ENTRUST COMO ENCARGADO - GLOBAL

ADENDA DE TRATAMIENTO DE DATOS

Esta Adenda de Tratamiento de Datos ("**DPA**" por sus siglas en inglés) complementa y forma parte de los acuerdos escritos o electrónicos (individual y colectivamente el" Acuerdo ") entre Entrust (como se define a continuación) y el Cliente (como se define a continuación) para la compra, acceso y / o licencia de productos, servicios y / o plataformas (colectivamente los "Servicios") para reflejar el acuerdo de las partes con respecto al Tratamiento de Datos Personales. Los términos utilizados en esta DPA tendrán los significados establecidos en esta DPA. Los términos en mayúscula que no se definan de otra manera en este documento tendrán el significado que se les da en el Acuerdo. Salvo lo modificado en la DPA, los términos del Acuerdo permanecerán en pleno vigor y efecto.

1. INSTRUCCIONES

1.1. Esta DPA ha sido firmada previamente en nombre de Entrust Corporation, actuando por sí misma y por y en nombre de sus Afiliados. Para entrar en esta DPA, el Cliente debe:

1.1.1. Tener un acuerdo escrito o electrónico con Entrust;

1.1.2. Completar el punto de contacto del cliente solicitado en la Sección 9.1.

1.1.3. Completar el bloque de firmas a continuación proporcionando el nombre del firmante, su firma, su cargo, la dirección del Cliente y la fecha en que se firmó la DPA; y

1.1.4. Enviar la DPA completado y firmado a Entrust a privacy@entrust.com.

2. EFECTIVIDAD

2.1. Esta DPA solo será efectiva (a partir de la Fecha de Entrada en Vigor) si se firma y se envía a Entrust con precisión y en total conformidad con el párrafo 1 anterior y este párrafo 2. Si el Cliente hace cualquier eliminación u otra revisión de esta DPA que no se haya acordado explícitamente con Entrust, esta DPA se considerará nula y sin efecto.

2.2. Esta DPA será efectiva durante la vigencia del Acuerdo (o más allá en la medida requerida por la ley aplicable).

2.3. Las partes acuerdan que esta DPA reemplazará cualquier DPA existente u otras disposiciones contractuales relacionadas con el tema contenido en este documento que las partes hayan celebrado previamente en relación con los Servicios, y entrará en vigor a partir de la fecha en que Entrust reciba un DPA completo y firmado del Cliente indicado en el bloque de firma a continuación.

3. DEFINICIONES

"**Responsable del Tratamiento**" es sinónimo de "responsable de información de identificación personal", tal como se definen dichos términos en las Leyes de Protección de Datos y en la norma ISO 27701, y se refiere a la entidad que determina el propósito y los medios de Tratamiento de Datos Personales.

"**Cliente**" significa un cliente existente o potencial de Entrust.

"**Leyes de Protección de Datos**" se refiere a todas las leyes y regulaciones de protección de datos y privacidad de datos aplicables, que incluyen, entre otros, el Reglamento General de Protección de Datos (RGPD) de la UE, el Reglamento General de Protección de Datos del Reino Unido (RGPD del Reino Unido), la Ley de Protección de Información Personal y Documentos Electrónicos de Canadá (PIPEDA por sus siglas en inglés) y la Ley de Privacidad del Consumidor de California (CCPA por sus siglas en inglés).

"**Interesado**" es sinónimo de "mandante de información de identificación personal", tal como dichos términos se definen en las Leyes de Protección de Datos y en la norma ISO 27701 y se refiere a la persona o personas identificadas o identificables con las que se relacionan los Datos Personales.

"**Entrust**" significa la entidad Entrust Corporation que es parte del Acuerdo.

"**Datos Personales**" tendrá el significado que se le atribuye a "información de identificación personal", "información personal", "datos personales" o términos equivalentes según se definen dichos términos en las Leyes de Protección de Datos y en ISO 27701.

"Incidente de Datos Personales" tendrá el significado que se le atribuye en las Leyes de Protección de Datos a los términos "encidente de seguridad", "violación de seguridad" o "violación de datos personales" e incluirá cualquier situación en la que Entrust tenga conocimiento de que personas no autorizadas han accedido, divulgado, alterado, perdido, destruido o utilizado, o es probable que se haya accedido a los Datos personales , de manera no autorizada.

"**Tratamiento**" significa cualquier operación o conjunto de operaciones que se realice sobre Datos Personales, sea o no por medios automáticos, tales como recolección, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o de otro modo puesta a disposición, alineación o combinación, restricción, borrado o destrucción.

"**Encargado**" es sinónimo de " procesador de información de identificación personal "como se define en la norma ISO 27701 y se refiere a la entidad que procesa los datos personales en nombre del responsable.

"Cláusulas Contractuales Tipo de la UE" significa las cláusulas contractuales establecidas en el Anexo 2, modificado como se indica (entre corchetes y cursiva) en el Anexo 2 y modificado de otra manera, sustituido o reemplazado cada cierto tiempo de acuerdo con esta DPA.

"**Subencargado**" significa cualquier entidad designada por el Encargado para Procesar Datos Personales en nombre del Responsable.

4. TRATAMIENTO DE DATOS PERSONALES

4.1. **Funciones de las partes.** Las partes reconocen y acuerdan que con respecto al Tratamiento de Datos Personales en virtud del Acuerdo, el Cliente es el Responsable y Entrust es el Encargado.

4.2. **Instrucciones del Cliente para el Tratamiento de Datos Personales.** Las instrucciones del Cliente para el Tratamiento de Datos Personales deberán cumplir con las lLeyes de Protección de Datos. El Cliente será el único responsable de la precisión, calidad y legalidad de los Datos Personales y los medios por los cuales el Cliente adquirió los Datos personales..

4.3. **Tratamiento de Datos Personales de Entrust**. Entrust solo procesará los Datos Personales en nombre y de acuerdo con las instrucciones del Cliente y para los siguientes propósitos: (i) Tratamiento con el propósito específico de realizar los servicios especificados en el Acuerdo o según lo requiera la ley; y (ii) Tratamiento para cumplir con otras instrucciones razonables documentadas proporcionadas por el Cliente cuando dichas instrucciones sean consistentes con los términos del Acuerdo. Entrust informará inmediatamente al Cliente si, en opinión de Entrust, una instrucción infringe las Leyes de Protección de Datos. Para evitar dudas, Entrust no obtendrá, retendrá, usará, venderá ni divulgará Datos Personales para ningún propósito que no sea el propósito específico de prestar los Servicios o según lo requiera la ley.

4.4. **Detalles del Tratamiento.** El propósito del Tratamiento de Datos Personales por parte de Entrust es la prestación de los Servicios de conformidad con el Acuerdo. La duración del Tratamiento, la naturaleza y el propósito del Tratamiento, los tipos de Datos Personales procesados y las categorías de Interesados para quienes se procesan los Datos Personales se establecen en el Anexo 1.

4.5. **Personal**. Entrust se asegurará de que solo el personal autorizado que haya recibido la formación adecuada en la protección y el tratamiento de los Datos Personales, y que esté obligado por escrito a respetar la confidencialidad de los Datos Personales, tenga acceso a los Datos Personales.

