Análisis de herramientas de videoconferencia

Microsoft Teams

1. ¿Quién es el responsable del tratamiento de datos?

El responsable del tratamiento es, en principio, el bufete de abogados, en nuestro caso CMS. El RGPD exige que el responsable del tratamiento celebre un APD con Microsoft cuando utilice Teams. Microsoft ofrece una plantilla estándar para este fin.

Sin embargo, el responsable de protección de datos de Berlín ha sido la primera autoridad de control que ha determinado que MS Teams no cumple los requisitos del GDPR y ha emitido el 3 de julio de 2020 la siguiente declaración sobre MS Teams (con un resumen justo al principio en negrita) (traducido con Deepl):

Microsoft Teams (como parte de Microsoft 365 en virtud de la validez de las condiciones de servicio en línea)

El proveedor se reserva el derecho de procesar los datos del pedido para sus propios fines. Defectos en el contrato de procesamiento de pedidos. Muchas ambigüedades y contradicciones en el contrato de procesamiento de pedidos. Exportación ilegal de datos. El proveedor ha realizado amplias modificaciones posteriores al contrato de tramitación de pedidos publicado sin identificarlas; la versión (según los metadatos) del 3.1.2020 contiene restricciones inadmisibles del derecho a dar instrucciones.

Nota importante: Microsoft ha realizado amplios cambios posteriores en el "Apéndice de la política de privacidad para Microsoft Online Services (alemán, enero de 2020)" (en adelante: "DPA") sin marcarlo. Hay un documento que se creó el 3.1.2020 según la metainformación y un documento que se creó el 9.6.2020 según la metainformación. Los nombres de los documentos son los mismos, el documento publicado por Microsoft en Internet ha sido sustituido tácitamente. En el historial de cambios ("Aclaraciones y resumen de cambios") se indica explícitamente "Ninguno", a pesar de que se modificaron grandes partes del contrato. La mayoría de estos cambios son de carácter puramente lingüístico. En particular, en la versión de 9.6.2020, el anexo Cláusulas Contractuales Estándar, que originalmente contenía desviaciones muy amplias de la redacción de las cláusulas contractuales estándar aprobadas, se adaptó esencialmente al texto aprobado. Sin embargo, también hay cambios relevantes en el contenido. La mayoría de los cambios son positivos. No obstante, sigue existiendo uno de los problemas básicos más importantes del contrato, que es poco claro y contradictorio en muchos puntos.

Microsoft se reserva en el APD el derecho a procesar los datos personales que realmente se procesan en nombre de Microsoft para sus propios fines en el apartado "Disposiciones de protección de datos - Naturaleza del procesamiento de datos; propiedad". No existe una base legal aparente para la divulgación de los datos personales por parte del responsable a Microsoft. Del tratamiento de los datos del pedido también para fines propios de Microsoft se desprende el problema de la corresponsabilidad según el art. 26 del DS-GVO. Según la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas, dicha responsabilidad conjunta es obvia, pero no puede descartarse en ningún caso sobre la base de la información sólo rudimentaria del APD. Esto es un problema al menos en lo que respecta a la responsabilidad (art. 5(2) en relación con el art. 5(1)(a) GDPR). En el caso de la existencia real, también está el hecho de que no hay acuerdo en virtud del Art. 26 del RGPD.

En muchos lugares, la APD contiene disposiciones que contradicen los requisitos legales mínimos. En la sección "Disposiciones sobre protección de datos - Tratamiento de datos personales; APD", sin embargo, hay una referencia poco clara al anexo 3 de la APD, que a su vez reproduce contenido esencial de los artículos 28, 32 y 33 del RGPD, pero también deja poco claro si estas normas deben o no tener prioridad sobre el texto real -claramente ilegal- de la APD. La versión del archivo de 9.6.2020 incluso empeora esta cláusula al referirse ahora a "[los] datos personales del GDPR". Un acuerdo de procesamiento de contratos tan poco claro hace imposible que los responsables cumplan con su responsabilidad en virtud del artículo 5 (2) en relación con el artículo 5 (1) lit. a del GDPR.

Sin embargo, el Anexo 3 de la DPA (en la versión del archivo de 3.1.2020) tampoco adopta completamente la redacción pertinente del Art. 28 DEL GDPR. En cualquier caso, el nº 2 lit. g del Anexo 3 (en la versión de archivo de 3.1.2020) no cumple los requisitos legales mínimos del Art. 28 (3) lit. g GDPR en el sentido de que la supresión o la devolución de los datos del pedido tras la finalización del mismo sólo se contempla a petición del cliente y no en todos los casos. El punto 2 lit. a del Anexo 3 (en la versión de archivo de 3.1.2020) también restringe de forma inadmisible el derecho del cliente a dar instrucciones en contra del Art. 28 (3) lit. a GDPR, ya que las excepciones no están previstas únicamente sobre la base del Derecho de la Unión o del Derecho de los Estados miembros a los que Microsoft está sujeto. En la versión del expediente de 9.6.2020, estos defectos se eliminaron tácitamente, al igual que la redacción del anexo se aproximó más a la redacción de la ley. Sin embargo, la redacción de la ley de la versión del 3.1.2020 también ha sido parcialmente sustituida por sus propios términos en la versión del 9.6.2020. Además, una nueva desviación de los requisitos mínimos del Art. 28 (3) lit. a del GDPR al excluir la obligación de notificar al cliente si Microsoft se ve obligada a procesar los datos incumpliendo las instrucciones, no sólo sobre la base de la ley aplicable a la obligación de procesamiento, sino sobre la base de cualquier ley (redacción "la legislación"). Otra desviación en perjuicio del cliente en la nueva versión de 9.6.2020 del número 7 del anexo 3 es que Microsoft no está obligada a notificar al cliente una llamada (en lugar de en la medida en que, es decir, ahora sólo si se cumple la condición de toda la información y ya no, como antes, en parte si se cumple la condición de partes de la información) esta información está a disposición de Microsoft a su discreción razonable (en lugar de la redacción objetiva "de manera razonable", es decir, ahora basada en una decisión equitativa de Microsoft que sólo está sujeta a una revisión judicial limitada). Además, no es evidente y, debido a la modificación oculta del contrato por parte de Microsoft, no cabe esperar que esta nueva versión del contrato también se haya acordado con los clientes existentes.

La DPA prevé restricciones de las cláusulas contractuales estándar en el punto "Seguridad de los datos - verificación del cumplimiento". Se trata de un "apéndice a la cláusula 5, apartado f, y a la cláusula 12, apartado 2, de las cláusulas contractuales tipo" y se afirma que las cláusulas contractuales tipo no se modifican con ello. Es cierto que en la introducción de la DPA hay una declaración general de que las Cláusulas Contractuales Tipo tienen prioridad sobre la DPA, al igual que las propias Cláusulas Contractuales Tipo, con su prohibición de modificación, contienen una norma de prioridad correspondiente. Ya es cuestionable -y problemático en relación con el art. 5 (2) DS-BER- si la cláusula de prioridad general de la introducción del APD es aplicable en general si la restricción concreta de las cláusulas contractuales tipo en cuestión pretende por sí misma no constituir una restricción, de modo que bajo este supuesto la cláusula de prioridad no puede aplicarse lógicamente. Sin embargo, esto puede quedar abierto, porque cualquier restricción de los derechos y obligaciones derivados de las cláusulas contractuales tipo, independientemente de su redacción e incluso si se declara subordinada y, por tanto, no aplicable en otro lugar, conduce a una modificación inadmisible de las cláusulas contractuales tipo. Ello se debe a que se pretende, y en consecuencia se consigue regularmente, que las cláusulas contractuales tipo no puedan aplicarse en su totalidad. En consecuencia, el considerando 109 del Reglamento de Exención por Categorías de DS también subraya que otras cláusulas

contractuales no pueden contradecir directa o indirectamente las cláusulas estándar de protección de datos. Así pues, a pesar de su presunta invalidez con arreglo al Derecho civil, la presente cláusula "adicional" de restricción también supone una modificación inadmisible de las cláusulas contractuales estándar, de modo que no pueden justificar la exportación de datos. Aunque Microsoft se ha sometido adicionalmente a la autocertificación de acuerdo con el Escudo de Privacidad, ésta sólo se aplica a los Estados Unidos. No obstante, Microsoft se reserva el derecho de procesar los datos del pedido en cualquier lugar en el que se encuentre Microsoft o sus subprocesadores (DPA, sección "Política de privacidad - Transferencias de datos y lugar de almacenamiento - Transferencias de datos").

Nos gustaría señalar que, en vista del posterior cambio no documentado del acuerdo de procesamiento de contratos publicado por Microsoft, tenemos la intención, en el curso de las auditorías, de comprobar también el cumplimiento de la forma del acuerdo de procesamiento de contratos de conformidad con el Art. 28 Párrafo 9 del GDPR y la correspondiente verificabilidad (Art. 5 Párrafo 2 del REPD).

Además, en Alemania, el BRAO (código de conducta de los abogados) exige que el bufete de abogados celebre un acuerdo de servicio por escrito con Microsoft; sin dicho acuerdo de servicio, el uso de los equipos de Microsoft para los datos relacionados con los clientes sería ilegal en Alemania.

Se adjunta el DPA de julio de 2020.

