Anexo de tratamiento de datos

El presente Anexo de tratamiento de datos ("ATD") se incorpora al Contrato y lo complementa, con sus actualizaciones periódicas, entre la entidad de Clarivate que sea parte del Contrato (junto con sus Filiales, "Clarivate") y la entidad del Cliente que sea parte del Contrato ("Cliente" o "usted").

El Cliente suscribe el presente ATD en su propio nombre y, en la medida en que lo requieran las Leyes de protección de datos aplicables, en nombre y por cuenta de sus Filiales autorizadas si, y en la medida en que, Clarivate trate Datos personales para los que dichas Filiales autorizadas se consideren Responsables del tratamiento. Únicamente a efectos del presente ATD, y salvo que se indique lo contrario, el término "Cliente" incluirá al Cliente y a las Filiales autorizadas.

Todos los términos en mayúsculas no definidos en el presente ATD tendrán el significado establecido en el Contrato. Para evitar dudas, todas las referencias al "Contrato" incluirán el presente ATD, incluyendo las CCT (cuando sean aplicables), tal y como se definen en el presente documento.

1. Definiciones

(a) "**Filial**" se refiere a una entidad que directa o indirectamente controla, es controlada por, o está bajo el control común de, una entidad.

(b) "**Contrato**" se refiere a cualquier acuerdo entre Clarivate y el Cliente en virtud del cual Clarivate proporcione uno o más de los Servicios al Cliente que incorpore este ATD. Este ATD u otras condiciones de tratamiento de datos incorporadas a dicho Contrato por referencia son, colectivamente, el "Contrato".

(c) "**Filial autorizada**" se refiere a cualquier Filial del Cliente que (a) esté sujeta a las Leyes de protección de datos de la UE y (b) esté autorizada a utilizar los Servicios de conformidad con el Contrato entre el Cliente y Clarivate, pero que no haya firmado su propio Formulario de pedido con Clarivate y no sea un "Cliente", tal y como se define en este ATD.

(d) "**Datos personales del Cliente**" se refiere a cualquier dato personal que Clarivate trate como encargado del tratamiento en nombre del Cliente a través del Servicio, tal y como se describe más concretamente en este ATD. Para mayor claridad, los Datos personales del Cliente no incluyen los datos personales de los que Clarivate es responsable del tratamiento y que trate de conformidad con el **Aviso de privacidad corporativo** de Clarivate.

(e) "**Control**" significa una participación en la propiedad, en el voto o similar que represente el cincuenta por ciento (50 %) o más del total de las participaciones de la entidad en cuestión en circulación en ese momento. El término "Controlado" se interpretará en consecuencia.

(f) "**Leyes de protección de datos**" se refiere a todas las leyes y reglamentos de protección de datos aplicables al tratamiento de los Datos personales del Cliente por una de las partes en virtud del Contrato, incluyendo, en su caso, la Ley de Protección de Datos de la UE; la Ley de Privacidad del Consumidor de California ("CCPA"); la Ley de Protección de Datos Personales y Documentos Electrónicos de Canadá ("LPRPDE"); la Ley General de Protección de Datos de Brasil ("LGPD"), Ley Federal n.º 13.709/2018; la Ley de Privacidad de 1988 de Australia, con sus modificaciones ("Ley de Privacidad de Australia") y la Ley de Protección de Datos de Reino Unido.

(g) "**Ley de Protección de Datos de la UE**" se refiere a todas las leyes y reglamentos de protección de datos aplicables en Europa, incluyendo (i) el Reglamento 2016/679 del Parlamento Europeo y del Consejo 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 (Reglamento General de Protección de Datos) ("RGPD") (ii) la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas; (iii) las transposiciones nacionales aplicables de (i) y (ii).

(h) "**CCT de la UE**" se refiere a las cláusulas contractuales tipo para los encargados del tratamiento aprobadas por la Comisión Europea.

(i) "**Europa**" se refiere, a efectos de este ATD, a la Unión Europea, el Espacio Económico Europeo y/o sus estados miembros y Suiza.

(j) "**Violación de la seguridad de los datos personales**" se refiere a cualquier violación no autorizada o ilegal de la seguridad que conduzca a la destrucción, a la pérdida o a la alteración accidental o ilegal, o a la divulgación o al acceso no autorizados a los Datos personales del Cliente en los sistemas gestionados o controlados en general por Clarivate.

(k) "**Servicios**" se refiere a los servicios pertinentes identificados en el Contrato.

(l) "**CCT**" se refiere a las CCT de la UE y el Anexo de Reino Unido.

(m) "**Categoría especial de datos personales**" se refiere a: (a) datos genéticos; (b) datos biométricos con el fin de identificar de forma exclusiva a una persona física; (c) datos relativos a la salud o a la vida sexual u orientación sexual de una persona física; (d) datos personales que revelen convicciones raciales, étnicas, políticas o religiosas, o la pertenencia a un sindicato; y (e) datos personales relativos a condenas e infracciones penales.

(n) "**Subencargado del tratamiento**" se refiere a cualquier encargado del tratamiento contratado por Clarivate o sus Filiales para ayudar a cumplir sus obligaciones con respecto a la prestación del Servicio de conformidad con el Contrato o este ATD. Los Subencargados del tratamiento podrán incluir a terceros o Filiales de Clarivate, pero excluirán a los empleados, contratistas o consultores de Clarivate.
(o) "**Anexo de Reino Unido**" se refiere al anexo de transferencia internacional de datos a las Cláusulas contractuales tipo de la Comisión de la UE emitido por la Oficina del Comisionado de Información del Reino Unido.
(p) "Ley de protección de datos de Reino Unido" se refiere a cualquier ley y reglamento de protección de datos, privacidad y marketing electrónico aplicable, tanto actual como futuro, incluida la Ley de protección de datos de Reino Unido de 2018, el RGPD tal y como se ha implantado en las leyes de Reino Unido ("RGPD de Reino Unido") y el Reglamento de privacidad y comunicaciones electrónicas de 2003.
(q) "**Transferencia internacional de Reino Unido**" se refiere a una transferencia de datos personales para la que se requieren las garantías adecuadas, a partir del momento, en virtud de la Ley de Protección de Datos del Reino Unido.

Los términos "**garantías adecuadas**", "**responsable del tratamiento**", "**interesado**", "**datos personales**", "**encargado del tratamiento**" y "**tratamiento**" tendrán el significado que se les atribuye en las Leyes de protección de datos aplicables o, si no se definen en ellas, en el RGPD, y "**tratar**", "**tratando**" y "**tratado**", con respecto a cualquier Dato personal del Cliente, se interpretarán en consecuencia.

2. Funciones y responsabilidades

(a) **Funciones de las partes**. Si las Leyes de protección de datos aplicables se aplican al tratamiento de los Datos personales del Cliente por cualquiera de las partes, las partes reconocen y aceptan que, (i) con respecto al tratamiento de los Datos personales del Cliente, el Cliente es el responsable del tratamiento y Clarivate es un encargado del tratamiento que actúa en nombre del Cliente, tal y como se describe con más detalle en el Apéndice A (Detalles del tratamiento de datos) de este ATD y (ii) los Datos personales del cliente se tratarán de conformidad con las leyes de protección de datos aplicables.
(b) Limitación de la finalidad. Clarivate tratará los Datos personales del Cliente únicamente de conformidad con las instrucciones legales documentadas del Cliente, según sea necesario para cumplir con la legislación aplicable. Las partes acuerdan que en este ATD y el Contrato se establecen las instrucciones completas y definitivas del Cliente a Clarivate en relación con el tratamiento de los Datos personales del Cliente, y un tratamiento ajeno al ámbito de estas instrucciones (si lo hubiera) habrá de establecerse por escrito entre las partes ("Fines permitidos").
(c) Datos prohibidos. A menos que se establezca lo contrario en el Apéndice A de este ATD, el Cliente no proporcionará (ni hará que se proporcione) ninguna Categoría especial de Datos personales a Clarivate para su tratamiento en virtud del Contrato, y Clarivate no tendrá responsabilidad alguna por dichos datos, ya sea en relación con una Violación de la seguridad de los datos personales o de otra manera.
(d) Cumplimiento del Cliente. El Cliente declara y garantiza que (i) ha cumplido, y seguirá cumpliendo, con todas las leyes aplicables, incluidas las Leyes de protección de datos, con respecto a su tratamiento de los Datos personales del Cliente y cualquier instrucción de tratamiento que emita a Clarivate; y (ii) ha proporcionado, y seguirá proporcionando, toda notificación y ha obtenido, y seguirá obteniendo, todos los consentimientos y derechos necesarios en virtud de las Leyes de protección de datos para que Clarivate pueda tratar los Datos personales del Cliente con los fines descritos en el Contrato. El Cliente será el único responsable de la exactitud, calidad y legalidad de los Datos personales del Cliente y de los medios por los que el Cliente adquirió los Datos personales del Cliente.
(e) Legalidad de las instrucciones del Cliente. El Cliente se asegurará de que el tratamiento por parte de Clarivate de los Datos personales del Cliente de conformidad con las instrucciones del Cliente no hará que Clarivate infrinja ninguna ley, reglamento o norma aplicable, incluidas, entre otras, las Leyes de protección de datos. Clarivate informará inmediatamente al Cliente por escrito, a menos que se le prohíba hacerlo en virtud de las Leyes de protección de datos pertinentes, si tiene conocimiento o cree que cualquier instrucción de tratamiento de datos del Cliente infringe el RGPD o alguna aplicación del RGPD en el Reino Unido.