4.6. **Controles de Seguridad**. Entrust implementará las medidas técnicas y organizativas apropiadas para mantener la seguridad, la confidencialidad y la integridad de los Datos Personales, incluidas las medidas diseñadas para proteger contra el Tratamiento no autorizado o ilegal y contra la destrucción, pérdida o alteración o daño accidental o ilegal, la divulgación no autorizada o el acceso a Datos Personales.

4.7. **Solicitudes del Interesado.** Entrust, teniendo en cuenta la naturaleza del Tratamiento, ayudará al Cliente, como Responsable, mediante las medidas técnicas y organizativas adecuadas, en la medida de lo posible, a cumplir con la obligación del Cliente de responder a las solicitudes de un Interesado que ejerza su/sus derechos en virtud de las Leyes de Protección de Datos.

4.8. **Evaluación de Impacto de la Protección de Datos.** Entrust, previa solicitud por escrito del Cliente y teniendo en cuenta la naturaleza del Tratamiento y la información disponible, brindará asistencia razonable al Cliente en relación con las obligaciones en virtud de los

Artículos 32 y 36 del RGPD o disposiciones equivalentes en virtud de las Leyes de Protección de Datos.

4.9. **Devolución o Eliminación de Datos Personales.** Entrust, previa solicitud por escrito del Cliente, destruirá, anonimizará o devolverá rápidamente cualquier Dato Personal después de la finalización de la prestación de los Servicios, a menos que la ley aplicable exija el almacenamiento de los Datos Personales..

4.10. **Punto de Contacto del Encargado del Tratamiento.** Si el Cliente tiene alguna pregunta sobre el Tratamiento de Datos Personales por Entrust, el Cliente puede enviar su pregunta al siguiente correo electrónico: privacy@entrust.com.

5. HIPAA

5.1. Si el Cliente es una "entidad cubierta" según la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA por sus siglas en inglés) y Entrust procesará "información médica protegida" en calidad de "socio comercial", según se definen estos términos en 45 CFR § 160.103, la firma de esta DPA incluye la firma del Acuerdo de Socio Comercial ("BAA" por sus siglas en inglés) de HIPAA, cuyo texto completo está disponible en https://www.entrust.com/legal-compliance/data-privacy. El BAA solo se puede usar con "Servicios cubiertos por HIPAA" como se definen en https://www.entrust.com/legal-compliance/data-privacy. El cliente puede optar por no ser parte del BAA enviando la siguiente información a privacy@entrust.com:

- el nombre legal completo del Cliente que opta por no formar parte; y
- si el Cliente tiene varios Acuerdos, el Acuerdo al que se aplica la exclusión voluntaria.

6. SUBENCARGADOS

6.1. **Nombramiento de Subencargados**. El Cliente reconoce y acepta que Entrust puede contratar Subencargados en relación con la prestación de los Servicios. Entrust celebrará un acuerdo por escrito con cualquier Subencargado contratado que contenga obligaciones de protección de datos no menos protectoras que las contenidas en esta DPA..

6.2. **Lista de Subencargados Actuales**. La lista actual de Subprocesadores para los Servicios se puede encontrar en www.entrust.com/sub-processors.

6.3. **Notificación de Nuevos Subencargados.** Entrust notificará al Cliente por escrito sobre cualquier cambio en esta lista de subencargados.

6.4. **Objección a Nuevos Subencargados**. El Cliente puede oponerse al uso de Entrust de un nuevo Subencargado notificando a Entrust por escrito dentro de los diez (10) días hábiles posteriores a la recepción de la comunicación de Entrust informando sobre el nuevo Subencargado. En el caso de que el Cliente objete razonablemente el uso de un nuevo Subencargado, Entrust hará todos los esfuerzos razonables para abordar las objeciones del Cliente. Si Entrust no puede realizar dicho cambio dentro de un período razonable, que no excederá los noventa (90) días, el Cliente puede rescindir el Acuerdo aplicable con respecto

solo a aquellos Servicios que Entrust no puede proporcionar sin el uso de nuevo Subencargado respecto al cual haya presentado una objeción, mediante notificación por escrito a Entrust. Entrust reembolsará al Cliente cualquier tarifa que haya pagado previamente que cubra el resto del plazo de dicho Acuerdo después de la fecha efectiva de la terminación con respecto a dichos Servicios terminados, sin imponer ningún recargo por dicha terminación al Cliente.

6.5. **Responsabilidad.** Entrust será responsable de los actos y omisiones de sus Subencargados en la misma medida que Entrust sería responsable si realizara los servicios de cada Subencargado directamente bajo los términos de esta DPA, excepto que se establezca lo contrario en el Acuerdo..

7. INCIDENTES DE DATOS PERSONALES

7.1. Entrust notificará al Cliente sin demora indebida después de tener conocimiento de un Incidente de Datos Personales. Entrust identificará la causa de dicho Incidente de Datos Personales y tomará las medidas que sean razonablemente necesarias para remediar la causa de dicho Incidente de Datos Personales..

8. TRANSFERENCIAS INTERNACIONALES DE DATOS

8.1. **Transferencias de Datos Personales**. El Cliente acepta permitir la transferencia de Datos Personales fuera del país desde el que se obtuvieron originalmente, siempre que dicha transferencia sea necesaria en relación con la prestación de Servicios en virtud del Acuerdo y que dicha transferencia se realice de conformidad con las Leyes de Protección de Datos, incluyendo, entre otros, completar las evaluaciones previas requeridas por las Leyes de Protección de Datos.

8.2. **Disposiciones Específicas Europeas.** Cuando Entrust transfiera Datos Personales recopilados en el Espacio Económico Europeo a un país fuera del Espacio Económico Europeo y sin una determinación de idoneidad en virtud del artículo 45 del RGPD, Entrust transferirá los Datos Personales de conformidad con las Cláusulas Contractuales Tipo de la UE según lo establecido en el Anexo 2. Las Cláusulas Contractuales Tipo de la UE se incorporan por la presente en su totalidad a esta DPA y, en la medida que sea aplicable, Entrust se asegurará de que sus Subencargados cumplan con las obligaciones de un importador de datos (como se define en las Cláusulas Contractuales Tipo de la UE). En caso de que exista algún conflicto entre esta DPA y las Cláusulas Contractuales Tipo de la UE, prevalecerán los términos de las Cláusulas Contractuales Tipo de la UE.

9. CERTIFICACIONES Y AUDITORÍAS

9.1. No más de una vez al año y con treinta (30) días de notificación por escrito por parte del Cliente, Entrust, en la medida en que actúe como Encargado del Tratamiento de datos del Cliente, pondrá a disposición del Cliente la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en las Leyes de Protección de Datos, siempre que Entrust no tenga la obligación de proporcionar información confidencial y / o propietaria. No más de una vez al año y con treinta (30) días de notificación por escrito, Entrust, en la medida en que actúe como Encargado del Tratamiento de datos del Cliente, a

raíz de una solicitud del Cliente y por cuenta del Cliente, permitirá y contribuirá a las auditorías e inspecciones externas por parte del Cliente o su auditor externo autorizado. El alcance, el tiempo, el costo y la duración de dichas auditorías, incluidas las condiciones de confidencialidad, serán acordados mutuamente por Entrust y el Cliente antes de la iniciación. El Cliente notificará de inmediato a Entrust información sobre el incumplimiento descubierto durante el curso de una auditoría, y Entrust hará todos los esfuerzos comercialmente razonables para abordar cualquier incumplimiento confirmado..