La crítica del responsable de la protección de datos de Berlín es muy similar a las dos primeras conclusiones clave del documento del Supervisor Europeo de Protección de Datos (SEPD) de 2 de julio de 2020 sobre su investigación del uso de productos y servicios de Microsoft por parte de las instituciones de la UE (las negritas son mías):

*En primer lugar, el acuerdo de licencia entre Microsoft y las instituciones de la UE permitía a Microsoft definir y cambiar los parámetros de sus actividades de tratamiento realizadas en nombre de las instituciones de la UE y las obligaciones contractuales de protección de datos**. La discrecionalidad de la que disponía Microsoft equivalía a un amplio derecho de Microsoft a actuar como responsable del tratamiento**. Dado el papel de las instituciones de la UE como instituciones de servicio público, el SEPD no consideró que esto fuera apropiado. El SEPD recomendó a las instituciones de la UE que actuaran para conservar la capacidad de control*

En segundo lugar, las instituciones de la UE debían establecer un acuerdo completo y conforme entre el responsable del tratamiento y los encargados del mismo, así como instrucciones documentadas de las instituciones de la UE a los encargados del tratamiento. ***Su falta de control sobre los subprocesadores que utiliza Microsoft y la falta de derechos de auditoría significativos también planteaban problemas importantes****. El SEPD formuló recomendaciones sobre la manera de mejorar el acuerdo entre el responsable del tratamiento y los encargados del mismo y de establecer controles de auditoría sólidos.*

El grupo de trabajo "Administración" de la conferencia de autoridades de protección de datos de Alemania recoge esta crítica y evalúa que Office 365 no cumple las leyes de protección de datos. Ha adoptado la siguiente decisión el 15 de julio de 2020 (traducida por DeepL):

Hechos

El Grupo de Trabajo Administración de la Conferencia de las Autoridades Independientes de Protección de Datos del Gobierno Federal y de los Estados Federales (AK Verwaltung der Konferenz der unabhängigen Datenschutzhaufsichtsbehörden des Bundes und der Länder) ha examinado las Condiciones de Servicio en Línea (TSO) en las que se basa el uso del producto Microsoft Office 365, así como el Apéndice de Procesamiento de Datos (APD) para los servicios en línea de Microsoft -ambos a

partir de enero de 2020- y los ha evaluado en lo que respecta a su conformidad con los requisitos del artículo 28, apartado 3, del Reglamento Básico de Protección de Datos (RGPD). Llega a la conclusión de que, sobre la base de estos documentos, no era posible utilizar Microsoft Office 365 de acuerdo con la normativa de protección de datos, al menos a partir de enero de 2020. Sobre esta base, DSK entablará un diálogo con Microsoft para resolver los problemas detectados. Las consecuencias de la sentencia del TJUE C-311/18 (Schrems II) aún no se consideran en este documento.

Evaluación de la Administración del Grupo de Trabajo:

1.) Tipo y finalidad del tratamiento, tipo de datos personales

Teniendo en cuenta también la clasificación del servicio MS Office 365 como servicio específico de la nube, según la cual puede ser adecuado definir los tipos de datos personales y su finalidad de tratamiento en términos generales, debe ser posible, sin embargo, que el cliente describa ambos con más detalle y, si es necesario, los especifique en términos más concretos. Esto se aplica, en particular, a la descripción de los datos personales en relación con los distintos requisitos de protección de datos y niveles de riesgo, por ejemplo, en el caso de los datos de conformidad con el art. 9 del RGPD, así como los fines pertinentes para el cliente. El contrato de tratamiento debe dejar claro en qué entorno (procedimientos especializados) se lleva a cabo el tratamiento de datos y con qué fines se van a tratar los datos. En este contexto, Microsoft recomienda reducir el grado de abstracción y utilizar campos libres que puedan adaptarse en caso necesario. Si es necesario, esto puede incluso permitir una designación concreta en casos individuales.

2.) La propia responsabilidad de Microsoft en el contexto del tratamiento con fines empresariales legítimos

El Acuerdo de Procesamiento de Datos (DPA) de Microsoft establece que, en la medida en que Microsoft utilice o procese de otro modo información personal en relación con las actividades empresariales legítimas de Microsoft, es como controlador de datos independiente responsable del uso y del cumplimiento de todas las leyes aplicables y de las obligaciones del controlador. Aunque se proporciona una lista de estas actividades comerciales legítimas, todavía no está claro qué otros datos personales se procesan en este contexto. Se trata, en particular, del tratamiento de datos personales relativos a las actividades de Microsoft en virtud de los puntos 3), 4), 5) y 6) de la definición de "actividad empresarial legítima". Además, no existe ninguna base jurídica para la transferencia de otros datos personales del responsable del tratamiento a Microsoft, por ejemplo en el contexto de la telemetría, que no sea el contrato de tramitación de pedidos. En la medida en que los responsables del tratamiento podrían demostrar un interés legítimo en el sentido del artículo 6 (1) (f) del RGPD para la transferencia a Microsoft como responsable independiente del tratamiento de datos del responsable del tratamiento y de terceros para "fines comerciales legítimos", esto no se aplica, de conformidad con el artículo 6 (1) frase 2 del RGPD, al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. Por lo tanto, se requiere una base jurídica independiente que permita a las autoridades públicas poner a disposición los datos de los empleados o ciudadanos para estos fines. La normativa respectiva sobre la permisibilidad del tratamiento de datos personales por parte de las autoridades públicas (de conformidad con el art. 6 (3) (b) REPD) sólo puede utilizarse como base jurídica de forma limitada debido al principio de estricta necesidad (por su relevancia para los derechos fundamentales). Sólo bajo la condición de que, por ejemplo, un uso seguro y sostenible del software sólo es posible si el proveedor puede procesar determinados datos personales del sistema, el tratamiento de datos correspondiente también puede ser necesario para el cumplimiento de las tareas.

En cualquier caso, para los lugares públicos no están representados todos los casos de uso de los "fines comerciales legítimos".

3) Divulgación de los datos procesados - Ley de la Nube

En las normas de protección de datos para los servicios en línea de Microsoft, Microsoft hace referencia al hecho de que los datos procesados también pueden divulgarse fuera de las instrucciones del cliente si las normas de protección de datos lo prevén o si así lo exige la ley. Esta descripción no es suficientemente concreta y no determina los derechos que debe definir contractualmente el cliente. La excepción sólo puede referirse al derecho de la Unión o al derecho nacional de un Estado miembro, sin que se excluya que los acuerdos de asistencia jurídica celebrados por la Unión o por los distintos Estados miembros con terceros países se apliquen también a este derecho. La aplicación concreta y los efectos de la Cloud Act, a la que Micro-soft, como fabricante estadounidense, está sujeta, sobre la cuestión de la protección de datos de la transferencia legalmente permitida de datos personales en este contexto, no se han aclarado de forma concluyente. Esta evaluación debe hacerse también a la luz de la reciente jurisprudencia del TJCE, que declara ineficaz el Escudo de Privacidad y cuestiona en general las transferencias de datos a EE.UU., véase TJCE, 16 de julio de 2020 - C-311/18 "Schrems II". Microsoft también utilizó cláusulas contractuales estándar para acompañar la certificación del Escudo de Privacidad. Estas también deben ser reevaluadas en base a la última jurisprudencia del TJUE.

4) Implementación de medidas técnicas y organizativas de acuerdo con el Art. 32 REPD

Por parte de la Conferencia de Supervisores de Protección de Datos Federales y Estatales, existe consenso en que el cliente debe poder revisar la implementación y descripción de las medidas técnicas y organizativas mediante las condiciones del servicio en línea, las normas de protección de datos y otra documentación proporcionada por Microsoft y obtener suficiente información (adicional). Aunque en la DPA se menciona una directriz de seguridad informática correspondiente (no en la OST), no está disponible antes de la celebración del contrato. Por lo tanto, hay que señalar que el estándar EAST de Microsoft no proporciona una descripción adecuada de las medidas ofrecidas por el servicio en línea para el tratamiento de datos personales que sean apropiadas para el riesgo. La política de Microsoft es que la parte responsable es la única responsable de determinar de forma independiente si las medidas técnicas y organizativas de un servicio en línea concreto cumplen sus requisitos, incluidas sus obligaciones de seguridad en virtud de la legislación de privacidad aplicable. Las actuales descripciones de las medidas técnicas y organizativas en los documentos contractuales no son suficientes por sí solas para que el responsable del tratamiento de datos (y además son difíciles de comprobar) realice una evaluación objetiva de si las medidas son adecuadas al riesgo.

5) Supresión y devolución de datos personales

Microsoft differentiates within the scope of processing between customer data arising from the contractual relationship and data that is processed independently for the purpose of providing "professional services" and processing for "legitimate business purposes". In accordance with its role as "controller", Microsoft will not delete data processed for its own purposes. Although it is understandable that this data is not part of the order processing according to the definition and is therefore processed on a different legal basis, it is nevertheless questionable how long the data is kept for own purposes. Microsoft does not comment on this.

6) Información sobre subcontratistas

En cuanto a la transferencia de datos personales a subcontratistas, el "consentimiento previo por escrito del cliente para subcontratar el tratamiento de los datos del cliente y de los datos personales por parte de Microsoft" solo es suficiente si se incluye una lista de subcontratistas aprobada por el responsable (cliente / mandante) en el momento de la firma del acuerdo de tratamiento del contrato (véase también el punto 3.2.7 del Dictamen 14/2019 del Comité Europeo de Protección de Datos). El "mecanismo de notificación al cliente de esta actualización" previsto para informar al cliente sobre la participación o la sustitución de los subcontratistas mediante la suscripción a las notificaciones push debe ser utilizado proactivamente por Microsoft en consecuencia.

El 2 de octubre de 2020, la Conferencia de Autoridades Independientes de Control de Protección de Datos del Gobierno Federal y de los Estados (Conferencia de Protección de Datos) ha apoyado la evaluación de su grupo de trabajo "Administración" sobre el tratamiento de datos por parte de Microsoft Office 365 del 15 de julio de 2020 con una mayoría de 9 sobre 8 miembros. Hay un gran número de autoridades de control que no comparten la opinión del grupo de trabajo.

Por lo tanto, las autoridades de control de protección de datos de Baden-Württemberg, Baviera, Hesse y Sarre publicaron el 2 de octubre de 2020 el siguiente comunicado de prensa (traducido por DeepL):

La Conferencia de las Autoridades Independientes de Control de Protección de Datos del Gobierno Federal y de los Estados (Conferencia de Protección de Datos) ha tomado nota de la evaluación de su grupo de trabajo Administración para el Procesamiento de Pedidos en Microsoft Office 365 del 15 de julio de 2020 por la mayoría de sus miembros. El grupo de trabajo había examinado "las condiciones de servicio en línea (OST) en las que se basa el uso del producto Microsoft Office 365, así como las normas de protección de datos para los servicios en línea de Microsoft (adenda de procesamiento de datos / DPA), ambas a partir de enero de 2020". El documento llega a la conclusión de que, sobre la base de los documentos mencionados, no es posible utilizar Microsoft Office 365 de acuerdo con la normativa de protección de datos.