3. Subtratamiento

(a) Subencargados del tratamiento autorizados. El Cliente proporciona a Clarivate una autorización general por escrito para contratar a Subencargados del tratamiento para que traten los Datos personales del Cliente en su nombre con el fin de prestar los Servicios. Clarivate pondrá a disposición del Cliente una lista de los Subencargados del tratamiento pertinentes **aquí** o mediante solicitud por escrito a data.privacy@clarivate.com. La lista incluye a nuestros Subencargados, sus respectivas jurisdicciones de organización y una descripción de sus actividades, junto con la publicación de las sustituciones o adiciones de Subencargados y las instrucciones sobre cómo el Cliente puede suscribirse para recibir notificaciones previas de dichas sustituciones y adiciones. En el momento de la suscripción, Clarivate informará al Cliente de cualquier cambio previsto en relación con dicha adición o sustitución de Subencargados y, si el Cliente se opone a la contratación de un nuevo Subencargado del tratamiento por motivos razonables en un plazo de diez (10) días a partir de dicha notificación, Clarivate hará esfuerzos razonables para realizar un cambio en los Servicios o recomendar un cambio comercialmente razonable para evitar el tratamiento por parte de dicho Subencargado. En el caso de que Clarivate no pueda poner a disposición dicho planteamiento alternativo dentro de un periodo de tiempo razonable, el Cliente podrá rescindir solo los Servicios afectados que no puedan prestarse sin el uso del nuevo subencargado objetado, sin incurrir en penalización ni responsabilidad para

ninguna de las partes, proporcionando una notificación de rescisión por escrito a Clarivate en un plazo de treinta (30) días y el Cliente tendrá derecho a recibir un reembolso de las tarifas prepagadas por el Servicio rescindido de forma prorrateada.

b) Obligaciones del Subencargado del tratamiento. Clarivate deberá: (i) celebrar un acuerdo por escrito con cada Subencargado del tratamiento que contenga obligaciones de protección de datos que proporcionen, como mínimo, el mismo nivel de protección de los Datos personales del Cliente que los recogidos en el presente ATD; y (ii) seguir siendo responsable del cumplimiento de las obligaciones de dicho Subencargado en virtud del presente ATD.

4. Seguridad

(a) Medidas de seguridad. Clarivate implementará y mantendrá las medidas de seguridad técnicas y organizativas apropiadas que están diseñadas para proteger los Datos personales del Cliente contra la Violación de la seguridad de los datos personales y diseñadas para preservar la seguridad y la confidencialidad de los Datos personales del Cliente de acuerdo con las normas de seguridad de Clarivate descritas en el Apéndice B ("Medidas técnicas y organizativas").

(b) Confidencialidad del tratamiento. Clarivate se asegurará de que las personas autorizadas por Clarivate para tratar los Datos personales del Cliente estén debidamente sujetas a la obligación de confidencialidad correspondiente.

(c) Actualizaciones de las medidas de seguridad. El Cliente es responsable de revisar la información puesta a disposición por Clarivate en relación con la seguridad de los datos y de tomar una determinación independiente sobre si el Servicio cumple con los requisitos del Cliente y las obligaciones legales en virtud de las Leyes de protección de datos. El Cliente reconoce que las Medidas de seguridad están sujetas al progreso y desarrollo técnico y que Clarivate puede actualizar o modificar las Medidas de seguridad de vez en cuando, siempre que dichas actualizaciones y modificaciones no supongan la degradación de la seguridad general del Servicio proporcionado al Cliente.

(d) Respuesta a la Violación de la seguridad de los datos personales. Al tener conocimiento de una Violación de la seguridad de los datos personales, Clarivate deberá: (i) informar al Cliente sin demora indebida, y cuando sea factible, y en un plazo no superior a 48 horas tras determinar que se ha producido una Violación de la seguridad de los datos personales; (ii) proporcionar información oportuna relativa a la Violación de la seguridad de los datos personales en cuanto se conozca o cuando el Cliente lo solicite razonablemente; y (iii) tomar rápidamente medidas razonables para contener e investigar cualquier Violación de la seguridad de los datos personales. El Cliente acepta que una Violación de la seguridad de los datos personales que no haya tenido consecuencias no estará sujeta a esta Sección 4 (d). Una Violación de la seguridad de los datos personales infructuosa o sin consecuencias es aquella que no da lugar a un acceso no autorizado a los Datos personales del Cliente o a una instalación o equipo de Clarivate que almacene Datos personales del Cliente. La notificación o la respuesta de Clarivate a una Violación de la seguridad de los datos personales en virtud de esta Sección 4 (d) no se interpretará como un reconocimiento por parte de Clarivate de culpa o responsabilidad alguna con respecto a la Violación de la seguridad de los datos personales.

5. Auditorías

(a) Derechos de auditoría del Cliente. En la medida en que Clarivate cuente con un informe de Controles del sistema y de la organización (SOC, por sus siglas en inglés) 2, un informe de Controles del sistema y de la organización (SOC) 3 o una certificación ISO 27001 realizada por terceros independientes que contemple los Servicios, el Cliente acepta ejercer cualquier derecho que tenga a realizar una auditoría o inspección en virtud de este ATD o de las CCT, en caso de que se apliquen, indicando a Clarivate por escrito que proporcione una copia de su informe o certificación más reciente, que se considerará Información confidencial de Clarivate. En caso de que sean de aplicación las CCT, nada de lo dispuesto en esta sección modifica o afecta a los derechos de la autoridad de control o del interesado en virtud de las CCT. En caso de que Clarivate no proporcione dicho informe o certificación, el Cliente tendrá derecho, a realizar una auditoría, limitada a una vez al año, a menos que se haya producido una Violación de la seguridad de los Datos personales o una reclamación oficial relacionada con nuestras prácticas de privacidad y seguridad.

(b) Notificación y ámbito. Tras un aviso por escrito del Cliente con al menos 30 días de antelación, Clarivate pondrá a disposición del Cliente toda la información que sea necesaria para demostrar el cumplimiento de este ATD y, según lo exigido por las leyes de protección de datos, permitirá y contribuirá a las auditorías, incluidas las inspecciones del Cliente para evaluar el cumplimiento de este ATD. Antes del comienzo de cualquier auditoría, el Cliente y Clarivate deberán acordar mutuamente el alcance, el momento y la duración de la auditoría. El Cliente reembolsará a Clarivate el tiempo invertido por Clarivate o sus Subencargados del tratamiento externos en cualquier auditoría. En el caso de que se solicite una auditoría de nuestros Subencargados, el Cliente reconoce que dicha auditoría puede estar sujeta a condiciones de auditoría adicionales o diferentes. Todas las tarifas de reembolso serán razonables, teniendo en cuenta los recursos gastados por Clarivate o sus Subencargados del tratamiento externos. Las auditorías e inspecciones están sujetas a las políticas razonables de protección de datos de Clarivate, y no incluyen la nómina de los empleados, los registros de personal o cualquier parte de los centros, libros, documentos, registros u otra información de Clarivate que no esté relacionada con los Datos personales del Cliente o que sea comercialmente sensible o legalmente privilegiada. La información obtenida durante una auditoría o inspección, así como los resultados de la misma, se considerarán Información confidencial de Clarivate.

6. Transferencias internacionales

(a) Ubicación de los centros de datos. Con arreglo a las Secciones 6 (b) y 6 (c)y salvo que se acuerde lo contrario por escrito, el Cliente reconoce que Clarivate puede transferir y tratar los Datos personales del Cliente a y en Estados Unidos y a cualquier otro lugar del mundo donde Clarivate, sus Filiales o sus Subencargados del tratamiento realicen operaciones de tratamiento de datos. Como se establece más concretamente a continuación, Clarivate se asegurará de que exista un mecanismo para proporcionar las garantías adecuadas y la aplicación de la protección de datos personales en cumplimiento de los requisitos de las Leyes de protección de datos y de este ATD con respecto a dichas transferencias.

(b) Transferencias australianas. En la medida en que Clarivate sea un receptor de Datos personales del Cliente protegidos por la Ley de privacidad australiana, las partes reconocen y aceptan que Clarivate puede transferir dichos Datos personales del Cliente fuera de Australia según lo permitan los términos acordados por las partes y con sujeción al cumplimiento por parte de Clarivate de este ATD y de la Ley de privacidad australiana.

(c) Transferencias de Datos europeos. En la medida en que Clarivate sea un receptor de Datos personales del Cliente protegidos por las Leyes de protección de datos de la UE ("Datos de la UE") en un país fuera de Europa que no esté reconocido como garante de un nivel adecuado de protección de los datos personales (según lo descrito en la Ley de protección de datos de la UE aplicable), las partes acuerdan respetar y tratar los Datos de la UE de conformidad con las CCT de la UE en la forma establecida en el Apéndice C. A efectos de las descripciones de las CCT de la UE, Clarivate acepta que es el "importador de datos" y el Cliente es el "exportador de datos" (a pesar de que el propio Cliente pueda ser una entidad ubicada fuera de Europa).

(d) Transferencias de datos de Reino Unido. En la medida en que exista una Transferencia internacional de Datos personales del Cliente de Reino Unido en virtud de este ATD y a los efectos del mismo, las partes acuerdan respetar y tratar los Datos personales del Cliente pertinentes de conformidad con el Apéndice del Reino Unido en la forma establecida en el Apéndice D. A los efectos de las descripciones del Anexo del Reino Unido, Clarivate acuerda que es el "Importador" y el Cliente es el "Exportador" (sin perjuicio de que el propio Cliente pueda ser una entidad ubicada fuera del Reino Unido).

(e) Mecanismo de transferencia alternativo. En la medida en que Clarivate adopte un mecanismo alternativo de exportación de datos (incluida cualquier nueva versión o sucesora de las CCT) para la transferencia de Datos de la UE o Datos de Reino Unido no descrito en este ATD ("Mecanismo alternativo de transferencia"), el Mecanismo alternativo de transferencia se aplicará en lugar de los mecanismos de transferencia descritos en este ATD (pero solo en la medida en que dicho Mecanismo alternativo de transferencia cumpla con la Ley de protección de datos aplicable y se extienda a los países a los que se transfieren los datos aplicables). Además, siempre y cuando, y en la medida en que, un tribunal de jurisdicción competente o una autoridad de control ordene (por el motivo que sea) que las medidas descritas en este ATD no pueden ser invocadas para transferir legalmente los Datos de la UE o Datos de Reino Unido (en el sentido de la Ley de protección de datos aplicable), Clarivate podrá aplicar cualquier medida o salvaguarda adicional que pueda ser razonablemente necesaria para permitir la transferencia legal de dichos datos.