10. Aviso

10.1. Cualquier aviso requerido por Entrust al Customer en virtud de esta Adenda se enviará a _____.

Lista de Anexos

Anexo 1: Detalles del Tratamiento

Anexo 2: Cláusulas Contractuales Tipo de la UE

Los signatarios autorizados de las partes han suscrito debidamente esta DPA:

En nombre del Cliente:

Nombre del Cliente: _____

Nombre (completo): _____

Cargo: _____

Dirección: _____

Firma: _____

Fecha: _____

En nombre de Entrust:

Nombre (completo): **Lisa J. Tibbits**

Cargo: **Chief Legal and Compliance Officer**

Dirección: **1187 Park Place, Shakopee, Minnesota 55379-3817 USA**

Firma: _____

ANEXO 1 - DETALLES DEL TRATAMIENTO DE DATOS PERSONALES

Naturaleza y Finalidad del Tratamiento

Entrust procesará los Datos personales según sea necesario para realizar los Servicios de conformidad con el Acuerdo, como se especifica en la documentación relacionada con los Servicios y según las instrucciones del Cliente en el uso de los Servicios.

Duración del Tratamiento

Entrust tratará los Datos Personales durante la vigencia del Acuerdo, a menos que se acuerde lo contrario por escrito o según lo exijan las leyes aplicables.

Categorías de los Interesados

El Cliente puede enviar Datos Personales a Entrust, cuyo alcance es determinado y controlado por el Cliente a su exclusivo criterio (pero de acuerdo con las Leyes de protección de datos), y que pueden incluir, entre otros, Datos Personales relacionados con las siguientes categorías de Interesados:

- Empleados, clientes, agentes y subcontratistas del cliente
- Los usuarios finales del Cliente autorizados por el Cliente para utilizar los Servicios
- Véase también el correspondiente aviso de privacidad de producto

Categorías de Datos Personales

El Cliente puede enviar Datos Personales a Entrust, cuyo alcance es determinado y controlado por el Cliente a su exclusivo criterio (pero de acuerdo con las Leyes de protección de datos), y que pueden incluir, entre otras, las siguientes categorías de Datos Personales:

- Datos de contacto comercial (nombre, cargo / puesto, dirección, número de teléfono, número de fax, dirección de correo electrónico, ubicación) de los empleados, clientes, agentes, subcontratistas y usuarios finales del Cliente autorizados por el Cliente para utilizar los Servicios
- Datos de conexión (dirección IP, nombre de usuario, datos de identificación utilizados con fines de autenticación) de los empleados, clientes, agentes, subcontratistas y usuarios finales del Cliente autorizados por el Cliente para utilizar los Servicios
- Datos biométricos de los empleados, clientes, agentes, subcontratistas y usuarios finales del Cliente autorizados por el Cliente para utilizar los Servicios.
- Véase también el correspondiente aviso de privacidad de producto

ANEXO 2 – CLÁUSULAS CONTRACTUALES TIPO (Responsable a encargado)

SECCIÓN I

Cláusula 1

Finalidad y ámbito de aplicación

a) La finalidad de estas cláusulas contractuales tipo es garantizar que se cumplan los requisitos que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (1) (Reglamento general de protección de datos)[1], exige para la transferencia de datos personales a un tercer país.

b) Las partes:

   i. la(s) persona(s) física(s) o jurídica(s), autoridad(es) pública(s), servicio(s) u organismo(s) (en lo sucesivo, «entidad» o «entidades») que va(n) a transferir los datos personales, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «exportador de datos»), y

   ii. la(s) entidad(es) en un tercer país que va(n) a recibir los datos personales del exportador de datos directamente o indirectamente por medio de otra entidad que también sea parte en el presente pliego de cláusulas, enumerada(s) en el anexo I.A (cada una denominada en lo sucesivo «importador de datos»),

   han pactado las presentes cláusulas contractuales tipo (en lo sucesivo, «pliego de cláusulas»).

c) El presente pliego de cláusulas se aplica a la transferencia de datos personales especificada en el anexo I.B.

d) El apéndice del presente pliego de cláusulas, que contiene los anexos que se citan en estas, forman parte del pliego.

Cláusula 2

Efecto e invariabilidad de las cláusulas.

a) El presente pliego de cláusulas establece garantías adecuadas, incluidos derechos exigibles de los interesados y acciones judiciales eficaces, de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679 y, en relación con las transferencias de datos de responsables a encargados o de encargados a otros encargados,

[1] Cuando el exportador de datos sea un encargado del tratamiento sujeto al Reglamento (UE) 2016/679 que actúe por cuenta de una institución u organismo de la Unión como responsable del tratamiento, se considera que la utilización del presente pliego de cláusulas al recurrir a otro encargado (subtratamiento) no sujeto al Reglamento (UE) 2016/679 también garantiza el cumplimento del artículo 29, apartado 4, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE (DO L 295 de 21.11.2018, p. 39), en la medida en que estén armonizados el presente pliego de cláusulas y las obligaciones en materia de protección de datos que imponga el contrato u otro acto jurídico celebrado entre el responsable y el encargado con arreglo al artículo 29, apartado 3, del Reglamento (UE) 2018/1725. Este será el caso, en particular, cuando el responsable y el encargado del tratamiento se basen en las cláusulas contractuales tipo incluidas en la Decisión 2021/915.

de conformidad con las cláusulas contractuales tipo a que se refiere el artículo 28, apartado 7, del Reglamento (UE) 2016/679 siempre que no se modifiquen, salvo para seleccionar el módulo o módulos adecuados o para añadir o actualizar información del apéndice. Esto no es óbice para que las partes incluyan en un contrato más amplio las cláusulas contractuales tipo que contiene el presente pliego, ni para que añadan otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, al presente pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

b) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el exportador de datos en virtud del Reglamento (UE) 2016/679.

Cláusula 3

Terceros beneficiarios

a) Los interesados podrán invocar, como terceros beneficiarios, el presente pliego de cláusulas contra el exportador y/o el importador de datos y exigirles su cumplimiento, con las excepciones siguientes.
   i. Cláusulas 1, 2, 3, 6 y 7.
   ii. Cláusula 8.1, letra b) y cláusla 8.9, letras a), c), d) y e).
   iii. Cláusula 9, letra a), c), d) y e).
   iv. Cláusula 12, letras a), d) y f).
   v. Cláusula 13.
   vi. Cláusula 15.1, letras c), d) y e).
   vii. Cláusula 16, letra e).
   viii. Cláusula 18, letras a) y b).

b) Lo dispuesto en la letra a) se entiende sin perjuicio de los derechos que el Reglamento (UE) 2016/679 otorga a los interesados.

Cláusula 4

Interpretación

a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en dicho Reglamento.
b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.
c) El presente pliego de cláusulas no se podrá interpretar de manera que entre en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679.

Cláusula 5

Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicarse el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 6

Descripción de la transferencia o transferencias

Los datos de la transferencia o transferencias y, en particular, las categorías de datos personales que se transfieren y los fines para los que se transfieren se especifican en el anexo I.B.

