

ADENDA DE TRATAMIENTO DE DATOS POR PARTE DEL PROVEEDOR

La presente Adenda de Tratamiento de Datos («Adenda») forma parte del contrato principal («Contrato Principal») celebrado entre el «CLIENTE», que actúa en su propio nombre y en representación de cada Afiliado de la Entidad; y (ii) EVOLMIND, SL «EVOLMIND» («Proveedor») que actúa en su propio nombre y como agente de cada Afiliado del Proveedor.

Al firmar el Contrato Principal, el Proveedor suscribe este Contrato de Tratamiento de Datos en su propio nombre y, en la medida en que lo exijan las leyes de protección de datos aplicables, en nombre y, en la medida en que lo exijan las leyes de protección de datos aplicables, en nombre y por cuenta de cualquier Subcontratista autorizado.

En el curso de la prestación de los Servicios al CLIENTE en virtud del presente Contrato, el Proveedor podrá tratar los Datos Personales en nombre del CLIENTE y las Partes acuerdan cumplir las siguientes disposiciones con respecto a cualesquiera Datos Personales; cada una de ellas actuará de forma razonable y de buena fe.

Los términos utilizados en la presente Adenda tendrán el significado que se indica en el mismo. Los términos en mayúsculas que no estén definidos en este documento tendrán el significado que se les da en el Contrato Principal. Salvo en la medida en que se modifique a continuación, los términos del Contrato Principal permanecerán en pleno vigor y efecto.

En consideración a las obligaciones mutuas aquí establecidas, las partes acuerdan por el presente que los términos y condiciones establecidos a continuación se añadirán como una Adenda al Contrato Principal. En consecuencia, salvo que el contexto exija lo contrario, cualquier referencia al Contrato Principal se entenderá hecha a dicho Contrato Principal incluyendo las modificaciones realizadas por esta Adenda.

1. OBJETO

1. La presente Adenda regula los términos y condiciones que se aplicarán al tratamiento de los Datos Personales a los que el Proveedor pueda tener acceso en virtud de los Servicios.
2. A efectos de la presente Adenda, los términos tendrán el significado que figura en el Anexo

2. OBJETIVOS DE TRATAMIENTO

1. El proveedor se compromete a tratar los datos personales en nombre de la Entidad de conformidad con las condiciones establecidas en el presente Contrato de Tratamiento de Datos. El tratamiento se realizará exclusivamente en el marco del Contrato y a todos los efectos que se acuerde posteriormente.
2. El Proveedor se abstendrá de hacer uso de los datos personales para cualquier propósito que no sea el especificado por la Entidad. La Entidad informará al Proveedor de cualquier propósito que no esté contemplado en este Contrato de Tratamiento de Datos.
3. Todos los datos personales tratados en nombre de la Entidad serán propiedad de la Entidad y/o de los Interesados pertinentes.
4. El Proveedor no tomará ninguna decisión unilateral sobre el tratamiento de los datos personales para otros fines, incluidas las decisiones relativas al suministro de los mismos a terceros y a la duración del almacenamiento de los datos.

5. En el Anexo 2.5 de la presente Adenda se establece cierta información relativa al Tratamiento de los Datos Personales de la Entidad por los Responsables del Tratamiento, tal como exige el artículo 28, apartado 3, del Reglamento General de Protección de Datos (RGPD) (y, posiblemente, requisitos equivalentes de otras Leyes de Protección de Datos). La Entidad puede hacer modificaciones razonables al Anexo 2.5 mediante notificación por escrito al Proveedor según lo considere razonablemente necesario la Entidad para cumplir con dichos requisitos. Nada de lo dispuesto en el Anexo 2.5 confiere derecho alguno ni impone obligación alguna a ninguna de las partes respecto a la presente Adenda.