7. Devolución o eliminación de datos

Tras la rescisión o el vencimiento de un Servicio y previa solicitud por escrito del Cliente y elección realizada dentro de los 30 días siguientes a dicha rescisión o vencimiento, Clarivate deberá (a elección del Cliente) eliminar o devolver al Cliente todos los Datos personales del Cliente (incluidas las copias) que estén en posesión o control de Clarivate, siempre y cuando dicha devolución pueda dar lugar a cargos adicionales para el Cliente según las tarifas horarias vigentes en ese momento de Clarivate. Dichos cargos deberán ser detallados en un presupuesto independiente y en una declaración de trabajo acordada por ambas partes. Este requisito no se aplicará (i) en la medida en que la ley aplicable exija a Clarivate que conserve algunos o todos los Datos personales del Cliente; o (ii) a los Datos personales del Cliente que Clarivate haya archivado en sistemas de copia de seguridad, que Clarivate aislará y protegerá de forma segura de cualquier tratamiento posterior hasta que se eliminen de acuerdo con las políticas de eliminación de Clarivate.

8. Derechos y cooperación del interesado

(a) Solicitudes de Interesados. Como parte del Servicio, Clarivate proporciona al Cliente varias funciones de autoservicio, que este puede utilizar para recuperar, rectificar, eliminar o restringir el uso de los Datos personales del Cliente, que el Cliente puede utilizar para asistirle en relación con sus obligaciones en virtud de las Leyes de protección de datos con respecto a la respuesta a las solicitudes de los interesados a través de la cuenta del Cliente, sin coste adicional. Además, Clarivate, teniendo en cuenta la naturaleza del tratamiento, proporcionará asistencia razonable al Cliente en la medida de lo posible para permitirle cumplir con sus obligaciones de protección de datos con respecto a los derechos del interesado en virtud de las Leyes de protección de datos aplicables. Si cualquier solicitud de este tipo es presentada directamente a Clarivate, este no responderá directamente a dicha comunicación sin la autorización previa del Cliente, excepto cuando sea razonablemente apropiado (por ejemplo, para indicar al interesado que se ponga en contacto con el Cliente o para dirigir al interesado a un enlace disponible públicamente con información sobre la función de autoservicio o para confirmar la naturaleza de la solicitud y con cuál de nuestros clientes está relacionada) o si lo exige la legislación aplicable. Si Clarivate debe responder a dicha solicitud, lo notificará inmediatamente al Cliente y le proporcionará una copia de la solicitud, a menos que a Clarivate se le prohíba legalmente hacerlo.

(b) Evaluación del impacto de la protección de datos. En la medida en que lo exijan las Leyes de protección de datos aplicables, Clarivate (teniendo en cuenta la naturaleza del tratamiento y la información de que disponga Clarivate) proporcionará toda la información razonablemente solicitada en relación con el Servicio para que el Cliente pueda llevar a cabo evaluaciones de impacto sobre la protección de datos o consultas previas con las autoridades de protección de datos, conforme a lo exigido por las Leyes de protección de datos.

9. Términos específicos de la jurisdicción

En la medida en que Clarivate trate Datos personales del Cliente originados y protegidos por las Leyes de protección de datos en una de las jurisdicciones que figuran en el Apéndice E, se aplicarán los términos especificados en el Apéndice E con respecto a la(s) jurisdicción(es) aplicable(s) ("Términos específicos de la jurisdicción"), además de los términos de este ATD. En caso de conflicto o ambigüedad entre los Términos específicos de la jurisdicción y cualquier otro término de este ATD, prevalecerán los Términos específicos de la jurisdicción aplicables, pero solo en la medida en que los Términos específicos de la jurisdicción sean aplicables a Clarivate.

10. Relación con el Contrato

(a) Vigencia. El presente ATD permanecerá en vigor mientras Clarivate lleve a cabo operaciones de tratamiento de Datos personales del Cliente en nombre del Cliente o hasta la rescisión del Contrato (y todos los Datos personales del Cliente hayan sido devueltos o eliminados de conformidad con la Sección 7 anterior).

(b) Precedencia. Las partes acuerdan que el presente ATD sustituirá a cualquier acuerdo de tratamiento de datos existente o documento similar que las partes puedan haber suscrito previamente en relación con el Servicio. En caso de conflicto o incoherencia entre el presente ATD y el resto del Contrato con respecto al tratamiento de Datos personales del cliente, prevalecerán las disposiciones de los siguientes documentos (en orden de precedencia): (i) las CCT; luego (ii) este ATD; y luego (iii) el resto del Contrato (que se interpretará de acuerdo con cualquier orden de precedencia establecido en el mismo).

(c) Efectos de los cambios. Salvo por los cambios introducidos por el presente ATD, el Contrato permanece invariable y en pleno vigor y efecto.

(d) Derechos de terceros. Nadie que no sea una de las partes de este ATD, sus sucesores y cesionarios permitidos tendrá derecho a hacer valer ninguno de sus términos.

(e) Derecho aplicable. El presente ATD se regirá e interpretará de acuerdo con las disposiciones sobre legislación y jurisdicción vigentes en el Contrato, salvo que las Leyes de protección de datos aplicables exijan lo contrario.

(f) Filiales autorizadas. Las partes reconocen y aceptan que, al suscribir el Contrato, el Cliente suscribe este ATD en su propio nombre y, en su caso, en nombre y representación de sus filiales autorizadas, estableciendo así un ATD independiente entre Clarivate y cada una de dichas filiales autorizadas. Cada Filial autorizada se compromete a cumplir con las obligaciones establecidas en este ATD. El Cliente será responsable de coordinar toda la comunicación con Clarivate en virtud de este ATD y tiene derecho a realizar y recibir cualquier comunicación en relación con este ATD en nombre de sus Filiales autorizadas. Excepto cuando las leyes de protección de datos aplicables requieran que la Filial autorizada ejerza un derecho o pretenda cualquier recurso en virtud de este ATD directamente por sí misma, el Cliente y cada Filial autorizada acuerdan que (i) el Cliente que es la parte contratante del Contrato ejercerá cualquier derecho o pretenderá cualquier recurso en nombre de la Filial autorizada, (ii) el Cliente que es la parte contratante del Acuerdo ejercerá cualquiera de tales derechos o recurrirá a cualquiera de tales recursos en virtud de este ATD de manera combinada para sí mismo y para todas sus Filiales autorizadas en conjunto, y (iii) cualquier referencia a la responsabilidad de una parte significa la responsabilidad conjunta de esa parte y de todas sus Filiales en virtud del Contrato y de este ATD en conjunto. Para evitar dudas, una Filial autorizada no es ni se convierte en parte del Contrato.

Apéndice A: Detalles del tratamiento de datos

Responsable del tratamiento de datos:
El Cliente y/o cualquier Filial autorizada que se califique como responsable del tratamiento según los términos de este ATD.

Encargado del tratamiento de datos:
La entidad de Clarivate y/o su Filial(es) que trate los Datos personales del Cliente conforme a los términos de este ATD.

Objeto:
El objeto del tratamiento de datos en virtud de este ATD son los Datos personales del Cliente.

Duración del tratamiento:
Clarivate tratará los Datos personales del Cliente conforme a lo indicado en las Secciones 7 y 10 (a) de este ATD.

Finalidad y naturaleza del tratamiento:
La finalidad y la naturaleza del tratamiento de los Datos personales del Cliente incluirán: (i) el tratamiento necesario para prestar los Servicios de conformidad con el Contrato; (ii) el cumplimiento de las obligaciones contractuales de Clarivate en virtud del Contrato y del presente ATD; y (iii) el cumplimiento de cualquier otra instrucción razonable proporcionada por el responsable del tratamiento de datos (p. ej., a través del correo electrónico o los tickets de asistencia) que sea coherente con los términos del Contrato y (iv) lo establecido por dicho Servicio aplicable a continuación.

Categorías de interesados:
El responsable del tratamiento puede enviar Datos personales del Cliente a los Servicios, cuyo alcance es determinado y controlado por el responsable del tratamiento a su entera discreción, y que puede incluir, entre otros, Datos personales del Cliente relativos a las categorías de interesados establecidas por el Servicio a continuación.

Categorías de datos personales:
El Responsable del tratamiento puede enviar los Datos personales del cliente a los servicios en consonancia con los fines para los que se prestan los Servicios, cuyo alcance, sujeto a cualquier restricción establecida en el presente documento o en el Contrato, es determinado y controlado por el Responsable del tratamiento a su entera discreción, y que puede incluir, pero no se limita a las categorías de datos personales establecidas por el Servicio a continuación y en la documentación del producto proporcionada.