SECCIÓN II: OBLIGACIONES DE LAS PARTES

Cláusula 8

Garantías en materia de protección de datos

El exportador de datos garantiza que ha hecho esfuerzos razonables para determinar que el importador de datos puede, aplicando medidas técnicas y organizativas adecuadas, cumplir las obligaciones que le atribuye el presente pliego de cláusulas..

8.1 Instrucciones

a) El importador de datos solo tratará los datos personales siguiendo instrucciones documentadas del exportador de datos. El exportador de datos podrá dar dichas instrucciones durante todo el período de vigencia del contrato.
b) El importador de datos informará inmediatamente al exportador de datos en caso de que no pueda seguir dichas instrucciones.

8.2 Limitación de la finalidad

El importador de datos tratará los datos personales únicamente para los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando siga instrucciones adicionales del exportador de datos

8.3 Transparencia

Previa solicitud, el exportador de datos pondrá gratuitamente a disposición del interesado una copia del presente pliego de cláusulas, incluido el apéndice cumplimentado por las partes. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como las medidas descritas en el anexo II y datos personales, el exportador de datos podrá expurgar el texto del apéndice del presente pliego de cláusulas antes de compartir una copia, pero deberá aportar un resumen significativo si, de no hacerlo, el interesado no pudiere comprender el tenor del apéndice o ejercer sus derechos. Previa solicitud, las partes comunicarán al interesado los motivos del expurgo, en la medida de lo posible sin revelar la información expurgada. La presente cláusula se entiende sin perjuicio de las obligaciones que los artículos 13 y 14 del Reglamento (UE) 2016/679 atribuyen al exportador de datos.

8.4. Exactitud

Si el importador de datos tiene conocimiento de que los datos personales que ha recibido son inexactos o han quedado obsoletos, informará de ello al exportador de datos sin dilación indebida. En este caso, el importador de datos colaborará con el exportador de datos para suprimir o rectificar los datos.

8.5. Duración del tratamiento y supresión o devolución de los datos

El tratamiento por parte del importador de datos solo se realizará durante el período especificado en el anexo I.B. Una vez se hayan prestado los servicios de tratamiento, el importador de datos suprimirá, a petición del exportador de datos, todos los datos personales tratados por cuenta del exportador de datos y acreditará al exportador de datos que lo ha hecho, o devolverá al exportador de datos todos los datos personales tratados en su nombre y suprimirá las copias existentes. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país. Lo anterior se entiende sin perjuicio de la cláusula 14 y, en particular, de la obligación que esta impone al importador de datos de informar al exportador de datos durante todo el período de vigencia del contrato si tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la cláusula 14, letra a).

8.6. Seguridad del tratamiento

a) El importador de datos y, durante la transferencia, también el exportador de datos aplicarán medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos; en particular, la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados (en lo sucesivo, «violación de la seguridad de los datos personales»). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para los interesados. Las partes deberán considerar, en particular, el cifrado o la seudonimización, especialmente durante la transmisión, si de este modo se puede cumplir la finalidad del tratamiento. En caso de seudonimización, la información adicional necesaria para atribuir los datos personales a un interesado específico quedará, en la medida de lo posible, bajo el control exclusivo del exportador de datos. Al cumplir las obligaciones que le impone el presente párrafo, el importador de datos aplicará, al menos, las medidas técnicas y organizativas que figuran en el anexo II. El importador de datos llevará a cabo controles periódicos para garantizar que estas medidas sigan proporcionando un nivel de seguridad adecuado.
b) El importador de datos solo concederá acceso a los datos personales a los miembros de su personal en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. Garantizará que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
c) En caso de violación de la seguridad de datos personales tratados por el importador de datos en virtud del presente pliego de cláusulas, el importador de datos adoptará medidas adecuadas para ponerle remedio y, en particular, medidas para mitigar los efectos negativos. El importador de datos también lo notificará al exportador de datos sin dilación indebida una vez tenga conocimiento de la violación de la seguridad. Dicha notificación incluirá los datos de un punto de contacto en el que pueda obtenerse más información, una descripción de la naturaleza de la violación (en la que figuren, cuando sea posible, las categorías y el número aproximado de interesados y registros de datos personales

afectados), las consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, especialmente, en su caso, medidas para mitigar sus posibles efectos negativos. Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

d) El importador de datos deberá colaborar con el exportador de datos y ayudarle para que pueda cumplir las obligaciones que le atribuye el Reglamento (UE) 2016/679, especialmente en cuanto a la notificación a la autoridad de control competente y a los interesados afectados, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el importador de datos.

8.7. Datos sensibles

En la medida en que la transferencia incluya datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, «datos sensibles»), el importador de datos aplicará las restricciones específicas y/o las garantías adicionales descritas en el anexo I.B.

8.8. Transferencias ulteriores

El importador de datos solo comunicará los datos personales a un tercero siguiendo instrucciones documentadas del exportador de datos. Por otra parte, solo se podrán comunicar los datos a terceros situados fuera de la Unión Europea[2] (en el mismo país que el importador de datos o en otro tercer país; en lo sucesivo, «transferencia ulterior») si el tercero está vinculado por el presente pliego de cláusulas o consiente a someterse a este, con elección del módulo correspondiente, o si:

i. la transferencia ulterior va dirigida a un país sobre el que haya recaído una decisión de adecuación, con arreglo al artículo 45 del Reglamento (UE) 2016/679, que abarque la transferencia ulterior;
ii. el tercero aporta de otro modo garantías adecuadas, con arreglo a los artículos 46 o 47 del Reglamento (UE) 2016/679, respecto del tratamiento en cuestión;
iii. si la transferencia ulterior es necesaria para la formulación, el ejercicio o la defensa de reclamaciones en el marco de procedimientos administrativos, reglamentarios o judiciales específicos; o
iv. si la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

[2] El Acuerdo sobre el Espacio Económico Europeo (en lo sucesivo, el «Acuerdo EEE») dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos y, en particular, el Reglamento (UE) 2016/679 están cubiertos por el Acuerdo EEE y han sido incorporados al anexo XI del mismo. Por lo tanto, toda comunicación del importador de datos a un tercero situado en el EEE no puede considerarse una transferencia ulterior a efectos del presente pliego de cláusulas.

La validez de las transferencias ulteriores depende de que el importador de datos aporte las demás garantías previstas en el presente pliego de cláusulas y, en particular, la limitación de la finalidad.

8.9. Documentación y cumplimiento

a) El importador de datos resolverá con presteza y de forma adecuada las consultas del exportador de datos relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.
b) Las partes deberán poder demostrar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos conservará suficiente documentación de las actividades de tratamiento que se realicen por cuenta del exportador de datos.
c) El importador de datos pondrá a disposición del exportador de datos toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y, a instancia del exportador de datos, permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el exportador de datos podrá tener en cuenta las certificaciones pertinentes que obren en poder del importador de datos.
d) El exportador de datos podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías podrán consistir en inspecciones de los locales o instalaciones físicas del importador de datos y, cuando proceda, realizarse con un preaviso razonable.
e) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refieren las letras b) y c) y, en particular, los resultados de las auditorías.