La decisión de la conferencia de protección de datos se tomó por una estrecha mayoría de 9 votos con 8 votos en contra. Los comisarios estatales de protección de datos de BadenWürttemberg, Baviera, Hesse y Sarre y el presidente de la Oficina Estatal de Supervisión de la Protección de Datos de Baviera, responsable de Microsoft Deutschland GmbH, fueron algunos de los que se pronunciaron en contra de la aprobación sin reservas.

Las autoridades supervisoras de la protección de datos de Baden-Württemberg, Baviera, Hesse y Sarre dejan claro que también ven un considerable potencial de mejora en Microsoft Office 365 en términos de la ley de protección de datos, en particular a la vista de la reciente decisión del Tribunal de Justicia de la Unión Europea sobre las transferencias internacionales de datos de 16 de julio de 2020 (C-311/18 - Schrems II). Por lo tanto, apoyan en principio los objetivos del grupo de trabajo, en la medida en que formula puntos de partida para mejorar el producto Microsoft Office 365 en términos de derecho de protección de datos. Sin embargo, no pueden compartir su evaluación general porque es demasiado indiferenciada. Además, la Administración del Grupo de Trabajo ha basado su evaluación en las disposiciones contractuales, que Microsoft ya ha revisado dos veces entretanto. Por último, todavía no se han podido tener en cuenta las conclusiones del Tribunal de Justicia de las Comunidades Europeas

sobre los requisitos del reglamento básico de protección de datos para las transferencias internacionales de datos.

En este contexto, las autoridades de control de la protección de datos de BadenWürttemberg, Baviera, Hesse y Sarre han considerado la evaluación de la Administración del Grupo de Trabajo del 15 de julio de 2020 como una base de trabajo pertinente, pero aún no está lista para tomar una decisión. Esto es tanto más cierto cuanto que Microsoft aún no ha sido escuchada formalmente sobre las evaluaciones del Grupo de Trabajo sobre Administración, como es parte de un proceso justo y constitucional.

Las cinco autoridades de control de la protección de datos se alegran aún más de que la Conferencia de Protección de Datos haya creado por unanimidad un grupo de trabajo que, bajo la dirección del Comisario Estatal de Protección de Datos de Brandemburgo y de la Oficina Estatal de Supervisión de la Protección de Datos de Baviera, va a iniciar próximamente las conversaciones con el fabricante.

Dr. Stefan Brink, Prof. Dr. Thomas Petri, Michael Will, Prof. Dr. Michael Ronellenfitsch y Monika Grethel: "Estamos de acuerdo con toda la conferencia de protección de datos en que las incertidumbres legales en el manejo de la protección de datos de Microsoft Office 365 deben resolverse de manera oportuna. Sería bueno que el recién nombrado grupo de trabajo de la conferencia, respetando los principios del Estado de Derecho, pudiera garantizar que el fabricante introduzca pronto mejoras duraderas en su producto Microsoft Office 365 en lo que respecta a la ley de protección de datos. En un diálogo constructivo con Microsoft, deben discutirse las normas que deben observarse en el caso de las transferencias desde terceros países según la última jurisprudencia del Tribunal de Justicia de las Comunidades Europeas.

2. ¿Dónde se almacenan los datos?

El lugar de almacenamiento de los datos depende de la ubicación del responsable del tratamiento. Encontrará la ubicación aquí https://docs.microsoft.com/en-us/office365/enterprise/o365datalocations haciendo clic en el país del controlador de datos en la parte derecha de la página y luego busque la línea "Microsoft Teams".

En el caso de Alemania, los datos de Teams se almacenan en Alemania: https://docs.microsoft.com/enus/office365/enterprise/o365-data-locations#germany

Sin embargo, el SEPD emitió esta crítica:

En tercer lugar, las instituciones de la UE se enfrentaron a una serie de problemas relacionados con la localización de los datos, las transferencias internacionales y el riesgo de divulgación ilegal de los datos. No pudieron controlar la ubicación de una gran parte de los datos procesados por Microsoft. Tampoco controlaron adecuadamente lo que se transfería fuera de la UE/EEE y cómo. Tampoco había garantías adecuadas para proteger los datos que salían de la UE/EEE. Las instituciones de la UE también tenían pocas garantías a su disposición para defender sus privilegios e inmunidades y asegurar que Microsoft sólo revelaría los datos personales en la medida en que lo permitiera la legislación de la UE. El SEPD formuló recomendaciones para ayudar a las instituciones de la UE a abordar estas cuestiones.

A menos que Microsoft tenga derecho a cambiar unilateralmente la ubicación de los datos, lo que debería quedar excluido por el contrato de servicio individual obligatorio que debe celebrarse entre el bufete de abogados alemán y Microsoft, parece que, al menos para el uso de Microsoft Teams en Alemania, no hay problema en cuanto a la ubicación de los datos. En otros países podría ser diferente.

3. **¿Cuáles son los aspectos más importantes en los términos y condiciones de la plataforma?**

Microsoft proporciona un cifrado de extremo a extremo de todos los datos.

Además, Microsoft ofrece un gran número de configuraciones de seguridad posibles que hacen que sea bastante difícil, especialmente para los pequeños bufetes de abogados, encontrar la configuración adecuada.

Los términos y condiciones de Microsoft Teams (y de la mayoría de los demás productos de Microsoft) se pueden encontrar fácilmente a través de Google aquí: https://www.microsoft.com/en/servicesagreement/ . La Declaración de Privacidad se incluye como un enlace justo al principio de los términos y condiciones y se puede encontrar aquí: https://privacy.microsoft.com/enus/privacystatement . La DPA (como se adjunta) es mucho más difícil de encontrar - hay que acceder a este sitio https://www.microsoftvolumelicensing.com/DocumentSearch.aspx e introducir las palabras "DPA" en el campo de búsqueda para encontrarla.

En este contexto, el SEPD critica la falta de transparencia:

La abundancia de documentos contractuales, las cláusulas superpuestas y conflictivas dentro de ellos, la falta de un orden claro de precedencia y las actualizaciones mensuales de las cláusulas hacen que, como mínimo, sea difícil para las instituciones, órganos y organismos de la UE cumplir con sus obligaciones de información a los interesados, tal y como exige el artículo 4, apartado 1, letra a), del Reglamento (UE) 2018/1725.

Además, hay que tener en cuenta que en la versión en inglés las normas sobre garantías y responsabilidad (que están muy redactadas a favor de Microsoft) no se ajustan a la legislación alemana sobre condiciones generales y, por lo tanto, no son válidas, al menos para los clientes alemanes. La versión alemana es diferente y tiene en cuenta las normas alemanas sobre condiciones generales, pero algunas de las normas parecen, no obstante, contrarias a la legislación alemana y probablemente no sean válidas.

4. **¿En qué medida los proveedores de la plataforma venden o comparten los datos personales?**

No se ha encontrado ningún indicio de que Microsoft venda datos de clientes u otros datos personales relacionados con sus clientes.

En caso de búsqueda por parte de las autoridades públicas, según la legislación alemana, Microsoft sólo tendría que poner a disposición de las autoridades los datos a los que tendría acceso si estuvieran almacenados localmente. Además, si los datos están almacenados fuera de Alemania, la autoridad pública tiene que presentar una solicitud formal en el país en el que se encuentran los datos, que a menudo tarda mucho en concederse. Podría decirse, por tanto, que los datos están más seguros en la nube que si se almacenan localmente en el bufete de abogados.

5. **¿A qué vigilancia podrían estar expuestos los datos de los proveedores de plataformas expuestos?**

Dado que los datos están encriptados de extremo a extremo, la vigilancia sería un reto. Incluso cuando la Ley de la Nube de EE.UU. le obligue a poner los datos a disposición de las autoridades estadounidenses, el cifrado de extremo a extremo podría dificultar el cumplimiento por parte de Microsoft.

6. **¿Cómo es la disponibilidad de recursos y la jurisdicción competente?**

Mientras que la versión en lengua inglesa no contiene ninguna norma sobre la jurisdicción competente para los clientes de la UE, en la versión en lengua alemana (traducida con Deepl) sí lo hace:

"10. empresa que celebra el contrato, elección de la ley y lugar de jurisdicción. Si usted vive en Europa (o tiene allí su sede principal como empresa) y utiliza los servicios gratuitos o de pago, la empresa contratante es Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublín 18, Irlanda (registrada en la Oficina de Registro de Empresas de Irlanda con el número 256796 y el número de IVA IE 8256796 U y con la dirección 70 Sir John Rogerson's Quay, Dublín 2, Irlanda). La legislación de Irlanda se aplicará a todas las reclamaciones relacionadas con los servicios gratuitos y de pago. Esto se entiende sin perjuicio de sus derechos en virtud de la Ley de Protección del Consumidor del país en el que le proporcionamos los Servicios y en el que tiene su residencia habitual (o como empresa, su sede principal). Usted y Microsoft aceptan someterse a la jurisdicción de los tribunales del país en el que le proporcionamos los Servicios y en el que usted tiene su residencia habitual (o, como empresa, su sede principal) para todos los litigios que surjan o estén relacionados con estas Condiciones. Alternativamente, puede elegir el tribunal competente en Irlanda".

BlueJeans

1. ¿Quién es el responsable del tratamiento de datos?