Servicio	Finalidad y naturaleza	Categorías de interesados	Categorías de datos personales
Converis	Alojamiento, implementación y/o soporte técnico	• Empleados, agentes, asesores y contratistas del responsable del tratamiento • Personas autorizadas por el responsable del tratamiento a utilizar los Servicios • Miembros de la comunidad académica, como revisores científicos externos, editores de revistas participantes • Otros interesados según lo determine el responsable del tratamiento	• Nombre y otros identificadores no sensibles, como el número de identificación del empleado, ID del investigador, nombre de usuario • Datos demográficos • Información de contacto comercial • Información profesional • Otras categorías de datos personales añadidos, generados o almacenados de otra forma en los Servicios según lo permitido por el Contrato
Soluciones de descubrimiento, investigación y flujo de trabajo de la biblioteca: **360 Core** **360 LINK** **360 MARC Updates**	Alojamiento, implementación y/o soporte técnico	• patrocinadores de la biblioteca, personal de la biblioteca, profesores, estudiantes, administradores, empleados, visitantes y antiguos alumnos	• Información básica del usuario y del patrocinador, que incluye ▪ Nombre y apellidos ▪ Direcciones postales ▪ Direcciones de correo electrónico ▪ Números de teléfono y otra información de contacto ▪ Números de identificación institucional ▪ Departamento y función

360 Resource Manager **360 Search** **Intota™ Assessment** **Pivot/Pivot-RP** **RefWorks** **Summon** **Ulrichsweb** **Ulrich's™ Serials Analysis System** **Intota™**			• Información básica y de contacto del personal • Información de uso relacionada con el personal, incluidos los registros de operaciones y actividades del personal • Actividad de investigación • Información general de uso, incluidos datos de conexión (p. ej., direcciones IP) • Información de proveedores
Primero en registrar	Preinscripción de la cuenta de usuario; alojamiento; implementación y/o soporte técnico; y servicios profesionales, según corresponda	• Empleados, agentes, asesores, trabajadores autónomos del responsable del tratamiento (que sean personas físicas) • Personas autorizadas por el responsable del tratamiento a utilizar los Servicios • Clientes potenciales, clientes, socios comerciales y proveedores del responsable del tratamiento (que sean personas físicas) • Empleados o personas de contacto de los clientes potenciales, clientes, socios comerciales y proveedores del responsable del tratamiento • Otros interesados que determine el responsable del tratamiento, incluidos inventores, solicitantes y cesionarios de patentes, propietarios de marcas y abogados	• Nombre y otros identificadores no sensibles, como firmas • Información de contacto comercial • Datos demográficos • Información profesional • Otras categorías de datos personales añadidos, generados o almacenados de otra forma en los Servicios según lo permitido por el Contrato
Sistemas de biblioteca integrados: **Millennium** **Polaris** **Sierra** **Vega** **Virtua** **y módulos asociados**	Alojamiento (a menos que sea alojado por el responsable del tratamiento o por un proveedor de alojamiento externo autorizado), implementación y/o soporte técnico	• Empleados, agentes, asesores, trabajadores autónomos del responsable del tratamiento (que sean personas físicas) • Personas autorizadas por el responsable del tratamiento a utilizar los Servicios, incluidos los patrocinadores de la biblioteca	• Datos de los patrocinadores de la biblioteca, como el número del carné de la biblioteca u otro número de identificación, que puede incluir una imagen del carné de la biblioteca del Interesado, la edad o fecha de nacimiento, información de contacto, prueba de residencia, que puede incluir copias de una tarjeta de identificación emitida por el gobierno u otros documentos que el Interesado haya proporcionado al Cliente • Información sobre el uso de los Servicios; en el caso de los patrocinadores de la biblioteca, esto puede incluir, por ejemplo, el uso de los recursos de la biblioteca (incluidos los lugares o sucursales visitados, el historial de materiales solicitados, retenidos, retirados o accedidos) • Interacciones con el personal de la biblioteca • Uso de otros servicios de la biblioteca; información proporcionada para facilitar cualquier pago; y cualquier cargo o multa por retraso • Nombre y otros identificadores no sensibles, como número de identificación del empleado y nombre de usuario • Información de contacto comercial • Datos demográficos • Información profesional • Otras categorías de datos personales añadidos, generados o almacenados de otra forma en los Servicios según lo permitido por el Contrato

Sistemas de gestión de PI: **FoundationIP** **IPfolio** **Ipendo** **Inprotech** **Memotech** **Patrawin** **Sistema de gestión de PI** **Unycom**	Alojamiento (a menos que sea alojado por el responsable del tratamiento o por un proveedor de alojamiento externo autorizado, como Salesforce), implementación y/o soporte técnico	• Empleados, agentes, asesores, trabajadores autónomos del responsable del tratamiento (que sean personas físicas) • Personas autorizadas por el responsable del tratamiento a utilizar los Servicios • Clientes potenciales, clientes, socios comerciales y proveedores del responsable del tratamiento (que sean personas físicas) • Empleados o personas de contacto de los clientes potenciales, clientes, socios comerciales y proveedores del responsable del tratamiento • Otros interesados que determine el responsable del tratamiento, incluidos inventores, solicitantes y cesionarios de patentes, propietarios de marcas y abogados	• Nombre y otros identificadores no sensibles, como número de identificación del empleado y nombre de usuario • Información de contacto comercial • Datos demográficos • Información profesional • Otras categorías de datos personales añadidos, generados o almacenados de otra forma en los Servicios según lo permitido por el Contrato
Profesional de PI Servicios	Prestación de servicios profesionales relacionados con la PI, incluidos, sin limitación, los servicios de renovación, registro y archivo	• Empleados, agentes, asesores, trabajadores autónomos del responsable del tratamiento (que sean personas físicas) • Personas autorizadas por el responsable del tratamiento a utilizar los Servicios • Clientes potenciales, clientes, socios comerciales y proveedores del responsable del tratamiento (que sean personas físicas) • Empleados o personas de contacto de los clientes potenciales, clientes, socios comerciales y proveedores del responsable del tratamiento • Otros interesados que determine el responsable del tratamiento, incluidos inventores, solicitantes y cesionarios de patentes, propietarios de marcas y abogados	• Nombre y otros identificadores no sensibles, como número de identificación del empleado y nombre de usuario • Información de contacto comercial • Datos demográficos • Información profesional • Otras categorías de datos personales añadidos, generados o almacenados de otra forma en los Servicios según lo permitido por el Contrato
Investigación de mercado: informes de seguridad y calidad exigidos por contrato como parte de un compromiso de investigación de mercado	Notificación al Cliente o al Titular de la autorización de comercialización de los eventos de seguridad y calidad según lo establecido en el Contrato	Participantes en estudios de mercado	• Nombre • Datos demográficos • Información profesional • Información de contacto • Información necesaria para procesar los honorarios
Investigación de mercado: reclutamiento basado en listas para proyectos de investigación de mercado primarios	Tratamiento de la lista proporcionada por el Cliente con el fin de reclutar determinadas personas para un estudio de mercado primario	Posibles participantes en estudios de mercado	• Nombre • Datos demográficos • Información de contacto • Información profesional • Información necesaria para procesar los honorarios
Mi organización (InCites Benchmarking	Permitir al Cliente cargar, analizar y gestionar su base de datos de investigadores en los	• Empleados, agentes, asesores y contratistas del responsable del	• Nombre y otros identificadores no sensibles, como el número de identificación del empleado, ID del investigador, nombre de usuario

and Analytics Module)	módulos Mi organización de Clarivate en InCites	tratamiento (que sean personas físicas) • Personas autorizadas por el responsable del tratamiento a utilizar los Servicios • Otros interesados según lo determine el responsable del tratamiento	• Datos demográficos • Información de contacto comercial • Información profesional • Otras categorías de datos personales añadidas, generadas o almacenadas de otro modo en los Servicios, según lo permitido por el Contrato
Gestión de la biblioteca basada en la nube, descubrimiento, investigación, lista de lectura y aplicación móvil/web (servicios SaaS de Ex Libris): **Alma** **Esploro** **CampusM** **Leganto** **Primo SaaS/Primo VE** **Rapido**	Alojamiento, implantación, soporte técnico y/u otros servicios relacionados	Patrocinadores de la biblioteca, personal de la biblioteca, profesores, estudiantes, administradores, empleados, investigadores, visitantes y antiguos alumnos	• Información básica del usuario y del patrocinador, que incluye ○ Nombre y apellidos ○ Direcciones postales ○ Direcciones de correo electrónico ○ Números de teléfono y otra información de contacto ○ Números de identificación institucional • Información del usuario y del patrocinador relacionada con la biblioteca/catálogo, incluyendo ○ Información sobre la actividad de la biblioteca, préstamos y multas • Información básica del personal, incluida la información de contacto • Información de uso relacionada con el personal, incluidos los registros de operaciones y actividades del personal • Actividad de investigación • Información general de uso, incluidos datos de conexión (p. ej., direcciones IP) • Información de proveedores • Información de la plataforma móvil, si procede ○ Información del dispositivo (p. ej., identificador y plataforma) ○ Datos de asistencia y ubicación, si procede
Servicios de soporte y mantenimiento de software para software Ex Libris instalado localmente, incluidos: **Aleph Local** **Primo Local** **Rosetta Local** **Voyager Local** **SFX**	Prestación de soporte y mantenimiento mediante el acceso remoto a las versiones instaladas localmente de los productos enumerados	Categorías de Interesados seleccionadas por el Cliente y almacenadas en sus sistemas instalados localmente a los que Clarivate puede tener acceso temporal	• Tipos de Datos personales almacenados por el Cliente en los sistemas locales que ejecutan los Programas a los que Clarivate tendrá acceso en relación con la prestación de los Servicios de soporte y mantenimiento del software y/o proporcionados por el Cliente a Clarivate en el curso de la prestación de los Servicios de soporte y mantenimiento del software • El tratamiento es muy limitado e implica principalmente el acceso incidental a los Datos personales durante el acceso remoto activo y temporal a los sistemas para resolver una llamada de servicio de soporte
Reconocimiento de revisores de Web of Science; **Web of Science - Conexión de autor** **Localizador de revisores de Web of Science**	Solo para gestionar listas (proporcionadas por el Cliente) de personas a las que se invitará a inscribirse en el Servicio correspondiente	Miembros de la comunidad académica, como investigadores y revisores científicos externos	• Nombre y otros identificadores no sensibles, como ID del investigador • Datos demográficos • Información de contacto comercial • Información profesional • Otra información asociada a las actividades de revisión científica externa de los interesados

ScholarOne	Alojamiento, soporte técnico y servicios asociados	• Empleados, agentes, asesores y contratistas del responsable del tratamiento (que sean personas físicas) • Miembros de la comunidad académica, como autores de publicaciones y revisores científicos externos • Otros interesados según lo determine el responsable del tratamiento	• Nombre y otros identificadores no sensibles, como el número de identificación del empleado, ID del investigador, nombre de usuario • Datos demográficos • Información de contacto comercial • Información profesional • Otras categorías de datos personales añadidas, generadas o almacenadas de otro modo en los Servicios, según lo permitido por el Contrato

Categorías especiales de Datos personales (según la definición del RGPD) o Datos sensibles:
Clarivate no desea ni pretende recopilar o tratar ninguna Categoría especial de Datos personales en relación con la prestación del Servicio, excepto los detalles relacionados con la salud que se tratan debido a eventos de seguridad y/o calidad notificables requeridos contractualmente como parte de un compromiso de investigación de mercado.