Cláusula 9

Recurso a subencargados

a) AUTORIZACIÓN GENERAL POR ESCRITO: El importador de datos cuenta con una autorización general del exportador de datos para contratar a subencargados que figuren en una lista acordada. El importador de datos informará al exportador de datos específicamente y por escrito de las adiciones o sustituciones de subencargados previstas en dicha lista con al menos [especificar período de tiempo] de antelación, de modo que el exportador de datos tenga tiempo suficiente para formular objeción a tales cambios antes de que se contrate al subencargado o subencargados de que se trate. El importador de datos proporcionará al exportador de datos la información necesaria para que este pueda ejercer su derecho a formular objeción.
b) Cuando el importador de datos recurra a un subencargado para llevar a cabo actividades específicas de tratamiento (por cuenta del exportador de datos), lo hará por medio de un contrato escrito que establezca, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al importador de datos en virtud del presente pliego de cláusulas, especialmente en lo que se refiere a los derechos de los interesados en cuanto

que terceros beneficiarios[3]. Las Partes convienen que, al cumplir el presente pliego de cláusulas, el importador de datos también da cumplimiento a las obligaciones que le atribuye la cláusula 8.8. El importador de datos se asegurará de que el subencargado cumpla las obligaciones que le atribuya el presente pliego de cláusulas.

c) El importador de datos proporcionará al exportador de datos, a instancia de este, una copia del contrato con el subencargado y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el importador de datos podrá expurgar el texto del contrato antes de compartir la copia.
d) El importador de datos seguirá siendo plenamente responsable ante el exportador de datos del cumplimiento de las obligaciones que imponga al subencargado su contrato con el importador de datos. El importador de datos notificará al exportador de datos los incumplimientos por parte del subencargado de las obligaciones que le atribuye dicho contrato.
e) El importador de datos pactará con el subencargado una cláusula de tercero beneficiario en virtud de la cual, en caso de que el importador de datos desaparezca de facto, cese de existir jurídicamente o sea insolvente, el exportador de datos tendrá derecho a rescindir el contrato del subencargado y ordenar a este que suprima o devuelva los datos personales.

Cláusula 10

Derechos del interesado

a) El importador de datos notificará con presteza al exportador de datos las solicitudes que reciba del interesado. No responderá a dicha solicitud por sí mismo, a menos que el exportador de datos le haya autorizado a hacerlo.
b) El importador de datos ayudará al exportador de datos a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos que el Reglamento (UE) 2016/679 atribuye a los interesados. A este respecto, las partes establecerán en el anexo II medidas técnicas y organizativas apropiadas, teniendo en cuenta la naturaleza del tratamiento, por las que se garantice que se prestará ayuda al responsable a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.
c) En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el importador de datos seguirá las instrucciones del exportador de datos.

Cláusula 11

Reparación

a) El importador de datos informará a los interesados, de forma transparente y en un formato de fácil acceso, mediante notificación individual o en su página web, del punto de contacto autorizado para tramitar reclamaciones. Este tramitará con presteza las reclamaciones que reciba de los interesados.

[3] Este requisito podrá satisfacerse si el subencargado se adhiere al presente pliego de cláusulas, con elección del módulo correspondiente, con arreglo a la cláusula 7.

b) En caso de litigio entre un interesado y una de las partes en relación con el cumplimiento del presente pliego de cláusulas, dicha parte hará todo lo posible para resolver amistosamente el problema de forma oportuna. Las partes se mantendrán mutuamente informadas de tales litigios y, cuando proceda, colaborarán para resolverlos.
c) El importador de datos se compromete a aceptar, cuando el interesado invoque un derecho de tercero beneficiario con arreglo a la cláusula 3, la decisión del interesado de:
    i. presentar una reclamación ante la autoridad de control del Estado miembro de su residencia habitual o su lugar de trabajo o ante la autoridad de control competente con arreglo a la cláusula 13.
    ii. ejercitar una acción judicial en el sentido de la cláusula 18.
d) Las partes aceptan que el interesado pueda estar representado por una entidad, organización o asociación sin ánimo de lucro en las condiciones establecidas en el artículo 80, apartado 1, del Reglamento (UE) 2016/679.
e) El importador de datos acepta acatar las resoluciones que sean vinculantes con arreglo al Derecho aplicable de la UE o del Estado miembro de que se trate.
f) El importador de datos acepta que la elección del interesado no menoscabe sus derechos sustantivos y procesales a obtener reparación de conformidad con el Derecho aplicable.

Cláusula 12

Responsabilidad

a) Cada parte será responsable ante la(s) otra(s) de cualquier daño y perjuicio que le(s) cause por cualquier vulneración del presente pliego de cláusulas.
b) El importador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el importador de datos o su subencargado ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas.
c) A pesar de lo dispuesto en la letra b), el exportador de datos será responsable ante el interesado; el interesado tendrá derecho a que se le indemnice por los daños y perjuicios materiales o inmateriales que el exportador de datos o el importador de datos (o su subencargado) ocasionen al interesado por vulnerar los derechos de terceros beneficiarios que deriven del presente pliego de cláusulas. Lo anterior se entiende sin perjuicio de la responsabilidad del exportador de datos y, cuando el exportador de datos sea un encargado que actúe por cuenta de un responsable, de la responsabilidad del responsable con arreglo al Reglamento (UE) 2016/679 o el Reglamento (UE) 2018/1725, según cuál sea de aplicación.
d) Las partes acuerdan que, si el exportador de datos es considerado responsable, de conformidad con la letra c), de los daños o perjuicios causados por el importador de datos (o su subencargado), estará legitimado para exigir al importador de datos la parte de la indemnización que sea responsabilidad del importador de los datos.
e) Cuando más de una parte sea responsable de un daño o perjuicio ocasionado al interesado como consecuencia de una vulneración del presente pliego de cláusulas, todas las partes responsables serán responsables solidariamente.

f) Las partes acuerdan que, si una parte es considerada responsable con arreglo a la letra e), estará legitimada para exigir a la otra parte la parte de la indemnización correspondiente a su responsabilidad por el daño o perjuicio.
g) El importador de datos no puede alegar la conducta de un subencargado del tratamiento para eludir su propia responsabilidad.

Cláusula 13

Supervisión

a) La autoridad de control responsable de garantizar que el exportador de datos cumpla el Reglamento (UE) 2016/679 en cuanto a la transferencia de los datos, indicada en el anexo I.C, actuará como autoridad de control competente.
b) El importador de datos da su consentimiento a someterse a la jurisdicción de la autoridad de control competente y a cooperar con ella en cualquier procedimiento destinado a garantizar el cumplimiento del presente pliego de cláusulas. En particular, el importador de datos se compromete a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Remitirá a la autoridad de control confirmación por escrito de que se han tomado las medidas necesarias.