3. OBLIGACIONES DEL PROVEEDOR

1. El Proveedor garantizará el cumplimiento de las leyes y los reglamentos aplicables, incluidas las leyes y los reglamentos que rigen la protección de datos personales.
2. El Proveedor suministrará a la Entidad sin demora, a solicitud de esta, detalles sobre las medidas que haya adoptado para cumplir sus obligaciones conforme a esta Adenda.
3. Las obligaciones del Proveedor que surjan en virtud de los términos de esta Adenda se aplican también a quienquiera que procese los Datos Personales de la Entidad con arreglo a las instrucciones del Proveedor

4. PERSONAL DEL PROVEEDOR Y DE LOS AFILIADOS DEL PROVEEDOR

1. El Proveedor y cada uno de los Afiliados del Proveedor tomarán las medidas razonables para asegurar la fiabilidad de cualquier empleado, agente o contratista de cualquier Responsable del Tratamiento que pueda tener acceso a los Datos Personales de la Entidad, asegurándose en cada caso de que el acceso esté estrictamente limitado a aquellas personas que necesiten conocer o acceder a los Datos Personales de la Entidad, cuando sea estrictamente necesario a los efectos del Contrato Principal, y para cumplir con las Leyes Aplicables en el contexto de los deberes de dicha persona respecto del Responsable del Tratamiento, garantizando que todas estas personas estén sujetas a compromisos de confidencialidad o a obligaciones de confidencialidad profesionales o estatutarias.

5. SEGURIDAD

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los objetivos del Tratamiento, así como el riesgo de que los derechos y libertades de las personas físicas varían en cuanto a su probabilidad y gravedad, el Proveedor y cada uno de los Afiliados del Proveedor implementarán las medidas técnicas y organizativas apropiadas para (i) proteger los Datos frente a la destrucción accidental o ilícita, y (ii) evitar la pérdida, alteración, divulgación no autorizada o acceso no autorizado a los Datos (un «Incidente de Seguridad»). Como mínimo, dichas medidas incluirán las medidas de seguridad identificadas en el Anexo 5.1.
2. Al evaluar el nivel de seguridad adecuado, el Proveedor y cada uno de los Afiliados del Proveedor tendrán en cuenta, en particular, los riesgos que presenta el Tratamiento, especialmente los derivados de una Violación de la Seguridad de los Datos Personales.
3. Incidentes de seguridad: al tener conocimiento de un Incidente de Seguridad, el Proveedor informará a la Entidad sin demoras indebidas (y, en cualquier caso, en las 24 horas siguientes) y proporcionará toda la información y cooperación oportuna que la Entidad pueda requerir para que la Entidad cumpla sus obligaciones de notificación de violación de datos en virtud de (y de acuerdo con los plazos requeridos por) la Ley de Protección de

Datos Aplicable. En particular, toda comunicación relativa a un Incidente de Seguridad se enviará utilizando el formulario normalizado de notificación que figura en el Anexo 5.3.

4. El Proveedor adoptará además todas las medidas y acciones necesarias para remediar o mitigar los efectos del Incidente de Seguridad y mantendrá a la Entidad informada de todos los acontecimientos relacionados con el Incidente de Seguridad. El Proveedor no notificará a terceros de un Incidente de Seguridad que afecte a los Datos a menos que y en la medida en que: (a) la Entidad haya aceptado dicha notificación (tal acuerdo no debe ser retenido, condicionado o demorado injustificadamente), y/o (b) el Proveedor deba hacer la notificación de acuerdo con la Ley de Protección de Datos Aplicable.