Operaciones de tratamiento:
Los Datos personales del Cliente se tratarán de conformidad con el Contrato (incluido el presente ATD y cualquier Declaración de trabajo o Formulario de pedido) y según sea necesario para prestar, mantener y mejorar los Servicios prestados al Cliente de conformidad con el Contrato y/o según lo exija la legislación aplicable, y pueden estar sujetos a las siguientes operaciones de tratamiento:
Toda operación o conjunto de operaciones, ya sea por procedimientos automatizados o no, como la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, el cotejo o la combinación, la limitación, la supresión o la destrucción.

Frecuencia de la transferencia de Datos personales:
Los Datos personales del Cliente se transferirán al inicio y durante el Plazo cuando sea necesario.

Periodo de conservación:
Los datos se conservarán durante el Plazo y según se indica en la Sección 7 de este ATD.

Las descripciones anteriores también se aplican a las transferencias de Clarivate a los Subencargados del tratamiento.

Apéndice B: Medidas técnicas y organizativas

Las medidas técnicas y organizativas aplicables al Servicio se describen aquí (actualizadas de vez en cuando conforme a la Sección 4 (c) de este ATD).

Programa de seguridad de la información

Clarivate cuenta con un Programa de seguridad de la información bien definido que abarca aspectos relevantes de las medidas técnicas y organizativas alineadas con las normas conocidas de la industria para la seguridad de la información con el fin de proteger la confidencialidad, la integridad y la disponibilidad de los activos de información

Personal

Todo nuestro personal está sujeto a nuestro código de conducta que abarca los valores y la misión de nuestra empresa. Son conscientes de sus responsabilidades, de nuestras políticas y normas, y reciben regularmente orientación y apoyo de nuestro equipo de Seguridad de la información.

Conforme a las leyes y reglamentos pertinentes, se realizan comprobaciones adecuadas de los antecedentes cuando se contrata a una persona física como personal permanente para reducir la posibilidad de que se produzcan amenazas a los activos de información críticos.

Llevamos a cabo una formación obligatoria en materia de seguridad de la información de forma continuada y proporcionamos formación complementaria a grupos objetivo y personas específicas, según sea necesario. Nuestro personal está sujeto a obligaciones de confidencialidad y entiende las consecuencias de no respetar nuestras políticas y sus responsabilidades.

En Clarivate se sigue un proceso de salida de los empleados que implica la revocación de los permisos/derechos de acceso al sistema y la devolución de los activos de la empresa de forma oportuna.

Cifrado de datos personales

Se utilizan medidas, incluido el cifrado, para garantizar que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización durante la transmisión o el transporte electrónicos, y que se puedan establecer y verificar las entidades de destino de cualquier transferencia de datos personales mediante instalaciones de transmisión de datos.

Gestión del acceso de los usuarios

Clarivate dispone de un proceso bien definido para conceder acceso a los activos de información. Hemos establecido medidas para evitar que personas no autorizadas utilicen los equipos de tratamiento de datos, incluyendo la gestión de accesos, los documentos de registro y la protección de contraseñas.

Los privilegios de los usuarios a los equipos de tratamiento de datos se conceden para restringir el acceso a dichos datos personales de acuerdo con sus funciones y responsabilidades para protegerlos contra el acceso y la divulgación no autorizados.

La política de contraseñas de Clarivate está definida de forma generalizada a todos los activos de información, con una longitud mínima, complejidad, caducidad de la contraseña, historial y requisitos de bloqueo de la cuenta en caso de intentos fallidos.

Seguridad de la infraestructura

Nuestros servicios se ofrecen a través de redes públicas y privadas. Las comunicaciones están protegidas contra las escuchas mediante canales seguros y cifrado. Clarivate ha asegurado su perímetro con sistemas de prevención de intrusiones (IPS), cortafuegos y/o grupos de seguridad para que AWS gestione y restrinja el acceso a la red, y VLANS en nuestro centro de datos.

Hay controles por niveles, incluido el uso de segmentación de la red, designados para garantizar el nivel adecuado de protección de los sistemas y los datos.

Protección contra malware

En consonancia con nuestras políticas, los sistemas operativos propiedad de Clarivate y compatibles que se alojan en nuestros centros de datos o se despliegan en la nube están protegidos con una solución antivirus de última generación.

Gestión de parches

Recogemos y revisamos la información sobre las amenazas a la seguridad a partir de nuestras herramientas internas de gestión de vulnerabilidades, de los proveedores y de otras organizaciones de seguridad externas. Nuestro estándar de gestión de parches proporciona prácticas de parcheo adecuadas a nuestros equipos tecnológicos. Nuestra aplicación de parches de seguridad comienza con la evaluación y definición de la gravedad del parche. Se emplea una certificación prioritaria y una prueba de control

de calidad completa para validar la estabilidad y la disponibilidad de los sistemas después de los parches. A veces, se pueden establecer controles de seguridad adicionales para mitigar las amenazas conocidas.

Supervisión de la seguridad

Clarivate cuenta con un Centro de operaciones de red y seguridad (NOC/SOC) dedicado que proporciona registro y supervisión permanente para el acceso lógico de la red a los datos del Cliente y el uso de los activos de información. Los registros de seguridad se envían a nuestro SOC (Centro de operaciones de seguridad) con el fin de conocer en tiempo real, correlacionar eventos y responder a incidentes. También se registra la entrada de datos, para garantizar que es posible comprobar y determinar si los datos personales se han introducido, alterado o eliminado de los sistemas de tratamiento de datos personales y, en caso afirmativo, por quién.

Respuesta ante incidentes de seguridad y privacidad

Existe un proceso de respuesta ante incidentes para tratarlos a medida que se identifican. Los incidentes son gestionados por un equipo de respuesta ante incidentes que sigue un procedimiento documentado de mitigación y comunicación.

El proceso de Respuesta ante incidentes de Clarivate requiere que los incidentes sean efectivamente comunicados, investigados y vigilados para asegurarse de que se tomen acciones correctivas de cara a controlar y corregir los incidentes de seguridad de manera oportuna.

Seguridad de las operaciones

Los cambios en el entorno de los sistemas de información operativos, incluidos los cambios en servidores, equipos de red y software, están sujetos a un proceso formal de gestión de cambios.

Las copias de seguridad de la información y el software se mantienen de forma segura con el fin de recuperar los datos en caso de eventos como la caída del sistema o el borrado accidental de la información.

Gestión y control de la capacidad

El control de los sistemas, los servicios y las operaciones se lleva a cabo para mantener el buen estado de nuestros entornos operativos. Se han implantado herramientas de gestión para supervisar y mantener un entorno adecuadamente escalonado.

Exploración de vulnerabilidades

Clarivate ha implantado un programa de gestión de la vulnerabilidad de la seguridad de varios niveles que incluye comprobaciones de seguridad y revisiones de seguridad automatizadas o manuales, escaneos de evaluación de la vulnerabilidad de las aplicaciones e infraestructuras. Existen medidas para evaluar, validar, priorizar y corregir los problemas identificados.

Los sitios orientados a Internet de nuestra red mundial se exploran periódicamente como práctica de nuestro programa centrado en la gestión de vulnerabilidades.

Gestión de riesgos

Nuestros equipos de productos y tecnología contratan regularmente a expertos en seguridad de la información para que presten servicios de evaluación de riesgos. Las revisiones de arquitectura, los exámenes de vulnerabilidad, las pruebas de seguridad de las aplicaciones y las revisiones de cumplimiento técnico son algunos de los servicios que se realizan durante las actividades de evaluación de riesgos.

Tras las actividades de evaluación de riesgos, nuestro equipo de Gestión de riesgos de la seguridad de la información consulta a los equipos de productos y tecnología para desarrollar planes de corrección y hojas de ruta que aborden las lagunas de cumplimiento o las áreas de riesgo identificadas.

Además, nuestro equipo de Gestión, riesgo y cumplimiento de TI realiza auditorías con respecto a las políticas, normas y disposiciones reglamentarias, y registra las conclusiones para que se revisen y se pongan en marcha iniciativas de corrección dentro de la empresa.

Seguridad física y gestión de proveedores externos

Todos los centros de datos estratégicos, incluidos los proveedores de servicios en la nube que alojan los productos de Clarivate, se implementan y gestionan de acuerdo con las normas de seguridad física del sector que Clarivate ha adoptado. Nuestras directrices incluyen requisitos de seguridad física, mantenimiento del edificio, extinción de incendios, aire acondicionado, SAI con generador de reserva y acceso a diversas fuentes de energía y comunicaciones. Clarivate revisa los informes de garantía de los centros de datos de terceros como parte de nuestro programa de gestión de riesgos de proveedores.

