyes y regulaciones vigentes, así como con las Instrucciones previstas en las mismas;
- si su tratamiento de Datos Personales cumple con los requisitos establecidos por el Decreto Legislativo Nº 196/2003,
- almacenar los datos personales recopilados de acuerdo con las medidas de seguridad previstas en los art. 31 y siguientes. Decreto Legislativo 196/2003, que garantiza el cumplimiento de las medidas mínimas de seguridad.

Tanto el Controlador como el Operador reconocen que las Medidas Técnicas y Organizativas del Anexo 1 del DPA son actualmente suficientes para cumplir con las medidas del Art. 31 ysiguientes del Decreto Legislativo 196/2003.

Si es necesario, se nombrará un administrador del sistema en una carta de cita separada para el administrador del sistema.

7. Estados Unidos de América (USA)

Las siguientes definiciones en la cláusula 1 de este DPA deben considerarse de la siguiente manera:

"Datos personales (en los Estados Unidos, se utiliza el término Información de identificación personal): cualquier elemento individual de información relacionada con las circunstancias personales o materiales de un individuo identificado o identificable;

Datos confidenciales (también conocidos como "Datos personales confidenciales"): información sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual, número de seguro social, número de licencia de conducir o número de tarjeta de identificación estatal o emitida federalmente, número de cuenta o número de tarjeta de crédito o débito, o un número de cuenta en combinación con cualquier código de seguridad, código de acceso o contraseña requerido que permita el acceso a la cuenta financiera de un individuo o cualquier otra información cuya divulgación no autorizada pueda requerir que el Controlador notifique a las personas afectadas".

8. Singapur

Si el Controlador se encuentra en Singapur, se agregará el siguiente texto a la cláusula 4 de este DPA:

"El Operador cumplirá de manera oportuna con las instrucciones o decisiones de cualquier autoridad competente de protección de datos y privacidad en relación con los Datos. El Operador proporcionará al Controlador la cooperación, asistencia e información que el Controlador solicite razonablemente para cumplir con sus obligaciones en virtud de la legislación de protección de datos".

9. Malasia

Si el Controlador se encuentra en Malasia, la definición de categorías especiales de datos ("Datos personales sensibles" significa información sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, salud o vida sexual) en la cláusula 1 de este DPA (Definiciones) se reemplazará por lo siguiente: "Datos personales sensibles" significa información sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, asociación con sindicatos, práctica o presunta práctica de cualquier delito, salud física o mental o vida sexual".

Si el Controlador se encuentra en Malasia, el siguiente texto de la cláusula 8 de este DPA se complementará con "El Operador implementará medidas técnicas y organizativas según lo especificado en la Legislación de Protección de Datos y el Anexo 1 para proteger los Datos de accidentes o destrucción ilegal o pérdida accidental, alteración, divulgación, uso o acceso no autorizados y contra todas las demás formas ilegales de tratamiento".

Si el Controlador se encuentra en Malasia, se agregará el siguiente texto a la cláusula 9.1 (b) de este DPA:

"Ambas Partes se comprometen a mantener la confidencialidad sobre toda la información adquirida en virtud del Acuerdo y este DPA, especialmente con respecto a los Datos, teniendo en cuenta el secreto del Controlador. Esta obligación sigue aplicándose después de la terminación del DPA".

Si el Controlador se encuentra en Malasia, se agregará el siguiente texto a la cláusula 11 de este DPA "El informe cubrirá los objetivos de las medidas técnicas y organizativas establecidas en el Anexo 1 y la Legislación de Protección de Datos".

10. India

Las siguientes definiciones de la cláusula 1 del presente DPA deben modificarse como sigue:

"**Datos Personales"** significa cualquier elemento individual de información sobre las circunstancias personales o materiales de un individuo identificado o identificable. Información personal, que es cualquier información relativa a una persona física que, directa o indirectamente, en combinación con otra información disponible o que pueda estar disponible con una entidad jurídica, es capaz de identificar a esa persona.