SECCIÓN III: DERECHO DEL PAÍS Y OBLIGACIONES EN CASO DE ACCESO POR PARTE DE LAS AUTORIDADES PÚBLICAS

Cláusula 14

Derecho y prácticas del país que afectan al cumplimiento de las cláusulas

a) Las partes aseguran que no tienen motivos para creer que el Derecho y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales por el importador de datos, especialmente los requisitos para la comunicación de los datos personales o las medidas de autorización de acceso por parte de las autoridades públicas, impidan al importador de datos cumplir las obligaciones que le atribuye el presente pliego de cláusulas. Dicha aseveración se fundamenta en la premisa de que no se oponen al presente pliego de cláusulas el Derecho y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1, del Reglamento (UE) 2016/679.
b) Las partes declaran que, al aportar la garantía a que se refiere la letra a), han tenido debidamente en cuenta, en particular, los aspectos siguientes:

    i. las circunstancias específicas de la transferencia, como la longitud de la cadena de tratamiento, el número de agentes implicados y los canales de transmisión utilizados; las transferencias ulteriores previstas; el tipo de destinatario; la finalidad del tratamiento; las categorías y el formato de los datos personales transferidos; el sector económico en el que tiene lugar la transferencia; el lugar de almacenamiento de los datos transferidos.

ii. el Derecho y las prácticas del tercer país de destino —especialmente las que exijan comunicar datos a las autoridades públicas o autorizar el acceso de dichas autoridades— que sean pertinentes dadas las circunstancias específicas de la transferencia, así como las limitaciones y garantías aplicables [4];

iii. las garantías contractuales, técnicas u organizativas pertinentes aportadas para complementar las garantías previstas en el presente pliego de cláusulas, especialmente incluidas las medidas aplicadas durante la transferencia y el tratamiento de los datos personales en el país de destino.

c) El importador de datos asegura que, al llevar a cabo la valoración a que se refiere la letra b), ha hecho todo lo posible por proporcionar al exportador de datos la información pertinente y se compromete a seguir colaborando con el exportador de datos para garantizar el cumplimiento del presente pliego de cláusulas.

d) Las partes acuerdan documentar la evaluación a que se refiere la letra b) y ponerla a disposición de la autoridad de control competente previa solicitud.

e) El importador de datos se compromete a notificar con presteza al exportador de datos si, tras haberse vinculado por el presente pliego de cláusulas y durante el período de vigencia del contrato, tiene motivos para creer que está o ha estado sujeto a normativa o prácticas que no se ajustan a los requisitos de la letra a), incluso a raíz de un cambio de la normativa en el tercer país o de una medida (como una solicitud de comunicación) que indique una aplicación de dicha normativa en la práctica que no se ajuste a los requisitos de la letra a).

f) De realizarse la notificación a que se refiere la letra e) o si el exportador de datos tiene motivos para creer que el importador de datos ya no puede cumplir las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos determinará con presteza las medidas adecuadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que deberán adoptar el exportador de datos y/o el importador de datos para poner remedio a la situación [módulo tres:, si procede, tras consultar al responsable]. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone [módulo tres: el responsable o] la autoridad de control competente. En este supuesto, el exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con

[4] Por lo que se refiere al efecto de dicho Derecho y prácticas en el cumplimiento del presente pliego de cláusulas, a la hora de realizar una valoración integral de esta cuestión pueden tenerse en cuenta distintos aspectos. Uno de estos aspectos puede ser que haya experiencia práctica pertinente y documentada en casos anteriores de solicitudes de comunicación por parte de las autoridades públicas, o la ausencia de tales solicitudes, en un período suficientemente representativo. Con esto se quiere decir, en particular, los registros internos u otra documentación elaborados de forma continua con la diligencia debida y certificados en los niveles más altos de la dirección siempre que esta información pueda compartirse legalmente con terceros. Cuando se use esta experiencia práctica para llegar a la conclusión de que el importador de datos no tendrá impedimento para cumplir el presente pliego de cláusulas, deberá estar respaldada por otros elementos pertinentes y objetivos; corresponde a las partes valorar minuciosamente si la suma de estos factores es suficientemente determinante, en términos de fiabilidad y representatividad, para respaldar esta conclusión. En particular, las partes deben tener en cuenta si su experiencia práctica está corroborada y no se ve desmentida, por información que sea fiable y de dominio público o accesible de cualquier otro modo acerca de la existencia o ausencia de solicitudes en el mismo sector o acerca de la aplicación de la normativa de que se trate en la práctica, como jurisprudencia e informes de organismos de supervisión independientes.

respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa. En caso de resolución del contrato en virtud de la presente cláusula, será de aplicación la cláusula 16, letras d) y e).

Cláusula 15

Obligaciones del importador de datos en caso de acceso por parte de las autoridades públicas

15.1 Notificación

a) El importador de datos se compromete a notificar con presteza al exportador de datos y, cuando sea posible, al interesado (de ser necesario, con la ayuda del exportador de datos) si:
   i. recibe una solicitud jurídicamente vinculante de comunicación de datos personales transferidos con arreglo al presente pliego de cláusulas presentada por una autoridad pública (sobre todo, judicial) en virtud del Derecho del país de destino; dicha notificación contendrá información sobre los datos personales solicitados, la autoridad solicitante, la base jurídica de la solicitud y la respuesta dada; o
   ii. tiene conocimiento de que las autoridades públicas han tenido acceso directo a los datos personales transferidos con arreglo al presente pliego de cláusulas en virtud del Derecho del país de destino; dicha notificación incluirá toda la información de que disponga el importador de datos.

b) Si se prohíbe al importador de datos enviar la notificación al exportador de datos y/o al interesado en virtud del Derecho del país de destino, el importador de datos se compromete a hacer todo lo posible para obtener una dispensa de la prohibición, con el fin de comunicar toda la información disponible y lo antes posible. El importador de datos se compromete a documentar las actuaciones que realice a tal fin para poder justificar su diligencia si se lo pide el exportador de datos.

c) En la medida en que lo permita el Derecho del país de destino, el importador de datos se compromete a proporcionar al exportador de datos, a intervalos regulares durante el período de vigencia del contrato, la mayor cantidad posible de información pertinente sobre las solicitudes recibidas (en particular, el número de solicitudes, el tipo de datos solicitados, la autoridad o autoridades solicitantes, la impugnación de las solicitudes, el resultado de tales impugnaciones, etc.).

d) El importador de datos se compromete a conservar la información a que se refieren las letras a) a c) durante el período de vigencia del contrato y a ponerla a disposición de la autoridad de control competente previa solicitud.

e) Las letras a) a c) se entenderán sin perjuicio de la obligación del importador de datos, contemplada en la cláusula 14, letra e), y en la cláusula 16, de informar con presteza al exportador de datos cuando no pueda dar cumplimiento al presente pliego de cláusulas.

15.2 Control de la legalidad y minimización de datos

a) El importador de datos se compromete a controlar la legalidad de la solicitud de comunicación y, en particular, si la autoridad pública solicitante está debidamente facultada para ello, así como a impugnar la solicitud si, tras una valoración minuciosa, llega a la conclusión de que existen motivos razonables para considerar que la solicitud es ilícita con arreglo al Derecho del país de destino, incluidas las obligaciones aplicables en virtud del

Derecho internacional y los principios de cortesía internacional. El importador de datos agotará, en las mismas condiciones, las vías de recurso. Al impugnar una solicitud, el importador de datos instará la aplicación de medidas cautelares para suspender los efectos de la solicitud hasta que la autoridad judicial competente se haya pronunciado sobre el fondo. No comunicará los datos personales solicitados hasta que se lo exija la normativa procesal aplicable. Estos requisitos se entienden sin perjuicio de las obligaciones que la cláusula 14, letra e), atribuye al importador de datos.

b) El importador de datos se compromete a documentar sus valoraciones jurídicas y las impugnaciones de solicitudes de comunicación y a poner dicha documentación a disposición del exportador de datos en la medida en que lo permita el Derecho del país de destino. También pondrá dicha documentación a disposición de la autoridad de control competente previa solicitud..

c) El importador de datos se compromete a proporcionar la mínima información posible al responder a las solicitudes de comunicación, basándose en una interpretación razonable de la solicitud.