6. SUBCONTRATACIÓN

1. Se adjunta como Anexo 6.1 un listado de Subcontratistas que el Proveedor utiliza para la prestación. Cada Miembro del Grupo de Entidades autoriza al Proveedor y a cada uno de los Afiliados del Proveedor a designar (y permitir que cada uno de los Subcontratistas designados de acuerdo con esta sección 6 designen) a Subcontratistas de acuerdo con esta sección 6 y cualquier restricción en el Contrato Principal.
2. El Proveedor y cada uno de los Afiliados del Proveedor podrán seguir recurriendo a aquellos Subcontratistas ya contratados por el Proveedor o por cualquier Afiliado del Proveedor en la fecha de esta Adenda, que acaten las órdenes del Proveedor y de cada Afiliado del Proveedor en cada caso y que cumplan tan pronto como sea factible las obligaciones establecidas en la sección 6.4.
3. Se adjunta como Anexo 6.3 un listado de Subcontratistas que el Proveedor utiliza en la actualidad para la prestación de los servicios. El Proveedor notificará previamente por escrito a la Entidad el nombramiento de cualquier nuevo Subcontratista, incluidos los detalles completos del Tratamiento que realizará el Subcontratista. Si, en los 30 días siguientes a la recepción de dicha notificación, la Entidad notifica al Proveedor por escrito cualquier objeción (sobre bases razonables) al nombramiento propuesto, ni el Proveedor ni ningún Afiliado del Proveedor designarán (o revelarán ningún Dato Personal de la Entidad) a dicho Subcontratista propuesto hasta que se hayan tomado las medidas necesarias y razonables para abordar las objeciones planteadas por cualquier Miembro del Grupo de Entidades y la Entidad haya recibido una explicación escrita razonable de las medidas adoptadas.
4. Con respecto a cada Subcontratista, el Proveedor o Afiliado del Proveedor pertinente deberá:
 - i. Antes de que el Subcontratista trate por primera vez los Datos Personales de la Entidad (o, en su caso, de conformidad con la sección 6.2), actuar con la diligencia debida y apropiada para garantizar que el Subcontratista sea capaz de proporcionar el nivel de protección de los Datos Personales de la Entidad requerido por el Contrato Principal.
 - ii. Asegurar que el acuerdo entre, por una parte, (a) el Proveedor, (b) el Afiliado del Proveedor pertinente o (c) el Subcontratista intermediario pertinente y, por otra parte, el Subcontratista, se rija por un contrato escrito que incluya términos que ofrezcan al menos el mismo nivel de protección para los Datos Personales de la Entidad que los establecidos en esta Adenda y que cumpla los requisitos del artículo 28, apartado 3, del Reglamento General de Protección de Datos.

- iii. Si ese acuerdo implica una Transferencia Restringida, asegúrese de que las Cláusulas Contractuales Estándares estén incorporadas en todo momento al contrato entre, por un lado, (a) el Proveedor, (b) el Afiliado del Proveedor pertinente, o (c) el Subcontratista intermedio pertinente, y, por otro lado, el Subcontratista, o antes de que el Subcontratista trate los Datos Personales de la Entidad, asegúrese de que suscriba un contrato que incorpore las Cláusulas Contractuales Estándar con el/los Miembro(s) del Grupo de Entidades pertinente(s) (y la Entidad procurará que cada una de las Partes Asociadas a la Entidad que estén sujetas a cualquiera de dichas Cláusulas Contractuales Estándar cooperen con la aportación de datos y la ejecución de las mismas).
- iv. Proporcionar a la Entidad para su revisión las copias de los contratos de los Responsables del Tratamiento con los Subcontratistas (que podrán modificarse para eliminar la información comercial confidencial que no sea pertinente para los requisitos de esta Adenda) que la Entidad pueda solicitar cuando lo considere oportuno.
- v. El Proveedor y cada uno de los Afiliados del Proveedor se asegurarán de que cada uno de los Subcontratistas cumplan las obligaciones de esta Adenda, tal como se aplican al Tratamiento de Datos Personales de la Entidad llevado a cabo por ese Subcontratista, como si fueran parte de esta Adenda en lugar del Proveedor.

7. DERECHOS DEL INTERESADO

1. Teniendo en cuenta la naturaleza del Tratamiento, el Proveedor y cada uno de los Afiliados del Proveedor asistirán a cada uno de los Miembros del Grupo de Entidades implementando las medidas técnicas y organizativas apropiadas, en la medida de lo posible, para el cumplimiento de las obligaciones de los Miembros del Grupo de Entidades, según lo entienda razonablemente la Entidad, con tal de responder a las solicitudes para ejercer los derechos del Interesado conforme a la Ley de Protección de Datos.
2. El Proveedor deberá:
 - i. Notificar inmediatamente a la Entidad si algún Responsable del Tratamiento recibe una solicitud del Interesado en virtud de cualquier Ley de Protección de Datos con respecto a los Datos Personales de la Entidad.
 - ii. Asegurarse de que el Responsable del Tratamiento no responde a esa solicitud excepto con arreglo a las instrucciones documentadas de la Entidad o del Afiliado de la Entidad pertinente, o según lo exijan las Leyes Aplicables a las que esté sujeto el Responsable del Tratamiento, en cuyo caso el Proveedor informará a la Entidad, en la medida permitida por las Leyes Aplicables, de ese requisito legal antes de que el Responsable del Tratamiento responda a la solicitud.

8. VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

1. El Proveedor notificará a la Entidad sin demora injustificada cuando el Proveedor o cualquier Subcontratista tenga conocimiento de una Violación de la Seguridad de los Datos Personales que afecte a los Datos Personales de la Entidad, proporcionando a la Entidad suficiente información para que cada Miembro del Grupo de Entidades pueda cumplir

cualquier obligación de notificar o informar a los Interesados de la Violación de la Seguridad de los Datos Personales en virtud de las Leyes de Protección de Datos.

2. El Proveedor cooperará con la Entidad y con cada uno de los Miembros del Grupo de Entidades y tomará las medidas comerciales razonables dispuestas por la Entidad para ayudar en la investigación, mitigación y solución de cada una de dichas Violaciones de Datos Personales.

9. EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS Y CONSULTA PREVIA

1. El Proveedor y cada uno de los Afiliados del Proveedor proporcionarán asistencia razonable a cada Miembro del Grupo de Entidades con cualquier evaluación del impacto de la protección de datos, y consultas previas con las Autoridades Supervisoras u otras autoridades competentes de privacidad de datos, que la Entidad considere razonablemente exigible a cualquier Miembro del Grupo con arreglo al artículo 35 o 36 del Reglamento General de Protección de Datos o a disposiciones equivalentes de cualquier otra Ley de Protección de Datos, en cada caso únicamente en relación con el Tratamiento de Datos Personales de la Entidad y teniendo en cuenta la naturaleza del Tratamiento y la información a disposición de los Responsables del Tratamiento.

10. ELIMINACIÓN O DEVOLUCIÓN DE DATOS PERSONALES DE LA ENTIDAD

1. Al finalizar o expirar el Contrato, el Proveedor deberá (a elección de la Entidad) destruir o devolver a la Entidad todos los Datos Personales de la Entidad (incluidas todas las copias de los Datos) en su posesión o control (incluido cualquier dato subcontratado a un tercero para su tratamiento). Este requisito no se aplicará en la medida en que el Proveedor esté obligado por cualquier ley aplicable a retener parte o la totalidad de los Datos, en cuyo caso el Proveedor deberá aislar y proteger los Datos de cualquier tratamiento posterior, excepto en la medida requerida por dicha ley.
2. A petición de la Entidad, el Proveedor proporcionará una certificación escrita de que ha cumplido los requisitos de esta Sección, firmada por un agente del Proveedor.

11. DERECHOS DE AUDITORÍA

1. Ya sea a raíz de un incidente de seguridad sufrido por el Proveedor, o a las órdenes de una autoridad de protección de datos, el Proveedor permitirá a la Entidad (o a sus auditores externos designados) auditar el cumplimiento del Proveedor respecto de esta Adenda, y pondrá a disposición de la Entidad toda la información, sistemas y personal necesarios para que esta (o sus auditores externos) lleven a cabo dicha auditoría. El Proveedor acepta que la Entidad (o sus auditores externos) pueden entrar en sus instalaciones para llevar a cabo esta auditoría, siempre que la Entidad le notifique razonablemente su intención de auditar, lleve a cabo su auditoría durante el horario normal laboral y tome todas las medidas razonables para evitar interrupciones innecesarias en las operaciones del Proveedor. Dicha auditoría estará sujeta a los términos de confidencialidad acordados entre las partes.

12. TRANSFERENCIAS RESTRINGIDAS

1. Cada Miembro del Grupo de Entidades (como «exportador de datos») y cada Responsable del Tratamiento, según corresponda, (como «importador de datos») suscribe por la presente las Cláusulas Contractuales Estándares con respecto a cualquier Transferencia Restringida de ese Miembro del Grupo de Entidades a ese Responsable del Tratamiento.
2. Las Cláusulas Contractuales Estándares entrarán en vigor a más tardar:
 - i. En el momento en que el exportador de datos se convierta en parte de ellas.
 - ii. En el momento en que el importador de datos se convierta en parte de ellas.
 - iii. Cuando dé comienzo la Transferencia Restringida pertinente.
3. La Sección 12.1 no se aplicará a una Transferencia Restringida a menos que su efecto, junto con otras medidas de cumplimiento razonablemente practicables (que, para evitar dudas, no incluyan la obtención de consentimientos de los Interesados), sea permitir que la Transferencia Restringida pertinente tenga lugar sin infringir la Ley de Protección de Datos aplicable.
4. El Proveedor garantiza y manifiesta que, antes del comienzo de cualquier Transferencia Restringida a un Subcontratista que no sea un Afiliado del Proveedor, la adhesión por parte del Proveedor o del Afiliado del Proveedor pertinente a las Cláusulas Contractuales Estándares, y la conformidad con las variaciones a esas Cláusulas Contractuales Estándares, en representación y en nombre de ese Subcontratista, habrán sido debidamente y efectivamente autorizadas (o posteriormente ratificadas) por dicho Subcontratista.