"**Datos Personales confidenciales"** significa los datos o información personal confidencial de una persona; esto significa dicha información personal que consiste en información relacionada con;—(i) contraseña; (ii) información financiera, como información bancaria o tarjeta de crédito o débito u otros detalles de instrumentos de pago; iii) estado de salud física, fisiológica y mental; iv) orientación sexual; (v) registros médicos e historial; vi) información biométrica; (vii) cualquier detalle relacionado con las cláusulas anteriores, según lo dispuesto por la persona jurídica para la prestación del servicio; y (viii) cualquiera de la información recibida de conformidad con las cláusulas anteriores por una entidad legal para su tratamiento, almacenada o procesada bajo contrato legal o de otra manera: siempre que cualquier información que esté disponible o accesible libremente en el dominio público o proporcionada de acuerdo con la Ley de Derecho a la Información de 2005 o cualquier otra ley vigente no se considerará datos sensibles o información personal a los efectos de estas reglas.

El siguiente texto se añadirá a la cláusula 8 de este DPA:

"El Operador cumplirá con las prácticas y procedimientos de seguridad razonables prescritos por el Controlador y/o la política de privacidad del Controlador constituirá prácticas y procedimientos de seguridad razonables de acuerdo con la sección 43A de la Ley de Tecnología de la Información (india) de 2000 y las reglas emitidas por el gobierno indio en virtud de dicha disposición, por lo tanto, no se aplicará".

11. China

El siguiente texto se añadirá a la cláusula 16 de este DPA:

"La responsabilidad legal bajo las leyes de la República Popular de China puede aplicarse dependiendo de los acuerdos del Controlador con su cliente".

12. Brasil

Las siguientes definiciones de la cláusula 1 del presente DPA deben modificarse como sigue:

"Datos personales Sensibles" significa datos personales sensibles: esto significa dichos datos sobre origen racial o étnico, creencias religiosas, opinión política, afiliación sindical u organización religiosa, filosófica o política, dados a la salud o la vida sexual, datos genéticos o biométricos, cuando están vinculados a una persona física.

"Tratamiento de datos" significa cualquier operación realizada con datos personales, como las referidas a la recopilación, producción, recepción, clasificación, uso, acceso, reproducción, transmisión, distribución, tratamiento, archivo, almacenamiento, eliminación, evaluación o control de información, modificación, comunicación, transferencia, difusión o extracción.

Si los suboperadores están ubicados en Brasil, no se aplicarán las obligaciones establecidas en las cláusulas 7.2, 7.4 y 7.5 de este DPA.

13. Colombia

Además de lo acordado en la cláusula 8 y la cláusula 15 de este DPA, lo siguiente se aplica en relación con el procesamiento y la transferencia de Datos Personales:

El Responsable del Tratamiento reconoce que el Encargado del Tratamiento puede transferir, almacenar y procesar Datos Personales en territorios fuera de Colombia, por lo que los Datos Personales estarán sujetos a las leyes de las jurisdicciones extranjeras en las que se almacenen. El Responsable del Tratamiento reconoce que tiene todos los consentimientos necesarios y la autoridad legal otorgada por los titulares de los Datos Personales, así como registros de bases de datos que permitan al Encargado del Tratamiento procesar Datos Personales dentro de bases de datos y en países que garantizan mínimamente el mismo estándar de protección de datos (nivel adecuado de protección) que el previsto en la legislación colombiana (como, pero no limitado al artículo 26 de la Ley Estatutaria 1581 de 2012, artículos 24 y 25 del Decreto Reglamentario 1377 de 2013, Decreto 90 de 2018, la Circular Única de la Superintendencia de Industria y Comercio y la Circular Externa N° 005 de 2017 de la Superintendencia de Industria y Comercio).

14. Argentina

Además de lo acordado en la cláusula 8 y la cláusula 15 de este DPA. las Partes acuerdan ejecutar las siguientes Cláusulas Contractuales de Tipo Argentino para transferencia internacional, siempre que el Responsable de Datos

Personales sea de Argentina y/o la Legislación de Protección de Datos aplicable y/o la Autoridad Argentina de Protección de Datos requieran que se lleven a cabo estas cláusulas.

Modelo de contrato de transferencia internacional de datos personales con motivo de la prestación de servicios

Introduce, por una parte, _____localidad_____ calle_____ condiciones que se detallan a continuación.