SECCIÓN IV: DISPOSICIONES FINALES

Cláusula 16

Incumplimiento de las cláusulas y resolución del contrato

a) El importador de datos informará con presteza al exportador de datos en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.

b) En caso de que el importador de datos incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el exportador de datos suspenderá la transferencia de datos personales al importador de datos hasta que se vuelva a garantizar el cumplimiento o se resuelva el contrato. Lo anterior se entiende sin perjuicio de la cláusula 14, letra f).

c) El exportador de datos estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:

   i. el exportador de datos haya suspendido la transferencia de datos personales al importador de datos con arreglo a la letra b) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;

   ii. el importador de datos vulnere de manera sustancial o persistente el presente pliego de cláusulas; o

   iii. el importador de datos incumpla una resolución vinculante de un órgano jurisdiccional o autoridad de control competente en relación con las obligaciones que le atribuye el presente pliego de cláusulas.

   En este supuesto, informará a la autoridad de supervisión competente [módulo tres: y al responsable] de su incumplimiento. Si el contrato tiene más de dos partes contratantes, el exportador de datos solo podrá ejercer este derecho de resolución con respecto a la parte pertinente, a menos que las partes hayan acordado otra cosa.

d) Los datos personales que se hayan transferido antes de la resolución del contrato con arreglo a la letra c) deberán, a elección del exportador de datos, devolverse inmediatamente al exportador de datos o destruirse en su totalidad. Lo mismo será de aplicación a las copias

de los datos. El importador de datos acreditará la destrucción de los datos al exportador de datos. Hasta que se destruyan o devuelvan los datos, el importador de datos seguirá garantizando el cumplimiento con el presente pliego de cláusulas. Si el Derecho del país aplicable al importador de datos prohíbe la devolución o la destrucción de los datos personales transferidos, el importador de datos se compromete a seguir garantizando el cumplimiento del presente pliego de cláusulas y solo tratará los datos en la medida y durante el tiempo que exija el Derecho del país.

e) Cualquiera de las partes podrá revocar su consentimiento a quedar vinculada por el presente pliego de cláusulas si: i) la Comisión Europea adopta una decisión de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 que regule la transferencia de datos personales a los que se aplique el presente pliego de cláusulas; o ii) el Reglamento (UE) 2016/679 pasa a formar parte del ordenamiento jurídico del país al que se transfieren los datos personales. Ello se entiende sin perjuicio de otras responsabilidades que sean de aplicación al tratamiento en cuestión en virtud del Reglamento (UE) 2016/679.

Cláusula 17

Derecho aplicable

El presente pliego de cláusulas se regirá por el Derecho del Estado miembro de la Unión Europea en que esté establecido el exportador de datos. Cuando dicho Derecho no admita la existencia de derechos de los terceros beneficiarios, se regirá por el Derecho de otro Estado miembro de la Unión Europea que sí la admita. Las partes acuerdan que sea el Derecho de Irlanda.

Cláusula 18

Elección del foro y jurisdicción

a) Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente en un Estado miembro de la Unión Europea.
b) Las partes acuerdan que sean los órganos jurisdiccionales de Irlanda.
c) Los interesados también podrán ejercer acciones judiciales contra el exportador de datos y/o el importador de datos en el Estado miembro en el que el interesado tenga su residencia habitual.
d) Las partes acuerdan someterse a la jurisdicción de dicho Estado miembro.

ANEXO I DE LAS CLÁUSULAS CONTRACTUALES TIPO

A. Lista de Partes

Exportador de datos

El exportador de datos es el cliente.

Importador de datos

El importador de datos es la entidad legal de Entrust con la que el Cliente tiene un Acuerdo.

B. Descripción de la Transferencia

Interesados

Los datos personales transferidos se refieren a las siguientes categorías de interesados:

- Véase el anexo 1

Categorías de datos

Los datos personales transferidos se refieren a las siguientes categorías de datos:

- Véase el anexo 1

Frecuencia de la transferencia

Los datos personales se transferirán de forma continua.

Naturaleza y finalidad del tratamiento

Los datos personales transferidos estarán sujetos a las siguientes actividades básicas de tratamiento:

- La prestación de los Servicios de conformidad con el Acuerdo

Periodo de retención

Los datos personales se conservarán durante la vigencia del Acuerdo o más allá si así lo exige la ley.

Transferencia a subencargados

El objeto, la naturaleza y la duración del tratamiento por parte de los subencargados son los siguientes:

https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

C. Autoridad de control competente

La autoridad de control de Irlanda responsable de garantizar el cumplimiento por parte del exportador de datos del Reglamento (UE) 2016/679 en lo que respecta a la transferencia de datos, actuará como autoridad de control competente.

ANEXO II DE LAS CLÁUSULAS CONTRACTUALES TIPO

Este Anexo forma parte de las Cláusulas y ha sido acordado por las partes en virtud de su firma del DPA.

Descripción de las medidas de seguridad técnicas y organizativas implementadas por el importador de datos de acuerdo con las Cláusulas 4, letra d) y 5, letra c) (o documento / legislación adjunta):

Confiabilidad del personal: En la medida en que lo permita la ley, Entrust realiza verificaciones de antecedentes de todos los empleados antes del empleo, y los empleados y contratistas reciben capacitación en seguridad de la información durante la incorporación, así como anualmente. Todos los empleados deben leer y firmar las políticas de seguridad de la información de Entrust.

Cumplimiento, auditorías y certificaciones: Entrust, con el pleno compromiso de su alta dirección, cree firmemente que el principio fundamental de su éxito en la innovación es su estrategia de seguridad de la información. Esta estrategia se basa en el cumplimiento de la gobernanza en toda la empresa, un conjunto de controles y el estricto cumplimiento de las normativas y políticas federales, financieras, internacionales y de la industria. El sistema de gestión de seguridad de la información corporativa (ISMS por sus siglas en inglés) de Entrust cumple con la norma ISO 27001. Además, Entrust mantiene certificaciones de cumplimiento de varios otros estándares y marcos, según el producto, el servicio y la ubicación geográfica, incluidos:

- ISO 27701
- ISO 9000
- ISO 14000
- PCI CP
- PCI SAQ
- CAIQ Cloud Security Alliance
- Webtrust – CAB Forum
- NIST/FISMA
- NIST 800-53
- ETSI
- Tscheme

Para garantizar que la estrategia de seguridad de la información sea eficaz, Entrust aplica políticas y procedimientos de seguridad de la información en toda su organización, así como en todos los proyectos comerciales y técnicos. Gobernanza, Riesgo y Cumplimiento (GRC), Gestión de Amenazas y Vulnerabilidades (TVM por sus siglas en inglés), Arquitectura de Seguridad, Centro de Operaciones de Seguridad, Recuperación de Desastres, Continuidad del Negocio y Respuesta a Incidentes son los componentes integrales de esta estrategia.