13. CONDICIONES GENERALES

1. Ley aplicable y jurisdicción
 - i. La Adenda y su aplicación se regirán por la legislación española.
 - ii. Cualquier controversia que pueda surgir en relación con la presente Adenda y/o se derive del mismo se regirá por los tribunales de la ciudad de Zaragoza (España).
2. Orden de prelación
 - i. Nada en esta Adenda reduce las obligaciones del Proveedor ni de cualquier Afiliado del Proveedor en virtud del Contrato Principal en relación con la protección de Datos Personales o permite al Proveedor o a cualquier Afiliado del Proveedor tratar (o permitir el tratamiento de) Datos Personales de una manera que se prohíba en el Contrato Principal. En caso de conflicto o incoherencia entre la presente Adenda y las Cláusulas Contractuales Estándares, prevalecerán las Cláusulas Contractuales Estándares.
 - ii. Con sujeción a lo dispuesto en la sección 13.2, en lo que respecta al objeto de la presente Adenda, en caso de discrepancias entre las disposiciones de la presente Adenda y cualesquiera otros contratos suscritos entre las partes, incluido el Contrato Principal y asimismo incluidos (salvo si se acuerda explícitamente otra cosa por escrito, y que se firme en nombre de las partes) los contratos suscritos o supuestamente suscritos con posterioridad a la fecha de la presente Adenda, prevalecerán las disposiciones del mismo.
3. Cláusula de salvedad
 - i. En el caso de que alguna disposición de la presente Adenda sea inválida o inaplicable, el resto de la presente Adenda seguirá siendo válido y vigente. La disposición inválida o inaplicable será: (i) modificada según sea necesario para

EVOLMIND S.L.

asegurar su validez y aplicabilidad, preservando las intenciones de las partes lo más estrictamente posible o, si esto no es posible, (ii) interpretada como si la parte inválida o inaplicable nunca hubiera estado contenida en él.

EN TESTIMONIO DE LO CUAL, la presente Adenda pasa a formar parte del Contrato Principal con efectos a partir de la fecha de la presente.

EVOLMIND SL "EVOLMIND"

Nombre: Javier Pérez Torres

Cargo CEO

ANEXO 1.2: DEFINICIONES

En esta Adenda, los siguientes términos tendrán el significado que se indica a continuación y los términos afines se interpretarán en consecuencia:

1. por «Leyes Aplicables» se entienden: a) las leyes de la Unión Europea o de los Estados miembros con respecto a cualquier Dato Personal de la Entidad en relación con el cual cualquier Miembro del Grupo de Entidades está sujeto a las Leyes de Protección de Datos de la UE; y b) cualquier otra ley aplicable con respecto a cualquier Dato Personal de la Entidad en relación con el cual cualquier Miembro del Grupo de Entidades está sujeto a cualquier otra Ley de Protección.
2. por «Afiliado de la Entidad» se entiende una entidad que posee o controla, es poseída o controlada por, o está o queda bajo el control o la propiedad común de la Empresa, donde el control se define como la posesión, directa o indirectamente, de la facultad de dirigir o disponer la dirección de la administración y las políticas de una entidad, ya sea a través de la propiedad de los valores con derecho a voto, por contrato o de otra manera;
3. por «Miembro del Grupo de Entidades» se entiende la Entidad o cualquier Afiliado de la Entidad;
4. por «Datos Personales de la Entidad» se entiende cualquier Dato Personal Tratado por un Responsable del Tratamiento en nombre de un Miembro del Grupo de Entidades de conformidad con o en conexión con el Contrato Principal;
5. por «Responsable del Tratamiento» se entiende un Proveedor o un Subcontratista;
6. por «Leyes de Protección de Datos» se entienden las Leyes de Protección de Datos de la UE y, en la medida en que sea aplicable, las leyes de protección de datos o de privacidad de cualquier otro país;
7. por «EEE» se entiende el Espacio Económico Europeo;
8. por «Leyes de Protección de Datos de la UE» se entiende la Directiva 95/46/CE de la UE, incorporada a la legislación nacional de cada Estado miembro y modificada, sustituida o reemplazada según corresponda, incluido el RGPD y las leyes que aplican o complementan el RGPD;
9. por «RGPD» se entiende el Reglamento General de Protección de Datos de la UE 2016/679;
10. por «Transferencia Restringida» se entiende:
 - a. una transferencia de Datos Personales de la Entidad de cualquier Miembro del Grupo de Entidades a un Responsable del Tratamiento; o
 - b. una transferencia ulterior de Datos Personales de la Entidad de un Responsable del Tratamiento a un Responsable del Tratamiento, o entre dos establecimientos de un Responsable del Tratamiento.