Se utiliza una serie de métodos de seguridad para controlar el acceso a nuestras instalaciones, con el fin de garantizar que el acceso solo se realice de forma controlada en función de las necesidades operativas. Dependiendo de la sensibilidad de la instalación, estos métodos pueden incluir algunos o todos los siguientes: el uso de un dispositivo de alarma o servicio de seguridad fuera de los horarios de servicio, la división de los locales en diferentes zonas de seguridad, de personal de seguridad,

tarjetas de identificación, control de acceso electrónico que incorpora lectores de tarjetas de proximidad, cerraduras físicas y códigos PIN.

Apéndice C: Cláusulas contractuales tipo de la UE (Encargado del tratamiento)

Responsable del tratamiento a Encargado del tratamiento

SECCIÓN I

Cláusula 1

Finalidad y ámbito de aplicación

(a) La finalidad de estas cláusulas contractuales tipo es garantizar el cumplimiento de los requisitos del 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 (Reglamento general de protección de datos), exige para la transferencia de datos 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, enumerados en el Anexo I.A (cada uno denominado 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, directa 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 acordado 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 mencionados en estas, forma parte del pliego de cláusulas.

Cláusula 2

Invariabilidad del pliego de cláusulas

(a) El presente pliego de cláusulas establece las 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, 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 importador de datos y exigirles su cumplimiento, con las excepciones siguientes:

(i) Cláusulas 1, 2, 3, 6 y 7.

(ii) Cláusula 8: cláusula 8.1, letra (b), y cláusula 8.9, letras (a), (c), (d) y (e).

(iii) Cláusula 9: cláusula 9, letras (a), (c), (d) y (e).

(iv) Cláusula 12: 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: 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.

Cláusula 7 (opcional)
[Omitido intencionadamente].
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 periodo 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 el fin o los fines específicos de la transferencia indicados en el anexo I.B, salvo cuando 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 periodo 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, en la letra (e), 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 o 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 (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) la transferencia ulterior es necesaria para proteger intereses vitales del interesado o de otra persona física.

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 15 días de antelación, siempre que sea comercialmente razonable hacerlo, pero con no menos de 5 días de antelación en todos los casos, 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. 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.

(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 conjunta y solidariamente y el interesado tendrá derecho a interponer una acción judicial contra cualquiera de estas partes.

(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) Cuando el exportador de datos esté establecido en un Estado miembro de la UE, 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.

Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, y haya nombrado a un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679, la autoridad de control del Estado miembro en que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, indicada en el anexo I.C, actuará como autoridad de control competente.

Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679 de la Comisión, de conformidad con el artículo 3, apartado 2, y no haya nombrado a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679 de la Comisión, la autoridad de control de uno de los Estado miembros en que estén situados los interesados cuyos datos personales se transfieran en virtud del presente pliego de cláusulas en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado, 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;

(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. El exportador de datos suspenderá la transferencia de los datos si considera que no hay garantías adecuadas o si así lo dispone 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 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 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) Ninguna 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

En caso de que el Derecho aplicable del Contrato (tal como se define en la ATD) sea la de un Estado miembro de la UE, el presente pliego de cláusulas se regirá por el Derecho de dicho Estado miembro de la UE, siempre que dicho Derecho admita la existencia de derechos de los terceros beneficiarios. Si dicho Derecho no admite la existencia de derechos de los terceros beneficiarios, o si el Derecho aplicable del Contrato no es el de un Estado miembro de la UE, se regirá por el Derecho de otro Estado miembro de la UE que sí admita la existencia de derechos de los terceros beneficiarios. Las partes acuerdan que este será 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 del Estado miembro de la UE que se establecen en la cláusula 17.

(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 1 A LAS CLÁUSULAS CONTRACTUALES TIPO DE LA UE

A. LISTA DE PARTES

Exportador(es) de datos:
El Cliente y/o las Filiales autorizadas que transfieren los Datos personales del Cliente en virtud de los términos de la Adenda de tratamiento de datos ("ATD") a la que se adjunta el presente pliego de cláusulas.

Importador(es) de datos:
La entidad Clarivate, que actúa como importador de datos por cuenta suya en por cuenta de sus Filiales cuando proceda, que acepta recibir del Exportador de d*at*os los Datos personales del Cliente en virtud de los términos de la ATD a la que se adjunta el presente pliego de cláusulas.

B. DESCRIPCIÓN DE LA TRANSFERENCIA
Consulte los detalles expuestos en el apéndice A de la ATD a la que se adjunta el presente pliego de cláusulas.

C. AUTORIDAD DE CONTROL COMPETENTE
La autoridad de control competente será la autoridad de control del exportador de datos, tal y como exige la cláusula 13.

ANEXO 2 A LAS CLÁUSULAS CONTRACTUALES TIPO DE LA UE

MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

Según lo establecido en el apéndice B de la ATD.

ANEXO 3 A LAS CLÁUSULAS CONTRACTUALES TIPO DE LA UE

Las partes reconocen que la cláusula 2, letra (a) del pliego de cláusulas les permite incluir términos adicionales relacionados con el negocio siempre que no contradigan, directa o indirectamente, el pliego de cláusulas ni perjudiquen los derechos o libertades fundamentales de los interesados.

En consecuencia, este anexo establece la interpretación de las partes de sus respectivas obligaciones en virtud del pliego de cláusulas específicas identificadas a continuación. Cuando una parte cumpla con las interpretaciones establecidas en este anexo, la otra parte considerará que ha cumplido sus compromisos en virtud del pliego de cláusulas.

Cláusula 3 y cláusula 8, apartado 6, letra (d): Comunicación de este pliego de cláusulas

El exportador de datos acepta que el presente pliego de cláusulas constituye Información confidencial del importador de datos (tal y como se define este término en el Contrato) y no puede comunicarse por el exportador de datos a ningún tercero sin el previo consentimiento por escrito del importador de datos, a menos que se permita en virtud del Contrato. Esto no impedirá la comunicación del presente pliego de cláusulas a un interesado en virtud de la cláusula 3 o a una autoridad de control en virtud de la cláusula 8, apartado 6, letra (d).

Cláusula 8, apartado 1, letras (a) y (b): Suspensión de las transferencias de datos y terminación

1. Las partes reconocen que, a los efectos de la cláusula 8, apartado 1, letra (a), el importador de datos podrá tratar los datos personales únicamente por cuenta del exportador de datos y en cumplimiento de sus instrucciones documentadas, tal como se establece en la ATD, y que en virtud de la misma, estas instrucciones serán las instrucciones completas y definitivas del exportador de datos, y el tratamiento fuera del ámbito de dichas instrucciones (en su caso) se establecerá por escrito entre las partes.
2. Las partes reconocen que, si el importador de datos no puede garantizar el cumplimiento de la cláusula 8, apartado 1, letra (a) y/o la cláusula 8, apartado 1, letra (b), el importador de datos se compromete a informar inmediatamente al exportador de datos de su incapacidad de cumplimiento, en cuyo caso el exportador de datos tendrá derecho a suspender la transferencia de datos y/o a terminar las partes afectadas del Servicio de conformidad con los términos del Contrato.
3. Si el exportador de datos tiene la intención de suspender la transferencia de datos personales y/o terminar las partes afectadas del Servicio, deberá notificarlo primero al importador de datos y concederle un período de tiempo razonable para que pueda subsanar el incumplimiento («Período de subsanación»).
4. Además, el exportador de datos y el importador de datos cooperarán razonablemente entre sí durante el Período de subsanación para acordar qué salvaguardias adicionales u otras medidas, en su caso, pueden ser razonablemente necesarias para garantizar el cumplimiento del pliego de cláusulas por parte del importador de datos y de la legislación aplicable en materia de protección de datos.
5. Si, una vez transcurrido el Período de subsanación, el importador de datos no ha subsanado o no puede subsanar el incumplimiento de conformidad con los apartados 3 y 4 anteriores, el exportador de datos podrá suspender y/o terminar la parte afectada del Servicio de conformidad con las disposiciones del Contrato, sin responsabilidad para ninguna de las partes (pero sin perjuicio de los gastos en que haya incurrido el exportador de datos antes de la suspensión o la terminación).

Cláusula 8, apartado 9: Auditoría

El exportador de datos reconoce y acepta que ejerce su derecho de auditoría en virtud de la cláusula 8, apartado 9 dando instrucciones al importador de datos para que cumpla con las medidas de auditoría descritas en la cláusula 5 (Auditorí(a) de la ATD.

Cláusula 9, letra (c): Comunicación de contratos con subencargados del tratamiento

1. Las partes reconocen la obligación del importador de datos de enviar sin demora al exportador de datos una copia de cualquier contrato con un subencargado del tratamiento que celebre en virtud del pliego de cláusulas.
2. Las partes reconocen además que, en virtud de las restricciones de confidencialidad de los subencargados del tratamiento, el importador de datos puede tener restringida la comunicación al exportador de datos de los contratos con un subencargado. Sin perjuicio de ello, el importador de datos hará los esfuerzos razonables para exigir a cualquier subencargado del tratamiento que designe que le permita comunicar el contrato con dicho subencargado al exportador de datos.
3. Incluso cuando el importador de datos no pueda comunicar un acuerdo de subencargado del tratamiento al exportador de datos, las partes acuerdan que, a petición del exportador de datos, el importador de datos proporcionará al exportador de datos (de forma confidencial) toda la información que pueda, dentro de lo razonable, en relación con dicho contrato con el subencargado del tratamiento.

Cláusula 12: Responsabilidad

En la medida permitida, cualquier reclamación presentada en virtud del pliego de cláusulas estará sujeta a los términos y condiciones, incluidas, entre otras, las exclusiones y limitaciones establecidas en el Contrato. En ningún caso ninguna de las partes limitará su responsabilidad con respecto a los derechos de los interesados en virtud del presente pliego de cláusulas.