La única referencia que se puede encontrar en los Términos y Condiciones en relación con el controlador de datos está en el Número 4 (Datos del usuario, contenido y grabación) "En la medida en que los Datos del Usuario proporcionados o revelados por el Cliente (como controlador de datos o exportador de datos) se consideren "datos personales" en virtud de la legislación o normativa aplicable de la Unión Europea, (a) el Cliente acepta que BlueJeans pueda transferir a, almacenar y procesar los Datos de Usuario en los Estados Unidos y/o en otro país fuera del Espacio Económico Europeo donde BlueJeans utilice instalaciones en relación con los Servicios con el fin de prestar los Servicios y dar soporte a los mismos y (b) BlueJeans (i) cumplirá con las instrucciones razonables y legales del Cliente en relación con la seguridad y la confidencialidad de los Datos de Usuario, y mantendrá salvaguardas administrativas, físicas y técnicas destinadas a proteger la seguridad y la integridad de los Datos de Usuario y (ii) procesará los Datos de Usuario únicamente de acuerdo con las instrucciones legales del Cliente o las instrucciones legales del interesado."

2. ¿Dónde se almacenan los datos?

Los centros de datos de BlueJeans están situados en California (donde también se encuentra su sede), Virginia, Ámsterdam (para Europa), Sydney y Singapur. Sin embargo, para los ciudadanos europeos, los datos pueden almacenarse fuera del EEE (véase a continuación un extracto de la Política de Privacidad)

"Si usted es residente de la UE:

Su información puede ser transferida y almacenada en un destino fuera del Espacio Económico Europeo ("EEE") que puede no estar sujeto a una legislación de protección de datos equivalente. Puede ser tratada por personal situado fuera del EEE que trabaje para nosotros o para uno de nuestros proveedores.

Podemos transferir sus datos personales fuera del EEE

- Para almacenarla.

- Para permitirnos prestar servicios y cumplir nuestro contrato con usted o con la empresa para la que trabaja o la empresa que le proporciona acceso a los Servicios. Esto incluye el cumplimiento de los pedidos, el procesamiento de los datos de pago y la prestación de servicios de asistencia.

- Cuando estemos legalmente obligados a hacerlo.

- Para facilitar el funcionamiento de nuestro grupo de empresas, cuando sea en nuestro interés legítimo y hayamos llegado a la conclusión de que sus derechos no prevalecen.

- Cuando tengamos su consentimiento para hacerlo

Cuando compartimos información sobre usted dentro de BlueJeans y con terceros en países con leyes locales que pueden diferir de las suyas, hacemos uso de las cláusulas contractuales estándar de protección de datos, que han sido aprobadas por la Comisión Europea, y nos basamos en el Marco del Escudo de Privacidad UE-EE.UU. para salvaguardar la transferencia de la información que recopilamos desde el Espacio Económico Europeo a los Estados Unidos. En algunos casos podemos utilizar otros mecanismos legales apropiados para salvaguardar la transferencia.

Cuando su información se transfiera fuera del EEE, tomaremos todas las medidas razonablemente necesarias para garantizar que sus datos estén sujetos a las salvaguardias apropiadas, como por ejemplo confiar en un mecanismo de adecuación legal reconocido, y que se traten de forma segura y de acuerdo con esta política de privacidad."

En la base de datos de BlueJeans sólo se almacenan los datos más básicos de los clientes: nombre de usuario, contraseña (hash salado SHA-256), correo electrónico, nombre, cargo, empresa y foto de perfil. Al programar y realizar reuniones, se recogen y almacenan ciertos registros de detalles de las llamadas (fecha/hora de inicio, duración, etc.) para la elaboración de informes.

Las grabaciones se almacenan en contenedores seguros en la nube. Estos vídeos están encriptados en reposo (AES-256bit) y sólo son accesibles para el emisor de la grabación.

Detalles de la facturación: El servicio BlueJeans utiliza actualmente a un socio externo que cumple con la normativa PCI para gestionar todos los aspectos de facturación del servicio. Esto significa que la base de datos de BlueJeans no contiene información sobre la tarjeta de crédito o la facturación del usuario. Dado que el servicio es utilizado por miles de empresas en todo el mundo, BlueJeans también cumple con el marco de protección de la intimidad de la UE y los Estados Unidos.

3. ¿Cuáles son los aspectos más importantes en los términos y condiciones de la plataforma?

4. DATOS DEL USUARIO, CONTENIDO Y GRABACIÓN

4.1 Datos del usuario. Para configurar cuentas y utilizar los Servicios, el Cliente puede proporcionar información, como la dirección IP, el nombre de usuario, la contraseña y la información de identificación personal (por ejemplo, nombre, número de teléfono, dirección de correo electrónico, etc.) ("Datos del usuario"). El Cliente concede a BlueJeans y a sus subcontratistas el derecho a almacenar, procesar y recuperar los Datos de Usuario en relación con la prestación y el soporte de los Servicios. El Cliente garantiza que ha obtenido el consentimiento necesario de los Usuarios del Cliente para transferir los Datos de Usuario a BlueJeans y para procesar los Datos de Usuario tal y como se contempla en los Servicios, y acepta que BlueJeans pueda transferir, almacenar y procesar los Datos de Usuario en los lugares en los que BlueJeans utilice instalaciones en relación con los Servicios con el fin de prestar los Servicios y dar soporte a los mismos. En la medida en que los Datos de Usuario proporcionados o revelados por el Cliente (como controlador o exportador de datos) se consideren "datos personales" en virtud de la legislación o la normativa aplicable de la Unión Europea, (a) el Cliente acepta que BlueJeans pueda transferir, almacenar y procesar los Datos de Usuario en los Estados Unidos y/o en otro país fuera del Espacio Económico Europeo donde BlueJeans utilice instalaciones en relación con los Servicios con el fin de prestar los Servicios y dar soporte a los mismos y (b) BlueJeans deberá (i) cumplir con las instrucciones razonables del Cliente, (b) BlueJeans (i) cumplirá con las instrucciones razonables y legales del Cliente en relación con la seguridad y la confidencialidad de los Datos de Usuario, y mantendrá salvaguardias administrativas, físicas y técnicas destinadas a proteger la seguridad y la

integridad de los Datos de Usuario, y (ii) procesará los Datos de Usuario únicamente de acuerdo con las instrucciones legales del Cliente o las instrucciones legales del interesado. Si BlueJeans no puede cumplir el apartado 4.1(b), el único y exclusivo recurso del Cliente será rescindir el presente Acuerdo y dejar de utilizar los Servicios.

4.2. Contenido. Los usuarios pueden mostrar, cargar y almacenar archivos, grabaciones, sonido, música, gráficos e imágenes en relación con el uso del Servicio por parte del Cliente ("Contenido"). El Cliente declara y garantiza que es propietario o que tiene los permisos necesarios para utilizar y autorizar el uso del Contenido del Cliente. El Cliente concede a BlueJeans y a sus subcontratistas un derecho y una licencia no exclusivos, mundiales, libres de derechos, pagados y transferibles para alojar, almacenar en caché, copiar, guardar y mostrar el Contenido del Cliente con el fin de proporcionar y apoyar el Servicio. El Cliente reconoce y acepta que, salvo lo expresamente establecido en el presente documento, (a) BlueJeans no es responsable en modo alguno del Contenido del Cliente, (b) el Cliente asume todos los riesgos asociados a su Contenido y a la transmisión del mismo y (c) el Cliente es el único responsable de la exactitud, calidad, legalidad y adecuación de su Contenido.

4.3. Grabación. El Servicio puede proporcionar una función que permite a los Usuarios grabar Reuniones individuales. El Cliente tiene la opción de activar o desactivar la función de grabación. El Cliente es el único responsable de cumplir con todas las leyes de cualquier jurisdicción pertinente cuando utilice esta función. BlueJeans ha implementado medidas técnicas y organizativas diseñadas para proteger las Reuniones que el Cliente graba y almacena de pérdidas accidentales y del acceso, uso, alteración o divulgación no autorizados. Sin embargo, BlueJeans no puede garantizar que terceras partes no autorizadas no puedan anular dichas medidas. El Cliente reconoce que almacena dicha información bajo su propia responsabilidad.

11. LEY APLICABLE Y JURISDICCIÓN. El presente Acuerdo, así como cualquier reclamación, pleito, acción o procedimiento legal que se derive del mismo, ya sea de carácter contractual, extracontractual o de otro tipo, se regirá e interpretará de acuerdo con las leyes internas del Estado de Nueva York, sin dar efecto a las disposiciones o normas de elección o conflicto de leyes de cualquier jurisdicción. Cada una de las partes se somete irrevocablemente a la jurisdicción exclusiva de los tribunales federales de los Estados Unidos o de los tribunales del Estado de Nueva York, y renuncia a cualquier objeción basada en un lugar inadecuado o en un *forum non conveniens.*

4. ¿En qué medida los proveedores de la plataforma venden o comparten los datos personales?

Vea a continuación un extracto de la política de privacidad de BlueJeans:

"Hay ciertas circunstancias en las que podemos compartir su información con determinados terceros. Cualquier acceso de un tercero a la información es gestionado por BlueJeans, y los terceros son investigados basándose en parte en su capacidad para proteger la información. El movimiento internacional de la información en consonancia con esta forma de compartirla se trata en la sección "Cómo movemos la información" más adelante. Como parte de su uso del Servicio, usted puede compartir información con otros usuarios del Servicio. Esos usuarios del Servicio pueden estar ubicados en casi cualquier lugar del mundo, pueden estar comunicándose con Sitios de Terceros

(como se define más adelante) mientras usan los Servicios, y pueden estar limitados por la ley o por un acuerdo con nosotros sobre el uso de la información que usted comparte. Sin embargo, esta Política sólo se refiere a nuestro uso de la información.

Podemos compartir la información con empleados, contratistas, agentes o consultores con una estricta necesidad de conocimiento bajo las obligaciones de confidencialidad apropiadas.