En cada caso, cuando dicha transferencia esté prohibida por las Leyes de Protección de Datos (o por los términos de los contratos de transferencia de datos establecidos para abordar las restricciones a la transferencia de datos de las Leyes de Protección de Datos) en ausencia de (i) las Cláusulas Contractuales Estándares, o (ii) una autocertificación de la Protección de Privacidad (que se mantendrá mientras el Proveedor trate los Datos Personales de la Entidad), asumiendo que el alcance de dicha autocertificación cubre todos los Datos Personales de la Entidad que el Proveedor trate en virtud del Contrato y esta Adenda, y el Proveedor acepta cumplir los Principios de Protección de la Privacidad cuando trate dichos Datos Personales de la Entidad;

11. por «Servicios» se entienden los servicios y otras actividades que suministre o lleve a cabo el Proveedor o que se suministren o lleven a cabo en su nombre para los Miembros del Grupo de Entidades de conformidad con el Contrato Principal;
12. por «Cláusulas Contractuales Estándares» se entienden las cláusulas contractuales que figuran en el Anexo 5.1, modificadas según se indica (entre corchetes y en cursiva) en dicho Anexo;
13. por «Subcontratista» se entiende cualquier persona (incluidos cualquier tercero y cualquier Afiliado del Proveedor, pero excluyendo a los empleados del Proveedor o a cualquiera de sus subcontratistas) designada por el Proveedor o por cualquier Afiliado del Proveedor, o bien en su nombre, para tratar Datos Personales en nombre de cualquier Miembro del Grupo de Entidades en relación con el Contrato Principal;
14. por «Afiliado del Proveedor» se entiende una entidad que posee o controla, es poseída o controlada por, o está o queda bajo el control o la propiedad común del Proveedor, donde el control se define como la posesión, directa o indirectamente, de la facultad de dirigir o disponer la dirección de la administración y las políticas de una entidad, ya sea a través de la propiedad de los valores con derecho a voto, por contrato o de otra manera.

Los términos «Comisión», «Responsable» o «Responsable del tratamiento», «Interesados», «Estado miembro», «Datos Personales», «Violación de la Seguridad de los Datos Personales», «Tratamiento» y «Autoridad de Control» tendrán el mismo significado que en el RGPD, y sus términos afines se interpretarán en consecuencia.

La palabra «incluye» se interpretará como incluir sin limitación, y los términos afines se interpretarán en consecuencia.

ANEXO 2.5: DETALLES SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES DE LA ENTIDAD

Este Anexo 2.5 incluye ciertos detalles sobre el Tratamiento de los Datos Personales de la Entidad según lo requerido por el artículo 28, apartado 3, del RGPD.

Objeto y duración del Tratamiento de los Datos Personales de la Entidad

El objeto y la duración del Tratamiento de los Datos Personales de la Entidad se establecen en el Contrato Principal y en esta Adenda.

La naturaleza y finalidad del Tratamiento de los Datos Personales de la Entidad

Prestar el servicio de la plataforma de EVOLMIND para la cual ha sido diseñada. Los datos recogidos de las personas físicas se utilizarán como forma de acceso a sus cuentas de EVOLMIND, así como formas de contacto entre la empresa y las cuentas de empresa, entre otras finalidades siempre relacionadas con la prestación de servicios para la cuál ha sido diseñada la aplicación.