Apéndice D - Anexo del Reino Unido

De conformidad con la legislación aplicable en materia de protección de datos, incluido el RGPD del Reino Unido, Clarivate (en adelante, el "Importador") y el Cliente (en adelante, el "Exportador"), cada uno de ellos una "parte"; conjuntamente, "las partes", HAN ACORDADO el siguiente Anexo con el fin de aportar las garantías adecuadas con respecto a la protección de la privacidad y los derechos y libertades fundamentales de las personas para la transferencia por parte del Exportador al Importador de los datos personales especificados en el Anexo 1.

Parte 1: Tablas

Tabla 1: Partes

Fecha de inicio	La fecha en que ambas partes firman el Contrato.	
Las Partes	**Exportador (que envía la Transferencia restringid(a)**	**Importador (quien recibe la Transferencia restringid(a)**
Datos de las partes	Según se describe en el Contrato.	Según se describe en el Contrato.
Contacto clave	Según se describe en el Anexo 1 de las CCT de la UE adjuntas.	Según se describe en el Anexo 1 de las CCT de la UE adjuntas.
Firma (si se requiere a efectos de la Sección 2)	N/A	N/A

Tabla 2: CCT seleccionados, módulos y cláusulas seleccionadas

Anexo de las CCT de la UE	☒ La versión de las CCT de la UE aprobadas a la que se adjunta este Anexo, que se detalla a continuación, incluye la Información del Apéndice: Fecha: En vigor a partir de la fecha de la firma de ambas partes a continuación (Módulo 2: Cláusulas contractuales tipo para la transferencia de datos personales a terceros países: del responsable al encargado del tratamiento)

Tabla 3: Información del Apéndice

"**Información del Apéndice**" se refiere a la información que debe proporcionarse para los módulos seleccionados según lo establecido en el Apéndice de las CCT de la UE aprobadas (distintas de las Partes), y que para este Anexo se establece en:

Anexo 1A: Lista de Partes: Consulte el Anexo I de las CCT de la UE adjuntas.
Anexo 1B: Descripción de la transferencia: Consulte el Anexo I de las CCT de la UE adjuntas.
Anexo II: Medidas técnicas y organizativas, incluidas las medidas técnicas y organizativas para garantizar la seguridad de los datos: Consulte el Anexo 2 de las CCT de la UE adjuntas.
Anexo III: Lista de subencargados del tratamiento (solo Módulos 2 y 3): Este Anexo III no es aplicable porque no se ha seleccionado la Opción 1 de la cláusula 9 (a) (autorización especifica de los subencargados) del Anexo adjunto de las CCT de la UE.

Tabla 4: Finalización de este Anexo cuando cambie el Anexo aprobado

Finalización de este Anexo cuando cambia el Anexo aprobado	¿Qué Partes pueden finalizar este Anexo según se establece en la Sección 19? ☒ Importador ☒ Exportador ☐ Ninguna de las partes

Parte 2: Cláusulas obligatorias

Firma de este Anexo

1. Cada una de las Partes acepta quedar sujeta a los términos y condiciones establecidos en este Anexo, a cambio de que la otra Parte también acepte quedar sujeta a este Anexo.
2. Aunque el Anexo 1A y la cláusula 7 de las CCT de la UE aprobadas requieren la firma de las Partes, a efectos de realizar transferencias restringidas, las Partes pueden suscribir el presente Anexo de cualquier forma que las haga jurídicamente vinculantes para las Partes y que permita a los interesados ejercer sus derechos según lo establecido en el presente Anexo. La suscripción de este Anexo tendrá el mismo efecto que la firma de las CCT de la UE aprobadas y de cualquier parte de las CCT aprobadas.

Interpretación de este Anexo

3. En los casos en que este Anexo utilice términos que se definen en las CCT de la UE aprobadas, dichos términos tendrán el mismo significado que en las CCT de la UE aprobadas. Además, los siguientes términos tienen los siguientes significados:

Anexo	El presente Anexo de transferencia internacional de datos que se compone de este Anexo que incorpora las CCT de la UE.
Anexo de las CCT de la UE	La(s) versión(es) de las CCT de la UE aprobadas a las que se adjunta el presente Anexo, tal como se indica en la Tabla 2, incluida la Información del Apéndice.

Información del Apéndice	Según lo establecido en la Tabla 3.
Garantías adecuadas	El nivel de protección de los datos personales y de los derechos de los interesados que exige la Ley de protección de datos del Reino Unido cuando realiza una Transferencia restringida apoyándose en las cláusulas tipo de protección de datos según el artículo 46 2) (d) del RGPD del Reino Unido.
Anexo aprobado	El modelo de Anexo emitido por la ICO y presentado al Parlamento de conformidad con el artículo 119A de la Ley de protección de datos de 2018 el 2 de febrero de 2022, ya que se revisa en virtud de la Sección 18.
CCT de la UE aprobadas	Las Cláusulas contractuales tipo establecidas en el Anexo de la Decisión de Ejecución de la Comisión (UE) 2021/914 de 4 de junio de 2021.
ICO	El Comisionado de información.
Transferencia restringida	Una transferencia que está contemplada en el Capítulo V del RGPD del Reino Unido.
REINO UNIDO	El Reino Unido de Gran Bretaña e Irlanda del Norte.
Leyes de protección de datos del Reino Unido	Todas las leyes relacionadas con la protección de datos, el tratamiento de datos personales, la privacidad y/o las comunicaciones electrónicas vigentes en cada momento en el Reino Unido, incluyendo el RGPD del Reino Unido y la Ley de Protección de Datos de 2018.
RGPD DEL REINO UNIDO	Según se define en la sección 3 de la Ley de protección de datos de 2018.

4. El presente Anexo debe interpretarse siempre de forma coherente con la Ley de Protección de Datos del Reino Unido y de forma que cumpla con la obligación de las Partes de proporcionar las Garantías apropiadas.
5. Si las disposiciones incluidas en el Anexo CCT de la UE modifican las CCT aprobadas de alguna manera que no esté permitida por las CCT de la UE aprobadas o por el Anexo aprobado, dicha(s) enmienda(s) no se incorporará(n) a este Anexo y su lugar será ocupado por la disposición equivalente de las CCT de la UE aprobadas.
6. Si existe alguna incoherencia o conflicto entre las Leyes de protección de datos del Reino Unido y este Anexo, se aplicarán las Leyes de protección de datos del Reino Unido.
7. Si no está claro el significado de este Anexo o hay más de un significado, se aplicará el que más se ajuste a las Leyes de protección de datos del Reino Unido.
8. Cualquier referencia a la legislación (o a disposiciones específicas de la legislación) implica esa legislación (o disposición específic(a) en la forma que pueda evolucionar con el tiempo. Esto incluye los casos en los que esa legislación (o disposición específic(a) se haya consolidado, vuelto a promulgar y/o sustituido después de la celebración de este Anexo.

Jerarquía

9. Aunque la cláusula 5 de las CCT de la UE aprobadas establece que las CCT de la UE aprobadas prevalecen sobre todos los acuerdos relacionados entre las partes, estas acuerdan que, para las Transferencias restringidas, prevalecerá la jerarquía de la Sección 10.
10. Cuando exista alguna incoherencia o conflicto entre el Anexo aprobado y las CCT de la UE (según proced(a), el Anexo aprobado prevalecerá sobre las CCT de la UE, excepto cuando (y en la medida en que) las condiciones incoherentes o

conflictivas de las CCT de la UE proporcionen una mayor protección a los interesados, en cuyo caso dichas condiciones prevalecerán sobre el Anexo aprobado.

11. Cuando este Anexo incorpore las CCT de la UE del Anexo que se hayan celebrado para proteger las transferencias sujetas al Reglamento General de Protección de Datos (UE) 2016/679, las Partes reconocen que nada de lo dispuesto en este Anexo afecta a dichas CCT de la UE del Anexo.

Incorporación y cambios en las CCT de la UE

12. El presente Anexo incorpora las CCT de la UE que se enmiendan en la medida necesaria para que:
    a. funcionen conjuntamente para las transferencias de datos realizadas por el exportador de datos al importador de datos, en la medida en que las leyes de protección de datos del Reino Unido se apliquen al tratamiento del exportador de datos al realizar esa transferencia de datos, y ofrezcan garantías adecuadas para esas transferencias de datos;
    b. las Secciones 9 a 11 anulan la cláusula 5 (Jerarquí(a) del Anexo CCT de la UE; y
    c. este Anexo (incluyendo las CCT de la UE incorporadas al mismo) está 1) regido por las leyes de Inglaterra y Gales y 2) cualquier disputa que surja del mismo será resuelta por los tribunales de Inglaterra y Gales, en cada caso a menos que las leyes y/o los tribunales de Escocia o Irlanda del Norte hayan sido expresamente seleccionados por las Partes.
13. A menos que las Partes hayan acordado enmiendas alternativas que cumplan con los requisitos de la Sección 12, se aplicarán las disposiciones de la Sección 15.
14. No se podrán hacer enmiendas a las CCT de la UE aprobadas aparte de las necesarias para cumplir los requisitos de la Sección 12.
15. Se introducen las siguientes enmiendas en el Anexo CCT de la UE (a efectos de la Sección 12):
    a. Las referencias a las “Cláusulas” se refieren a este Anexo, que incorpora las CCT de la UE;
    b. En la cláusula 2, suprimir las palabras:
       “y, con respecto a las transferencias de datos de responsables a encargados y/o encargados a encargados, cláusulas contractuales tipo de conformidad con el Artículo 28 7), del Reglamento (UE) 2016/679”;
    c. La cláusula 6 (Descripción de la(s) transferencia(s)) se sustituye por:
       “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, cuando las Leyes de protección de datos del Reino Unido se aplican al tratamiento del exportador de datos al realizar dicha transferencia”;
    d. La cláusula 8.7 (i) del Módulo 1 se sustituye por:
       “es a un país que se beneficia de la normativa de adecuación de conformidad con la Sección 17A del RGPD del Reino Unido que contempla la transferencia ulterior”;
    e. La cláusula 8.8 (i) de los Módulos 2 y 3 se sustituye por:
       “la transferencia ulterior va dirigida a un país sobre el que ha recaído una normativa de adecuación de conformidad, con arreglo a la Sección 17A del RGPD del Reino Unido, que abarca la transferencia ulterior;”
    f. Las referencias al “Reglamento (UE) 2016/679”, al “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 (Reglamento General de Protección de Datos)” y a “dicho Reglamento” se sustituyen por “Leyes de protección de datos del Reino Unido”. Las referencias a uno o varios artículos específicos del “Reglamento (UE) 2016/679” se sustituyen por el Artículo o Sección equivalente de las Leyes de protección de datos del Reino Unido;
    g. Se eliminan las referencias al Reglamento (UE) 2018/1725;
    h. Las referencias a la “Unión Europea”, “Unión”, “UE”, “Estado miembro de la UE”, “Estado miembro” y “UE o Estado miembro” se sustituyen por el “Reino Unido”;
    i. La referencia a la “cláusula 12 (c) (i)” en la cláusula 10 (b) (i) del Módulo uno, se sustituye por la “cláusula 11 (c) (i)”;
    j. No se utilizan la cláusula 13 (a) ni la Parte C del Anexo I;
    k. La “autoridad de control competente” y la “autoridad de control” se sustituyen por el “Comisionado de información”;
    l. En la cláusula 16 (e), el apartado (i) se sustituye por:
       “el Secretario de Estado dicta reglamentos de conformidad con la Sección 17A de la Ley de Protección de Datos de 2018 que contemplan la transferencia de datos personales a los que se aplican estas cláusulas”;
    m. La cláusula 17 se sustituye por:
       “Estas cláusulas se rigen por las leyes de Inglaterra y Gales”;
    n. La cláusula 18 se sustituye por:
       “Cualquier controversia derivada del presente pliego de cláusulas será resuelta judicialmente por los tribunales de Inglaterra y Gales. Los interesados también podrán ejercer acciones judiciales contra el exportador de datos y/o el