Respuesta a incidentes:

A nivel operativo, Entrust ha instituido un plan de respuesta a incidentes de seguridad para supervisar los eventos de seguridad de datos identificados o detectados por las diversas tecnologías utilizadas para monitorear y alertar en función de umbrales o circunstancias específicos. Los

objetivos del plan de respuesta a incidentes de seguridad son administrar y coordinar los incidentes de seguridad de datos en todos los aspectos del entorno informático de Entrust, independientemente de la ubicación, el producto o el proceso, así como brindar oportunidades para educar a nuestros colegas sobre los riesgos y los controles de seguridad establecidos.

Centro de operaciones de seguridad (SOC):

Entrust se compromete a proteger los intereses de las partes interesadas manteniendo un Centro de operaciones de seguridad (SOC por sus siglas en inglés) sólido. El SOC es una unidad centralizada que monitorea la confidencialidad, integridad y disponibilidad de la infraestructura de tecnología de la información y se ocupa de la seguridad a nivel organizativo.

Gestión de amenazas y vulnerabilidades (TVM):

Entrust tiene un programa continuo de detección y corrección de vulnerabilidades. Este proceso se basa en herramientas y procedimientos certificados por la industria y es facilitado por profesionales competentes y experimentados. Los controles y medidas de gestión de amenazas y vulnerabilidades (TVM por sus siglas en inglés) son auditados varias veces al año por auditores calificados para garantizar que cumplimos con las leyes aplicables y los marcos de estándares de la industria..

Recuperación de desastres:

Entrust se compromete a proteger los intereses de las partes interesadas en caso de una emergencia o interrupción del negocio. Para ello, Entrust mantiene un programa integral de continuidad del negocio en toda la organización para proteger al personal, salvaguardar los activos y entornos corporativos y garantizar la disponibilidad continua de sus productos y servicios. Para respaldar el Programa de Continuidad de Negocio, Entrust también mantiene un Plan de Respuesta a Incidentes y Comunicaciones de Crisis para ayudar a fortalecer nuestra capacidad de respuesta a emergencias.

Continuidad del negocio:

Entrust se compromete a proteger los intereses de las partes interesadas en caso de una emergencia o interrupción del negocio. Para ello, Entrust mantiene un Programa de Continuidad Comercial integral para toda la organización que es consistente con la guía emitida por la Asociación Nacional de Protección contra Incendios (NFPA) (EE. UU.) 1600 - Estándar sobre Programas de Continuidad de Negocio y Gestión de Desastres / Emergencias, y la norma internacional ISO 22301 - Seguridad social: estándares de sistemas de gestión de la continuidad del negocio. El Plan de Continuidad del Negocio identifica los roles y responsabilidades funcionales de las agencias, organizaciones y departamentos internos y externos.

Adquisición, desarrollo y mantenimiento de sistemas y productos:

El programa de seguridad de la información de Entrust incluye políticas, estándares y procesos para el ciclo de vida de desarrollo del sistema (SDLC por sus siglas en inglés) que están alineados con las prácticas reconocidas por la industria para la gestión segura de los sistemas a lo largo de su ciclo de vida. Las fases del SDLC incluyen: Requisitos, Diseño, Implementación, Pruebas, Despliegue, Operaciones y Retiro. La identificación y corrección de vulnerabilidades son un enfoque central con el objetivo de minimizar la cantidad de fallos de seguridad en los productos y servicios de Entrust, y

minimizar el impacto en el Cliente cuando se descubren tales fallos. Los procesos descritos en este documento se aplican a los productos y servicios de Entrust y a los componentes de un sistema asociado que pueden utilizarse junto con un producto o servicio de Entrust. El programa garantizará que los procesos SDLC sean coherentes con los objetivos y expectativas de seguridad de la información de Entrust. Además, se establecerán líneas de base del sistema para respaldar el software y el firmware de Entrust dentro del ciclo de vida (por ejemplo, repositorios de origen) y para respaldar la implementación en entornos de producción. Cuando sea práctico, las líneas base del sistema se alinearán con los requisitos de cumplimiento.

Seguridad de la red:

Entrust mantiene controles y políticas de acceso para administrar qué acceso está permitido a la red y los sistemas de Entrust desde cada conexión de red y usuario, incluido el uso de firewalls o tecnología funcionalmente equivalente y controles de autenticación. Entrust mantendrá planes de acción correctiva y respuesta a incidentes para responder a posibles amenazas de seguridad..

Seguridad física y ambiental:

Las instalaciones de Entrust que albergan activos de información tecnológica están equipadas con controles adecuados para restringir el acceso físico a las instalaciones. Los controles de entrada física incluyen un medio para identificar al personal y los visitantes, y garantizar que la persona esté autorizada a acceder al área segura antes de la entrada. Todas las entradas a áreas seguras se registran y los registros se revisan periódicamente. El personal está informado y sujeto a las pautas establecidas para trabajar en áreas seguras. Los puntos de acceso, como las áreas de entrega o carga, y otros puntos donde personas no autorizadas pueden ingresar a la instalación, están controlados para restringir la entrada y, en la medida en que sea práctico, aislados de las áreas de procesamiento de información. Las medidas de seguridad física incluyen la capacidad de monitorear las instalaciones de la empresa para detectar el uso no autorizado o ilegal. Entrust tiene un plan de seguridad física que incorpora un procedimiento definido para reportar actividades sospechosas, debilidades de seguridad identificadas o posibles eventos de seguridad, así como un procedimiento de escalamiento para comunicar eventos a la policía local según corresponda. El personal de la instalación y los visitantes están informados sobre estos procedimientos de seguridad física y su responsabilidad de informar acerca de eventos de seguridad.

Política de transferencia de información:

La información a transferir deberá estar en todo momento debidamente asegurada, de acuerdo con su clasificación, independientemente del medio empleado para llevar la información o el mecanismo de transmisión. Toda la información que se transfiera estará sujeta a inspección en busca de códigos de software maliciosos y otros peligros potenciales para la confidencialidad, integridad o disponibilidad. Cuando se requiera el uso de cifrado para su custodia, dicho uso estará sujeto a todos los controles de seguridad aplicables, así como a los requisitos legales o reglamentarios. La información a transferir estará sujeta a los requisitos establecidos de conservación y eliminación. Las instalaciones de transferencia de información deberán cumplir con todas las leyes y regulaciones aplicables. La información y el software no se transferirán a partes externas hasta que se cumplan todos los requisitos contractuales y de seguridad relevantes, incluidos los acuerdos formales por escrito cuando sea necesario..

Gestión de terceros:

Las terceras partes de Entrust, como proveedores, subcontratistas, subencargados y proveedores de servicios, que tienen acceso a datos, información, instalaciones o tienen impacto en los productos o servicios de Entrust, se gestionan, supervisan, revisan y obligan continuamente a mantener altos estándares de privacidad y seguridad de la información. Los terceros se evalúan periódicamente en función de la sensibilidad de su nivel de acceso a los sistemas y la información, así como la criticidad de sus servicios. Entrust limita el acceso a terceros sobre la base de la "necesidad de saber" y lo revoca cuando ya no es necesario.