Los tipos de Datos Personales de la Entidad por Tratar

Nombre y apellidos

Correo electrónico

Las categorías de Interesados a las que se refieren los Datos Personales de la Entidad

La categoría de datos recogidos por EVOLMIND es de datos identificativos y de contacto.

Las obligaciones y los derechos de la Entidad y de los Afiliados de la Entidad

Las obligaciones y los derechos de la Entidad y de los Afiliados de la Entidad se establecen en el Contrato Principal y en esta Adenda

ANEXO 5.1

DESCRIPCIÓN DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS MÍNIMAS QUE DEBERÁ APLICAR EL PROVEEDOR

1. Programa de Seguridad de la Información (PSI)

El Proveedor mantendrá un PSI diseñado para (a) ayudar a EVOLMIND a proteger los Datos Personales frente a pérdidas, acceso o divulgación accidentales o ilegales, (b) identificar los riesgos internos y razonablemente previsibles para la seguridad y el acceso no autorizado a la Red de Proveedores (se define a continuación) y (c) minimizar los riesgos de seguridad, inclusive a través de la evaluación de riesgos y pruebas regulares. El Proveedor designará a un empleado para que sea responsable del PSI.

El PSI incluirá las siguientes medidas:

1. Seguridad de Red

La Red de Proveedores será accesible a los empleados, contratistas y cualquier otra persona que sea necesaria para prestar los servicios de tratamiento de datos. El Proveedor mantendrá controles de acceso y políticas para administrar el acceso a la Red de Proveedores desde cada conexión de red y usuario, incluido el uso de controles de autenticación, cortafuegos o sistemas de Detección de Intrusiones. El Proveedor mantendrá planes de respuesta ante incidentes de seguridad para gestionar posibles incidentes de seguridad.

2. Seguridad Física

Los componentes físicos de la Red de Proveedores están alojados en instalaciones («Instalaciones») controladas por una Entidad certificada ISO 27001 (es decir, Servicios Web de Amazon o Google Cloud) o en instalaciones que cumplen o superan todos los siguientes requisitos de seguridad física:

- i. **Controles de Acceso Físico.** Se utilizan controles de barreras físicas para impedir la entrada no autorizada a las instalaciones tanto en el perímetro como en los puntos de acceso al edificio. El paso a través de las barreras físicas en las instalaciones requiere la validación electrónica del control de acceso (p. ej., sistemas de acceso con tarjeta, etc.) o la validación por parte del personal de seguridad humana (p. ej., servicio de guardia de seguridad interna o por contrato, recepcionista, etc.). A los empleados y contratistas se les asignan tarjetas de identificación con foto que deben llevar a la vista mientras los empleados y contratistas estén en cualquiera de las Instalaciones. Se requiere que los visitantes fichen a su entrada en presencia del personal designado, deben mostrar la identificación apropiada, se les asignará una tarjeta de identificación de visitante que deberán llevar a la vista mientras estén en cualquiera de las Instalaciones, y serán escoltados en todo momento por empleados o contratistas autorizados mientras visiten las Instalaciones.
- ii. **Acceso Limitado para Empleados y Contratistas.** El Proveedor proporciona acceso a las Instalaciones a aquellos empleados y contratistas que tengan una necesidad comercial legítima de tales privilegios de acceso. Cuando un empleado o contratista ya no necesite los privilegios de acceso que se le hayan asignado, los privilegios de

acceso se revocarán sin demora, incluso si el empleado o contratista sigue siendo un empleado del Proveedor o de sus afiliados.

- iii. Protecciones de Seguridad Física. Todos los puntos de acceso (excepto las puertas de entrada principales) se mantienen cerrados con llave. Los puntos de acceso a las Instalaciones se supervisan mediante videocámaras de vigilancia diseñadas para grabar a todas las personas que acceden a las Instalaciones. El Proveedor también mantiene sistemas electrónicos de detección de intrusión diseñados para detectar el acceso no autorizado a las Instalaciones, incluidos puntos de supervisión de vulnerabilidad (p. ej., puertas de entrada primaria, puertas de salida de emergencia, escotillas de techo, puertas de muelle de carga, etc.) con contactos de puerta, dispositivos de rotura de vidrio, detección de movimiento interior u otros dispositivos diseñados para detectar a las personas que intentan obtener acceso a las Instalaciones. Todo el acceso físico a las Instalaciones por parte de los empleados y contratistas es registrado y auditado de manera rutinaria.