Podemos compartir información con terceros que desempeñen funciones relacionadas con el negocio en nombre de BlueJeans, incluyendo

- Nuestros socios comerciales, clientes, proveedores, suministradores de servicios, vendedores y subcontratistas para el cumplimiento de cualquier contrato que celebremos u otros tratos que tengamos en el curso normal de los negocios con usted o con la empresa para la que trabaja o con la empresa que le proporciona acceso a los Servicios. Algunos ejemplos de estas funciones relacionadas con el negocio para las que podemos compartir información pueden incluir el alojamiento de datos, el análisis de datos, la prestación de asistencia de marketing, la prestación de servicio al cliente y soporte técnico, la tramitación de pedidos, el envío de comunicaciones a usted en nuestro nombre o bajo nuestra dirección, la participación de los usuarios y la incorporación, la solicitud de comentarios con respecto a los Servicios, la facilitación de la facturación y / o pagos, y otros a nuestra discreción razonable;
- Nuestros auditores, asesores jurídicos y otros asesores profesionales o proveedores de servicios; o las agencias de referencia de crédito con el fin de evaluar su puntuación de crédito cuando esto sea en el contexto de la celebración de un contrato con usted o la persona para la que trabaja;
- Podemos compartir información con nuestros distribuidores y revendedores autorizados si usted ha adquirido su licencia de los Servicios a través de una parte distinta de BlueJeans para permitir que esos distribuidores y revendedores cumplan sus obligaciones comerciales con usted; y
- Podemos compartir la información obtenida a través de nuestros Servicios con proveedores de análisis y motores de búsqueda que nos ayuden a mejorar y optimizar nuestro sitio y que estén sujetos a la sección de cookies de esta política.

Cuando contratamos a otra empresa para que preste servicios de esta naturaleza, sólo concedemos a dicha empresa el derecho a utilizar la información que sea razonablemente necesaria para realizar su función específica. Podemos compartir información con otros terceros, incluso cuando usted dé su consentimiento para una situación específica. Si BlueJeans tiene la intención de compartir cualquier información de una manera distinta a la descrita anteriormente, utilizando cualquier dato personal de cualquier manera que no sea compatible con esta Política de Privacidad, y no tenemos una base legal para compartir esa información sin su consentimiento, se le informará de dicho uso anticipado y se le dará la oportunidad de proporcionar su consentimiento para dicho uso.

Podemos compartir información con terceros si creemos razonablemente que dicha acción es necesaria para

- Cumplir con una obligación legal, un reglamento o una solicitud gubernamental,

- hacer cumplir nuestras políticas y acuerdos,

- proteger y defender los derechos, la propiedad y la seguridad de BlueJeans, nuestros clientes, usuarios, revendedores u otros, o

- actuar en circunstancias urgentes para proteger la seguridad personal de los usuarios de los Servicios o del público.

Esto incluye el intercambio de información con otras empresas y organizaciones con fines de protección contra el fraude y la reducción del riesgo crediticio y para prevenir la ciberdelincuencia. Podemos compartir información con nuestras subsidiarias y filiales corporativas que apoyan nuestro procesamiento de datos personales bajo esta Política. A medida que desarrollamos nuestro negocio, podemos vender o comprar empresas o activos. En el caso de una venta, adquisición, fusión, reorganización, disolución o evento similar, la información puede formar parte de los activos transferidos. Se le notificará por correo electrónico y/u otros medios cualquier noticia sobre una transacción y las opciones que pueda tener en relación con su información. A efectos de la Ley de Privacidad del Consumidor de California, no "vendemos" su información personal".

5. ¿A qué vigilancia podrían estar expuestos los datos de los proveedores de plataformas?

Para más información:

• BlueJeans Terms & Conditions: https://www.bluejeans.com/terms-andconditions

• BlueJeans Privacy Policy: https://www.bluejeans.com/privacy-policy

• BlueJeans Network Security and Privacy: https://www.bluejeans.com/sites/default/files/pdf/Blue-Jeans-NetworkSecurity.pdf

Cisco Terms and Conditions

Términos y condiciones:

Al hacer clic en el enlace "Términos y condiciones" de la página de inicio de Cisco, se accede a los términos y condiciones del sitio web. Para acceder a los términos y condiciones relevantes para la plataforma de reuniones Cisco Webex, hay que ir primero a la página de inicio del producto. Las condiciones aplicables de condiciones aplicables se encuentran en el Acuerdo Universal de la Nube de Cisco (26 de abril, 2020) leído junto con la Declaración de privacidad en línea (1 de mayo de 2020). Si se sigue buscando en el sitio lleva a una serie de Hojas de Datos de Privacidad que "complementan la Declaración de Privacidad de Cisco de Cisco y describen los datos personales que Cisco recopila y procesa como parte de la como parte de la prestación del Servicio en la Nube", así como Mapas de Datos de Privacidad. Esto proporciona un alto grado de transparencia. Un pdf de la Hoja de Datos de Privacidad de Webex se produce adjunto.

1. **¿Quién es el responsable del tratamiento de datos?**

Evidentemente, la recogida y el tratamiento de los datos por parte de Cisco la convierten en responsable del tratamiento, aunque es posible concebir circunstancias en las que Cisco pueda ser sólo un encargado del tratamiento. Ambas situaciones se reflejan en los apartados "Acceso y exactitud de sus datos personales" de la política de privacidad.

Más concretamente, la hoja de datos de privacidad de Webex deja claro que, en el caso de los contenidos generados por el usuario, el responsable del tratamiento es el cliente:

Si usted es un usuario y su empleador es el cliente que adquirió el servicio, su empleador es el "controlador de datos" para el contenido generado por el usuario (véase el mapa de datos de privacidad de Webex Meetings para visualizar quién hace qué con los datos). La información descrita en la siguiente tabla y en esta Hoja de Datos de Privacidad es accesible para su empleador y está sujeta a las políticas de su empleador en relación con el acceso, el uso, la supervisión, la eliminación, la conservación y la exportación de la información asociada al Servicio

No se nombra a ningún responsable de la protección de datos, pero en la política de privacidad, en el apartado "cómo ponerse en contacto con nosotros", se indica la siguiente dirección.

EMEAR Privacy Officer

Cisco Systems, Inc.

Haarlerbergweg 13-19,

1101 CH Amsterdam-Zuidoost,

Netherlands

En el apartado "Resolución de reclamaciones" aparece la siguiente nota:

"El principal establecimiento de Cisco en la UE está en los Países Bajos. Como tal, nuestra autoridad principal de la UE es la Autoritiet Persoonsgegevens holandesa".

Para las personas residentes en Europa (excluyendo Italia), Oriente Medio, África, Asia (excluyendo Japón y China), Oceanía (excluyendo Australia), la ley del contrato es la ley inglesa y la jurisdicción exclusiva se confiere a los tribunales ingleses. Para las personas residentes en Italia, se aplica la ley italiana y se confiere jurisdicción exclusiva al Tribunal de Milán. Para los problemas de privacidad no resueltos, se proporciona un enlace en la Declaración de Privacidad a un "proveedor de resolución de disputas de terceros con sede en Estados Unidos". Al hacer clic en el enlace se abre un formulario de reclamación en línea. En algunos casos, también se puede recurrir a un arbitraje vinculante.

2. **¿Dónde se almacenan los datos?**

El Acuerdo de Universal Cloud establece en la sección 4(d): Cisco podrá procesar y almacenar los Datos del Cliente y los Datos Personales fuera del país en el que se hayan recogido. Cisco sólo transferirá los Datos Personales de conformidad con la legislación aplicable. En la medida en que Cisco procese en su nombre datos personales procedentes del Espacio Económico Europeo o de Suiza, lo hará de conformidad con los principios del Escudo de Privacidad de la UE o de Suiza y Estados Unidos o los marcos que los sustituyan ("Principios")

La Declaración de Privacidad establece:

> **Transferencia, tratamiento y almacenamiento internacional de información personal**
>
> Dado que Cisco es una organización mundial, podemos transferir los datos personales del usuario a Cisco en los Estados Unidos de América, a cualquier filial de Cisco en el mundo, o a terceros y socios comerciales, tal como se ha descrito anteriormente, que se encuentran en diversos países del mundo. Al utilizar nuestros sitios web y Soluciones o al proporcionarnos cualquier información personal, cuando la legislación aplicable lo permita, el usuario reconoce y acepta la transferencia, el procesamiento y el almacenamiento de dicha información fuera de su país de residencia, donde las normas de protección de datos pueden ser diferentes.
>
> Cisco protege y permite la transferencia global de información personal de varias maneras:
>
> **Escudos de privacidad de la UE, el Reino Unido y Suiza-Estados Unidos**
>
> Cisco Systems Inc. y sus filiales con sede en EE.UU... participan y han certificado el cumplimiento de los Marcos y Principios del Escudo de Privacidad UE-EE.UU. y Suiza-EE.UU., según lo establecido por el Departamento de Comercio de EE.UU. en relación con la recopilación, el uso y la retención de información personal transferida desde la Unión Europea (UE), el Reino Unido (RU) y Suiza, respectivamente. Cisco-US se compromete a someter toda la información personal recibida de los países miembros de la Unión Europea (UE), el Reino Unido y Suiza, en virtud de los Marcos de Privacidad UE-EEUU y Suiza-EEUU, a los Principios aplicables de los Marcos. Si existe algún conflicto entre los términos de esta Declaración de Privacidad y los Principios del Escudo de Privacidad, regirán los Principios del Escudo de Privacidad... Cisco-US es responsable del tratamiento de la información personal que recibe, en virtud de estos Marcos del Escudo de Privacidad, y que posteriormente transfiere a un tercero que actúa como agente en su nombre. Cisco-US cumple con los Principios del Escudo de Privacidad para todas las transferencias posteriores de información personal desde la UE, el Reino Unido y Suiza, incluidas las disposiciones de responsabilidad de las transferencias

posteriores. En determinadas situaciones, Cisco-US puede verse obligado a revelar información personal en respuesta a solicitudes legales de las autoridades públicas, incluyendo el cumplimiento de requisitos de seguridad nacional o de aplicación de la ley. Con respecto a la información personal recibida o transferida en virtud de estos marcos de protección de la privacidad, Cisco-US está sujeto a los poderes de aplicación de la Comisión Federal de Comercio de los Estados Unidos.