importador de datos ante los tribunales de cualquier país del Reino Unido. Las partes acuerdan someterse a la jurisdicción de dicho Estado miembro".; y

o. Las notas a pie de página de las CCT de la UE aprobadas no forman parte del Anexo, excepto las notas a pie de página 8, 9, 10 y 11.

Enmiendas a este Anexo

16. Las Partes podrán acordar modificar las cláusulas 17 y/o 18 del Anexo CCT de la UE para referirse a las leyes y/o tribunales de Escocia o Irlanda del Norte.
17. Si las Partes desean cambiar el formato de la información incluida en la Parte 1: Tablas del Anexo aprobado, podrán hacerlo aceptando el cambio por escrito, siempre que este no reduzca las Garantías apropiadas.
18. Ocasionalmente, el ICO podrá emitir un Anexo aprobado revisado que:
    a. introduzca cambios razonables y proporcionados en el Anexo aprobado, incluida la corrección de errores en el mismo; y/o
    b. refleje los cambios en las Leyes de protección de datos del Reino Unido;

    El Anexo aprobado revisado especificará la fecha de inicio a partir de la cual los cambios del Anexo aprobado son efectivos y si las Partes necesitan revisar este Anexo, incluyendo la Información del Apéndice. Este Anexo se enmienda automáticamente según lo establecido en el Anexo Aprobado revisado a partir de la fecha de inicio especificada.
19. Si el ICO emite un Anexo aprobado revisado en virtud de la Sección 18, si alguna de las Partes seleccionadas en la Tabla 4 "Finalización del Anexo cuando el Anexo aprobado cambia", como resultado directo de los cambios en el Anexo aprobado tendrá un aumento sustancial, desproporcionado y demostrable en:
    a. sus costes directos de cumplimiento de sus obligaciones en virtud del Anexo; y/o
    b. su riesgo en virtud del Anexo,

    y en cualquiera de los dos casos ha tomado primero medidas razonables para reducir esos costes o riesgos de manera que no sean sustanciales y desproporcionados, esa Parte podrá poner fin a este Anexo al final de un período de notificación razonable, notificando por escrito ese período a la otra Parte antes de la fecha de inicio del Anexo aprobado revisado.
20. Las Partes no necesitan el consentimiento de ningún tercero para realizar cambios en este Anexo, pero cualquier cambio debe realizarse de acuerdo con sus condiciones.

Apéndice E - Condiciones específicas de la jurisdicción

Europa y Reino Unido:

(a) Objeción a los Subencargados del tratamiento. El Cliente podrá oponerse por escrito a la designación por parte de Clarivate de un nuevo Subencargado del tratamiento en un plazo de diez (10) días naturales a partir de la recepción de la notificación, de conformidad con la Sección 3 (a) del ATD, siempre que dicha objeción se base en motivos razonables relacionados con la protección de datos. En dicho caso, las partes examinarán de buena fe dichas preocupaciones con el fin de alcanzar una resolución comercialmente razonable. Si no se puede llegar a dicha resolución, Clarivate, a su entera discreción, se abstendrá de nombrar a dicho Subencargado del tratamiento, o bien permitirá al Cliente suspender o rescindir el Servicio afectado de conformidad con las disposiciones de rescisión del Contrato, sin responsabilidad para ninguna de las partes (pero sin perjuicio de los gastos incurridos por el Cliente antes de la suspensión o rescisión).

(b) Solicitudes públicas de acceso a datos. Como práctica general, Clarivate no proporciona voluntariamente a los organismos o autoridades públicas (incluidas las fuerzas del orden) Datos personales del Cliente. Si Clarivate recibe un requerimiento obligatorio (ya sea a través de una citación, una orden judicial, una orden de registro u otro proceso legal válido) de cualquier agencia o autoridad pública (incluidas las fuerzas del orden) para acceder a los Datos personales del Cliente pertenecientes a un interesado cuya información de contacto principal indica que el interesado se encuentra en Europa o el Reino Unido, Clarivate deberá: (i) informar al organismo público de que Clarivate es un encargado del tratamiento de los datos; (ii) intentar redirigir al organismo para que solicite los datos directamente al Cliente; y (iii) informar al Cliente a través de un correo electrónico enviado a la dirección de correo electrónico de contacto principal del Cliente sobre la solicitud para permitir que el Cliente solicite una orden de protección u otra solución adecuada. Como parte de dicha iniciativa, Clarivate puede proporcionar la información de contacto principal y de facturación del Cliente a la autoridad pertinente. Clarivate no estará obligada a cumplir con este apartado (b) si se le prohíbe legalmente hacerlo, o si cree razonablemente y de buena fe que el acceso urgente es necesario para prevenir un riesgo inminente de daño grave a cualquier persona, a la seguridad pública o a Clarivate.

California:

(a) Definiciones. Salvo que se describa lo contrario, las definiciones de: “responsable del tratamiento” incluye “Empresa”; “encargado del tratamiento” incluye “Proveedor de servicios”; “interesado” incluye “Consumidor”; “datos personales” incluye “Información personal”; en cada caso según se define en la CCPA. Solo para esta sección “California” del Anexo D, “Fines permitidos” incluirá el tratamiento de los Datos personales del Cliente solo para los fines descritos en este ATD y de acuerdo con las instrucciones legales documentadas del Cliente, tal y como se establece en este ATD, según sea necesario para cumplir con la legislación aplicable, según se acuerde por escrito, incluyendo, entre otros, en el Contrato, o según se permita de otro modo para los “proveedores de servicios” en virtud de la CCPA.

(b) Derechos del Consumidor. Las obligaciones de Clarivate en relación con las solicitudes de los interesados, tal como se describen en la Sección 8 (Derechos y cooperación del interesado) de este ATD, se aplican a los derechos del consumidor en virtud de la CCPA.

(c) Finalidad permitida. Sin perjuicio de cualquier restricción de uso contenida en otra parte de este ATD, Clarivate tratará los Datos personales del Cliente únicamente para prestar los Servicios, para los Fines permitidos y/o de acuerdo con las instrucciones legales documentadas del Cliente, excepto cuando la legislación aplicable exija lo contrario. Clarivate puede anonimizar o agrupar los Datos personales del Cliente como parte de la prestación del Servicio especificado en este ATD y en el Contrato.

(d) Subencargados del tratamiento. Cuando los Subencargados del tratamiento tratan los datos personales de los contactos del Cliente, Clarivate toma medidas para asegurarse de que dichos Subencargados del tratamiento son Proveedores de servicios en virtud de la CCPA con los que Clarivate ha celebrado un contrato escrito que incluya términos sustancialmente similares a los de este ATD o están exentos de otro modo de la definición de “venta” de la CCPA. Clarivate lleva a cabo la debida diligencia sobre sus Subencargados del tratamiento. Cuando los Subencargados del tratamiento tratan los datos personales de los contactos del Cliente, Clarivate toma medidas para asegurarse de que dichos Subencargados del tratamiento son Proveedores de servicios en virtud de la CCPA con los que Clarivate ha celebrado un contrato escrito que incluya términos sustancialmente similares a los de este ATD o están exentos de otro modo de la definición de “venta” de la CCPA. Clarivate lleva a cabo la debida diligencia sobre sus Subencargados del tratamiento.

Canadá:

(a) Subencargados del tratamiento de datos. Clarivate toma medidas para garantizar que los Subencargados del tratamiento de Clarivate, tal y como se describe en la Sección 3 (Subtratamiento) del ATD, son terceros en virtud de la LPRPDE, con los que Clarivate ha firmado un contrato por escrito que incluya términos sustancialmente similares a este ATD. Clarivate lleva a cabo la debida diligencia sobre sus Subencargados del tratamiento.

(b) Seguridad. Clarivate aplicará las medidas técnicas y organizativas establecidas en la Sección 4 (Seguridad) del ATD.

Última actualización: noviembre 2022 (Versión 2.1 ES)