3. Seguridad de los Datos Personales. Controles para la Protección de Datos Personales.

El Proveedor mantendrá las medidas técnicas y organizativas apropiadas para la protección de la seguridad (incluida la protección frente al tratamiento no autorizado o ilícito y frente a la destrucción accidental o ilícita, pérdida o alteración o daño, divulgación no autorizada o acceso no autorizado a los Datos Personales), confidencialidad e integridad de los Datos Personales de acuerdo con el riesgo. Entre ellas se incluirán, según corresponda: (i) la pseudonimización y el cifrado de los datos personales; (ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (iii) la capacidad de restablecer la disponibilidad de los datos personales y el acceso a los mismos de manera oportuna en caso de incidente físico o técnico; (iv) un proceso para comprobar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento. El Proveedor supervisa regularmente el cumplimiento de estas medidas. El Proveedor no reducirá significativamente la seguridad general de los servicios de tratamiento de datos durante el periodo de suscripción.

4. Continuidad del Negocio y Recuperación ante Desastres

El Proveedor mantendrá un plan de Continuidad del Negocio y Recuperación ante Desastres basado en el riesgo. Los planes de recuperación se prueban al menos una vez al año para garantizar que la recuperación completa sea posible para cumplir los Acuerdos de Nivel de Servicio (ANS) esperados.

5. Seguridad del empleado

El Proveedor firmará acuerdos de confidencialidad con los empleados y contratistas. Para los cargos con acceso a información personal, también se realizarán comprobaciones de antecedentes. Además, todos los empleados y contratistas tendrán una forma común de notificar incidentes aprobados por la organización y cursarán por lo menos una capacitación anual de concienciación sobre la seguridad.

2. Evaluación en curso

1. El Proveedor debe reevaluar y actualizar sus políticas de seguridad periódicamente. Los cambios se deben documentar y emplear controles de cambio.

ANEXO 5.3

FORMULARIO PARA NOTIFICAR UNA SOSPECHA DE INCIDENTE DE SEGURIDAD DE DATOS

| | | |
|-----------------------|--------------|-----------------------------|
| Nombre del Proveedor: | | Su nombre: |
| Fecha de hoy: | Nº Teléfono: | Correo electrónico (email): |

| | |
|-----------------------|--------------------------|
| Fecha del incidente: | Hora del incidente: |
| Quién fue notificado: | Hora de la notificación: |

Breve descripción del incidente:

¿Usted mismo presencié el incidente?

SÍ NO

¿Hubo otros testigos de incidente? (si la respuesta es afirmativa, indique a continuación):

Que usted sepa, ¿estuvo involucrado alguno de los siguientes elementos?

- | | |
|---|--|
| <input type="checkbox"/> Teléfono | <input type="checkbox"/> Robo |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Fraude |
| <input type="checkbox"/> Fotocopiadora | <input type="checkbox"/> Acceso no autorizado |
| <input type="checkbox"/> Hardware informático | <input type="checkbox"/> Clientes |
| <input type="checkbox"/> Correo electrónico | <input type="checkbox"/> Terceros |
| <input type="checkbox"/> Descarga de internet | <input type="checkbox"/> Copyright |
| <input type="checkbox"/> Virus | <input type="checkbox"/> Otros (especificar) : |

¿Se ha comprometido alguna información interna o confidencial de EVOLMIND?

SÍ NO

¿Denuncié este incidente a.... ?

Supervisor Autoridad policial Director de IT Auditor interno Otros:

| |
|--|
| |
|--|

| | | | |
|---------------|--------|---------------|--------|
| Iniciado por: | Fecha: | Revisado por: | Fecha: |
| Aprobado por: | Fecha: | Aprobado por: | Fecha: |

ANEXO 6.3

LISTADO DE SUBCONTRATISTAS QUE EL PROVEEDOR UTILIZA EN LA ACTUALIDAD PARA LA
PRESTACIÓN DE LOS SERVICIOS

OVH Hispano S.L.
Amazon Web Services
Vimeo