3. **¿Qué datos se recopilan?**

Esto se concreta en las tablas detalladas que figuran en el Mapa de Datos de Privacidad de Webex, tabuladas en función de la finalidad del tratamiento/interés legítimo. Se hace referencia al pdf.

4. **¿En qué medida vende o comparte Zoom los datos personales?**

El mapa de datos de privacidad no revela ninguna venta de datos personales.

Sin embargo, todos los datos personales en poder de Cisco serán susceptibles de ser recuperados en virtud de la Ley de la Nube y otras disposiciones estadounidenses de brazo largo.

5. **¿Cuál es la seguridad técnica de la plataforma?**

Webex proporciona cifrado en tránsito como estándar, pero ofrece cifrado de extremo a extremo como opción adicional.

Jitsi

1. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE DATOS?

La nota "Jitsy Meet Security & Privacy" remite al usuario al Suplemento de Privacidad de 8x8 y a las Condiciones de Servicio de meet.jit.si De acuerdo con lo anterior, 8×8 es el principal colaborador de la solución de vídeo reuniones de código abierto Jitsi.org. Meet.jit.si es una aplicación de la solución de reuniones de vídeo de código abierto Jitsi.org que 8×8 aloja y que permite a los usuarios celebrar reuniones de vídeo gratuitas. 8×8, Inc. ("8×8") es una sociedad de Delaware con sede en 675 Creekside Way, Campbell, California 95008, Estados Unidos.

2. ¿DÓNDE SE ALMACENAN LOS DATOS?

Según la nota "Seguridad y privacidad de Jitsy Meet", por defecto Jitsi Meet no requiere que los usuarios creen cuentas. Cualquier información que los usuarios decidan introducir, como su nombre o dirección de correo electrónico, es puramente opcional y sólo se comparte con otros participantes de la reunión. Jitsi no conserva esta información después de la reunión. Otros datos, como el chat o las estadísticas de los oradores, por ejemplo, se almacenan mientras dura la reunión y se destruyen cuando ésta termina. Muchas de estas cosas pueden ser personalizadas por la configuración de la implementación real que el usuario está utilizando. Jitsi/8x8 conserva todos los valores predeterminados anteriores, pero se recomienda encarecidamente al usuario que consulte también la política de privacidad y las condiciones de servicio de meet.jit.si. Las grabaciones se mantienen en los servidores de meet.ji.si hasta que se suben al lugar indicado por el usuario (actualmente Dropbox). Si meet.ji.si no ha conseguido hacerlo en 24 horas, las borran igualmente y desaparecen para siempre.

3. ¿Cuáles son los aspectos más importantes en los términos y condiciones de la plataforma?

I. 8x8 conserva la información personal que recopila de los usuarios cuando tiene una necesidad comercial legítima y continua de hacerlo (por ejemplo, para proporcionar a los usuarios un servicio que han solicitado o para cumplir con los requisitos legales, fiscales o contables aplicables). Cuando no tengan ninguna necesidad comercial legítima de procesar la información personal, la eliminarán o la convertirán en anónima o, si esto no es posible (por ejemplo, porque la información personal se ha almacenado en archivos de copia de seguridad), almacenarán de forma segura la información personal y la aislarán de cualquier tratamiento posterior hasta que sea posible su eliminación.

II. Según el Aviso de Privacidad de 8x8, los individuos de la UE tienen derecho a acceder a sus datos personales almacenados y a limitar su uso y divulgación. Con la certificación del Escudo de Privacidad, 8x8 se ha comprometido a respetar esos derechos. Dado que el personal de 8x8 Inc. tiene una capacidad limitada para acceder a los datos que los clientes u otros controladores de datos transmiten, reciben o almacenan a través de nuestros servicios, si el usuario es un individuo de la UE cubierto por el Escudo de Privacidad y el Aviso de Privacidad de 8x8, y desea solicitar acceso o limitar el uso o la divulgación de sus 20 datos personales, debe proporcionar el nombre del cliente de 8x8 Inc. u otro

controlador de datos que transmitió, recibió o almacenó datos personales a través de los servicios de 8x8. 8x8 remitirá la solicitud del usuario a ese cliente u otro controlador de datos y apoyará a esa empresa según sea necesario para responder a la solicitud del usuario.

III. Meet.jit.si utiliza Analytics como Amplitude, Datadog y Crashlytics para cubrir varios aspectos de las aplicaciones y la infraestructura en meet.jit.si. Las cosas que se rastrean en las analíticas incluyen, un identificador anónimo (los usuarios pueden correr en modo "incógnito" si esto les molesta), la tasa de bits, el ancho de banda disponible, las ofertas y respuestas de SDP, los eventos de utilización del producto, los volcados de la aplicación móvil (cuánto se utilizan en general las diversas características del producto). Una vez terminada la reunión, no conservan ningún nombre, dirección de correo electrónico o foto de perfil (sólo se transmiten a los demás participantes en la reunión).

IV. 8x8 advierte que la información personal puede ser transferida y procesada en países distintos al de residencia del usuario. Estos países pueden tener leyes de protección de datos diferentes a las del país del usuario (y, en algunos casos, pueden no ser tan protectoras). En concreto, los servidores de sus sitios web están ubicados en varios lugares, incluidos el Reino Unido y los Estados Unidos, y las empresas de su grupo y los proveedores de servicios y socios externos operan en todo el mundo. Esto significa que cuando recogen información personal, pueden procesarla en cualquiera de estos países. Sin embargo, 8x8 afirma que ha tomado las medidas de seguridad adecuadas para garantizar que la información personal quede protegida de acuerdo con su Aviso de Privacidad. Esto incluye la aplicación de un acuerdo intragrupo basado en las cláusulas contractuales tipo de la Comisión Europea para la transferencia de información personal entre empresas del grupo. 8x8 Inc. también se ha certificado en el marco del Escudo de Privacidad Unión Europea-Estados Unidos y en el marco del Escudo de Privacidad Estados Unidos-Suiza. 8x8 también exige a estos terceros que protejan la información personal que procesan desde el Espacio Económico Europeo ("EEE") de acuerdo con la legislación de protección de datos de la Unión Europea. Se pueden proporcionar más detalles si se solicita.

V. Cláusula sobre el Escudo de Privacidad

VI. En su Aviso de Privacidad, 8x8 tiene una sección especial sólo para los visitantes del EEE. En el caso de los visitantes del Espacio Económico Europeo, la base legal para la recogida y el uso de la información personal dependerá de la información personal en cuestión y del contexto específico en el que 8x8 la recoja. Sin embargo, 8x8 normalmente sólo recogerá información personal (i) cuando el tratamiento sea en su interés legítimo y no sea anulado por los derechos de los usuarios, (ii) cuando el tratamiento sea una necesidad contractual, o (iii) cuando tenga el consentimiento de los usuarios para hacerlo. En algunos casos, también pueden tener la obligación legal de recoger la información personal de los usuarios o pueden necesitar la información personal para proteger los intereses vitales de los usuarios o los de otra persona.

Si 8x8 pide al usuario que proporcione información personal para cumplir con un requisito legal o para entrar en contacto con la organización del usuario, lo dejará claro en el momento pertinente e informará al usuario de si el suministro de su información personal es obligatorio o no (así como de las posibles consecuencias si el usuario no proporciona su información personal).

Según su declaración, si recopilan y utilizan información personal en función de sus intereses legítimos (o los de un tercero), este interés será normalmente el de operar sus sitios web o servicios y comunicarse con los usuarios según sea necesario para prestar sus servicios a la organización del usuario; así como por sus intereses comerciales legítimos, por ejemplo, al responder a las consultas de los usuarios, mejorar su sitio web o sus servicios, emprender actividades de marketing, o con el fin

de detectar o prevenir actividades ilegales. Estipulan que pueden tener otros intereses legítimos y, si procede, aclararán al usuario en el momento pertinente cuáles son esos intereses legítimos. VII. Las leyes del Estado de California, EE.UU., excluyendo las normas de conflicto de leyes de California, se aplicarán a cualquier disputa que surja de o esté relacionada con los Términos o el Servicio. Todas las reclamaciones que surjan o estén relacionadas con las Condiciones o el Servicio se litigarán exclusivamente en los tribunales federales o estatales del condado de Santa Clara, California, EE.UU., y al aceptar el uso de la aplicación también se considera que se consiente la jurisdicción personal en dichos tribunales.

4. ¿EN QUÉ MEDIDA LOS PROVEEDORES DE LA PLATAFORMA VENDEN O COMPARTEN LOS DATOS PERSONALES?

Según el Aviso de Privacidad de 8x8, pueden revelar la información personal de los usuarios a las siguientes categorías de destinatarios:

- A las empresas de su grupo, a los proveedores de servicios de terceros y a los socios que les prestan servicios de procesamiento de datos, por ejemplo (i) para apoyar la entrega, proporcionar funcionalidad o ayudar a mejorar la seguridad de sus sitios web o servicios, (ii) para el control y la garantía de calidad, o (iii) para mejorar sus servicios y desarrollar nuevos servicios. También podrán compartir información personal con dichos terceros cuando consideren que dicha divulgación es necesaria para proteger la seguridad o los intereses comerciales legítimos de dichos terceros, incluso para investigar sospechas de fraude o para localizar a los deudores;

- a cualquier organismo policial, regulador, agencia gubernamental, tribunal u otro tercero competente cuando consideren que la divulgación es necesaria (i) en virtud de la legislación o la normativa aplicable, (ii) para ejercer, establecer o defender sus derechos legales, o (iii) para proteger los intereses vitales del usuario o de cualquier otra persona;

- a un comprador real o potencial (y a sus agentes y asesores) en relación con cualquier propuesta de compra, fusión o adquisición de cualquier parte de su negocio, siempre que se informe al comprador de que debe utilizar la información personal de los usuarios únicamente para los fines indicados en el Aviso de Privacidad;

- a cualquier otra persona con el consentimiento de los usuarios para la divulgación

Además, 8x8 Inc. puede revelar Datos Personales a sus afiliados, así como a un número limitado de socios comerciales de terceros, proveedores de servicios, vendedores, proveedores y otros contratistas (colectivamente "Proveedores de Servicios") con el fin de ayudar a 8x8 en la prestación, gestión, despliegue, mejora de sus servicios. 8x8 Inc. mantiene contratos con estas filiales de 8x8 Inc. y con los Proveedores de Servicios en los que se restringe su acceso, uso y divulgación de los Datos Personales en cumplimiento de las obligaciones del Escudo de Privacidad, y 8x8 Inc. puede ser responsable si dichas partes no cumplen con dichas obligaciones y 8x8 es responsable del hecho que origina el daño. 8x8 también puede compartir o divulgar Datos Personales en la medida en que el cliente u otro controlador de datos haya obtenido el consentimiento de la persona de la UE correspondiente.

5. ¿A qué vigilancia podrían estar expuestos los datos de los proveedores de plataformas?

8x8 Inc. puede verse obligada a revelar datos personales en respuesta a solicitudes legales de las autoridades públicas o a procesos administrativos o judiciales, incluso para cumplir con requisitos de seguridad nacional o de aplicación de la ley. Seguridad: 8x8 utiliza medidas técnicas y organizativas apropiadas para proteger la información personal que recoge y procesa sobre los usuarios. Las medidas que utilizan están diseñadas para proporcionar un nivel de seguridad adecuado al riesgo de procesar la información personal de los usuarios. Las medidas específicas que utilizan incluyen la tecnología de encriptación SSL para la protección de la información sensible, como los pagos, cuando está en tránsito. Disponen de salvaguardas administrativas, técnicas y físicas estándar en la industria para proteger la confidencialidad, integridad y disponibilidad de la información personal. Además, en EE.UU. están validados según las normas HIPPAA y FISMA, y en el Reino Unido están certificados según los esquemas de certificación ISO27001; ISO9000:2015 y Cyber Essentials.

PREOCUPACIONES DE SEGURIDAD DE LOS USUARIOS

1.- Según el "Jitsi Meet Security & Privacy" en muchos aspectos las reuniones de Jitsi son privadas por diseño. Las salas de reuniones son efímeras y se destruyen cuando el último participante se va. Sin embargo, se comentó que cuando has creado un enlace y cierras el chat, la sala se cierra, pero, en el futuro si vuelves a entrar en la misma sala, cualquiera que tuviera el enlace original puede verte o escucharte sin que lo sepas.

2.- La página oficial/seguridad dice: "Las reuniones de Jitsi pueden funcionar de 2 maneras: peer-to-peer (P2P) o a través del Jitsi Videobridge (JVB). Esto es transparente para el usuario. El modo P2P sólo se utiliza para las reuniones 1 a 1. En este caso, el audio y el vídeo se encriptan utilizando DTLS-SRTP en todo el trayecto desde el emisor hasta el receptor, incluso si atraviesan componentes de red como los servidores TURN". Sin embargo, parece que E2EE sólo es aplicable en las comunicaciones uno a uno, mientras que en los casos de más de 2 participantes en una sala WebRTC no proporciona actualmente las herramientas necesarias para hacer posible E2EE.

- entre 2 participantes la llamada está encriptada E2E y p2p, por lo que parece muy difícil, si no imposible, que "Big Bother" escuche/grabe

- entre 3 participantes la llamada está encriptada E2E, pero no p2p, porque el servidor necesita desencriptar la videollamada, así que si el Gran Hermano tiene acceso al servidor puede escuchar/grabar. En este caso, si el servidor es tuyo, la comunicación debería seguir siendo segura.

3.- Informes de usuarios desconocidos no invitados/espías

4.- Informes de trolls que invaden una sala de reuniones. En caso de que el usuario esté usando su propio servidor (en lugar de, por ejemplo, meet.jit.si) cualquiera que tenga root en el servidor podrá adivinar los nombres de las salas y obtener un posible acceso a la sala de reuniones.

5.- El servidor Jitsi intenta llegar a Internet, incluso cuando no hay reuniones. Un firewall podría detener la conexión, pero hay preocupaciones al respecto.

6.- Normalmente todos los usuarios tienen los mismos poderes, por lo que cualquiera en la sala de reuniones puede cambiar la contraseña.

7. Grabaciones: La forma más fácil de grabar es transmitir la conferencia en directo a YouTube y acceder a la grabación allí. Las implementaciones de Jitsi Meet autoinstaladas necesitarán configurar

Jibri para hacer esto. La otra forma es conectar Dropbox con Jitsi meet y guardar el vídeo en el Dropbox.

Kinly and StarLeaf

Kinly

Fuente: https://www.kinly.com/privacy/

¿Quién es el responsable del tratamiento de datos?

1. Kinly enumera todas las entidades que son responsables del tratamiento en el Reino Unido, Noruega, Estados Unidos y los Países Bajos (pero no en Singapur). La Declaración de Privacidad advierte que los controladores de datos son específicos de cada país.

2. En el Reino Unido, los responsables del tratamiento son: Kinly Ltd The Video Conference Bureau Ltd Vision Connected United Kingdom Ltd In the US, the data controller is: Kinly Inc

3. En los Países Bajos, los responsables del tratamiento de datos son: Kinly Netherlands B.V. MK2 Audiovisueel B.V. MK2 Audiovisueel Verhuur B.V. MK2 Group B.V.

4. En Noruega, los responsables del tratamiento de datos son: Kinly AS VCV Nordics AS Viju AS

5. El documento de Seguridad en la Nube de Kinly, establece que Kinly también tiene múltiples Puntos de Presencia (PoP) en todo el mundo. Estos están alojados en centros de datos gestionados por proveedores de servicios, Google Cloud Platform, IBM Cloud y Baseform. Kinly afirma que el cliente puede elegir qué PoP quiere utilizar (debido a los diferentes requisitos normativos y políticos).

¿Dónde se almacenan los datos?

1. Aunque la declaración de privacidad está redactada de forma sencilla (lo que facilita su lectura), resulta confusa a la hora de determinar dónde almacena realmente Kinly sus datos.

2. La Declaración de Privacidad informa de que "el alojamiento y el almacenamiento de sus datos se realiza en centros de datos situados en el Reino Unido, Países Bajos, Noruega y Estados Unidos. Utilizamos proveedores de terceros para almacenar esta información y tenemos un acuerdo con ellos que protege su información."

3. Sin embargo, según el documento "Seguridad en la Nube de Kinly", todos los datos almacenados por el servicio son manejados por el centro de datos gestionado por Kinly Cloud con certificación ISO27001 en Oslo, Noruega, o en los centros de datos de Google Cloud con encriptación en reposo para todos los datos.

4. Además, la seguridad en los documentos de Kinly Cloud establece que los PoP están situados en los centros de datos Frankfurt, Singapur, Finlandia y Sao Paolo no figuran en la Declaración de Privacidad como Centros de Datos y por lo tanto, no toda la información puede ser almacenada en los Centros de Datos, como sugiere la Declaración de Política.

5. El documento de Seguridad en la Nube de Kinly también afirma que sólo el personal autorizado puede acceder al centro de datos de Oslo, Noruega. Sin embargo, no hay ninguna definición de "personal".

Duración del almacenamiento

1. Kinly es imprecisa a la hora de identificar el tiempo que almacena los datos. El Aviso de Privacidad afirma que "Kinly no almacena los datos personales más tiempo del necesario para los fines para los que se tratan".

2. Afirma que "en general, nuestro objetivo es conservar los datos personales de los clientes/proveedores durante no más de dos (2) años, a menos que se aplique un periodo de conservación obligatorio más largo o más corto se aplique o la retención de los datos personales específicos sea necesaria".

3. Afirma que no conservará los datos durante más tiempo del que permite la legislación/GDPR.

¿Cuáles son los aspectos más importantes en los términos y condiciones de la plataforma?

1. No hemos podido encontrar los términos y condiciones de uso de Kinly en Europa.

2. Los únicos términos y condiciones accesibles son los términos y condiciones de venta (EE.UU.) de Kinly Inc (controlador de datos de EE.UU.) - https://www.kinly.com/kinly-inc-termsand-conditions-of-sale . Esto parece ser un contrato bastante estándar sin mención específica de información sobre el almacenamiento de datos o información.

¿En qué medida los proveedores de la plataforma venden o comparten los datos personales?

1. En el seno de Kinly, los datos personales sólo están a disposición de los empleados que deben tratarlos para alcanzar los objetivos establecidos para el tratamiento de datos.

2. Sin embargo, también puede compartir los datos con terceros, ya sea para cumplir un contrato o para satisfacer una obligación legal a la que está sujeta.

3. Kinly comparte datos personales con los siguientes terceros: proveedores de sistemas informáticos, procesadores, contables, aseguradores, asesores jurídicos externos, reguladores, empresas afiliadas, proveedores de servicios de terceros, socios publicitarios.

5. ¿A qué vigilancia podrían estar expuestos los datos en poder de los proveedores de la plataforma?

6. Como empresa, Kinly es propiedad de Avedon Capital Partners, con sede en los Países Bajos.

7. Sin embargo, las operaciones de Kinly incluyen la transferencia internacional de datos entre otras empresas del grupo o esta parte. Por ello, Kinly está ubicada en el Reino Unido, Noruega, Países Bajos y Singapur. El alojamiento y almacenamiento de datos se realiza en centros de datos ubicados en el Reino Unido, Países Bajos, Noruega y Estados Unidos.

8. Por lo tanto, está sujeto a las leyes de los países donde se almacenan los datos.

9. Kinly utiliza proveedores terceros para almacenar esta información y tiene acuerdos pertinentes para proteger los datos personales.

10. Para las transferencias internacionales de datos dentro de sus empresas, Kinly utiliza Cláusulas Contractuales Tipo.

¿Quién es el responsable del tratamiento de datos?

1. El responsable del tratamiento es la parte que celebra un Acuerdo de Servicio con StarLeaf Ltd (que es un procesador) registrado en el Reino Unido. Los términos se establecen en el Anexo de Procesamiento de Datos: https://318jud367y2743qanus941sz-wpengine.netdnassl.com/wp-content/uploads/guides/starleaf_dpa_v5.4.pdf .

2. Si la suscripción a StarLeaf se compró a través de un socio o revendedor, StarLeaf recibió esa información a través de esa agencia. El revendedor y el socio trabajan con StarLeaf para asegurar que el servicio pueda ser activado, y actúan como Controlador de Datos ("Controlador") mientras que StarLeaf actúa como Procesador de Datos ("Procesador").

3. StarLeaf también declara que "también puede recopilar información sobre el uso del servicio que genera su suscripción a StarLeaf. Estos datos son útiles para las actividades de operaciones de servicio, como la resolución de problemas, el diagnóstico y las tendencias de capacidad".

4. La política de privacidad incluye los detalles del Oficial de Protección de Datos (DPO) que está registrado en la Oficina de Comisionados de Información del Reino Unido (ICO)

1. Several legal mechanisms are employed to facilitate international data transfers. When using other processors located in the United States, StarLeaf ensures it is certified under the EU-U.S. Privacy Shield Framework, providing a level of protection in line with EU data protection law. This includes processors such as Google, MailChimp, Freshdesk, Salesforce, Plivo, Twilio, Sendgrid and AWS.

2. StarLeaf also monitors other developing regulations that will require non-EU international transfer mechanisms, and states it is committed to maintaining lawful compliance with all such applicable laws.
3. StarLeaf acknowledges third party software that is used in its products: https://support.starleaf.com/legal-information/third-party-acknowledgements/.

¿En qué medida los proveedores de la plataforma venden o comparten los datos personales?

1. StarLeaf asegura que no utiliza ni comparte la información personal de ninguna otra manera más allá de lo que está escrito en su política de privacidad. También aseguran que no venden información personal a nadie, incluyendo pero no limitándose a terceros para su propio uso de marketing.

2. 'Como procesador de datos, StarLeaf está actuando bajo las instrucciones del controlador de datos, y puede compartir sus datos con el controlador en apoyo de su servicio. El responsable del tratamiento tiene acceso administrativo al portal de StarLeaf, y puede acceder a los registros de detalles de las llamadas con el fin de solucionar problemas, realizar diagnósticos, gestionar la capacidad, facturar y

elaborar informes. Cabe señalar que el contenido de sus reuniones de vídeo no se comparte con nadie, y esta capacidad no existe en el portal administrativo.

3. Es importante destacar que StarLeaf afirma que en los casos en que la suscripción al servicio incluye la capacidad de grabación de conferencias, se integra con su socio Media Network Services AS (MNS) en Oslo, Noruega, para proporcionar ese servicio. Una copia de la política de privacidad de MNS se puede leer aquí: https://www.mns.vc/privacy/. 4. La política de privacidad de MNS establece que ésta puede aparecer tanto como controlador (en los casos en los que los servicios fueron comprados directamente con ellos) como procesador (si el servicio fue comprado a través de un proveedor de servicios o revendedor).

5. StarLeaf también puede compartir datos con sus subprocesadores que facilitan la prestación de su servicio, entre los que se encuentran G-Suite, MailChimp, Freshdesk, Salesforce, Pardot, Plivo, Twilio y Sendgrid. StarLeaf afirma que "Para cada entidad, existe un acuerdo de procesamiento de datos entre StarLeaf y el subprocesador, con términos de flujo descendente coincidentes que esbozan garantías suficientes de salvaguardias técnicas para la protección de la información personal".

¿A qué vigilancia podrían estar expuestos los datos en poder de los proveedores de la plataforma?

1. StarLeaf puede estar sujeto a las leyes de vigilancia de varios países, dependiendo de dónde se encuentren los datos.

2. StarLeaf afirma que el contenido de las llamadas no puede ser consultado por sus empleados ni por terceros: https://support.starleaf.com/legalinformation/starleaf-privacy-notice/. Además, "las llamadas no se vigilan ni se graban, excepto los mensajes de videomail y de voz, y las llamadas que son explícitamente grabadas y guardadas por nuestros clientes utilizando los productos de servicios de grabación de StarLeaf". Nadie ajeno a StarLeaf puede acceder a ellas.

Messenger Video

Para el servicio de vídeo de Messenger, se remite al usuario a la Política de Datos con fecha de abril de 2018 que es común para Facebook, Instagram, Messenger y otros productos y funciones ofrecidos por Facebook.

1. QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE DATOS

El responsable del tratamiento de datos es Facebook Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublín 2 Irlanda

2. DÓNDE SE ALMACENAN LOS DATOS

La información controlada por Facebook Ireland se transferirá o transmitirá a Estados Unidos o a otros países, o se almacenará y procesará en ellos, para los fines descritos en la Política de Datos. Los datos se almacenan hasta que dejan de ser necesarios para prestar los servicios y productos de Facebook o hasta que se elimina la cuenta del usuario, lo que ocurra primero. Se trata de una determinación caso por caso que depende de aspectos como la naturaleza de los datos, la razón por la que se recogen y procesan, y las necesidades de retención legales u operativas pertinentes. Por ejemplo, cuando el usuario busca algo en Facebook, puede acceder a esa consulta y eliminarla del historial de búsqueda en cualquier momento, pero el registro de esa búsqueda se elimina después de seis meses. Si el usuario presenta una copia de un documento de identidad con fotografía válida a efectos de verificación de la cuenta, Facebook elimina esa copia 30 días después de su presentación. Cuando se elimina la cuenta, Facebook borra las cosas que el usuario ha publicado, como fotos y actualizaciones de estado, y los usuarios no podrán recuperar esta información más adelante. La información que otros han compartido sobre el usuario no forma parte de la cuenta del usuario y no se eliminará. Si los usuarios no quieren eliminar su cuenta pero quieren dejar de usar temporalmente los Productos, pueden desactivar su cuenta en su lugar.

3. ¿CUÁLES SON LOS ASPECTOS MÁS IMPORTANTES EN LOS TÉRMINOS Y CONDICIONES DE LA PLATAFORMA?

I. En la Política de Datos se hace una amplia referencia a la información y los datos recogidos por los Productos de Facebook y cómo se utiliza esta información, es decir, la información y el contenido proporcionado por el usuario, las redes y las conexiones, el uso, las transacciones, la información del dispositivo, etc.

II. Reconocimiento facial: Si el usuario lo activa, FB utiliza la tecnología de reconocimiento facial para reconocer al usuario en fotos, vídeos y experiencias de cámara. Las plantillas de reconocimiento facial que crea FB son datos con protección especial según la legislación de la UE.

III. Facebook e Instagram comparten infraestructura, sistemas y tecnología con otras empresas de Facebook (entre las que se encuentran WhatsApp y Oculus) con el objetivo de ofrecer una experiencia innovadora, relevante, coherente y segura en todos los productos de la empresa Facebook. También procesan información sobre los usuarios en todas las empresas de Facebook para estos fines, según lo permitido por la legislación aplicable y de acuerdo con sus condiciones y políticas. Por ejemplo,

procesan información de WhatsApp sobre cuentas que envían spam en su servicio para poder tomar las medidas adecuadas contra esas cuentas en Facebook, Instagram o Messenger. También trabajan para entender cómo la gente usa e interactúa con los productos de la empresa Facebook, como por ejemplo, para entender el número de usuarios únicos en los diferentes productos de la empresa Facebook.

4. ¿EN QUÉ MEDIDA LOS PROVEEDORES DE LA PLATAFORMA VENDEN O COMPARTEN DATOS PERSONALES?

FB utiliza cláusulas contractuales estándar aprobadas por la Comisión Europea y se basa en las decisiones de adecuación de países de la Comisión Europea, según corresponda, para las transferencias de datos del EEE a Estados Unidos y otros países. Facebook advierte de la visibilidad de los datos personales compartidos por el usuario o por otros en la red social del usuario. Los dispositivos y sistemas operativos que ofrezcan versiones nativas de Facebook e Instagram (es decir, en los que FB/Insta no hayan desarrollado sus propias aplicaciones internas) tendrán acceso a toda la información que los usuarios decidan compartir con ellos, incluida la información que los amigos de los usuarios compartan con ellos, con el fin de ofrecer las funciones principales de FB/Insta a los usuarios. Según se informa, FB está en proceso de restringir aún más el acceso a los datos de los desarrolladores para ayudar a prevenir el abuso. Por ejemplo, FB eliminará el acceso de los desarrolladores a los datos de Facebook e Instagram de un usuario si este no ha utilizado su aplicación en 3 meses, y FB está cambiando el inicio de sesión, por lo que en la próxima versión, FB reducirá los datos que una aplicación puede solicitar sin revisión de la aplicación para incluir solo el nombre, el nombre de usuario y la biografía de Instagram, la foto de perfil y la dirección de correo electrónico. Solicitar cualquier otro dato requerirá la aprobación de FB. Aparte de la información pública y el contenido compartido por los usuarios, la política de datos de FB estipula los siguientes casos de transferencia de información a terceros:

I. Nuevo propietario. Si la propiedad o el control de todos o parte de los productos o activos de la FB cambia, la FB puede transferir la información personal al nuevo propietario.

II. Compartir con terceros asociados. FB trabaja con terceros asociados que ayudan a proporcionar y mejorar los productos de FB o que utilizan las herramientas de empresa de Facebook para hacer crecer sus negocios. FB no vende ninguna información de los usuarios a nadie, y afirma que nunca lo hará. FB también impone restricciones estrictas sobre cómo sus socios pueden usar y divulgar los datos que FB proporciona. Los tipos de terceros con los que FB comparte información son los siguientes:

(a) Socios que utilizan los servicios de análisis de FB. FB proporciona estadísticas y datos agregados que ayudan a las personas y a las empresas a entender cómo la gente participa en sus publicaciones, listados, páginas, vídeos y otros contenidos dentro y fuera de los productos de Facebook. Por ejemplo, los administradores de páginas y perfiles empresariales de Instagram reciben información sobre el número de personas o cuentas que han visto, reaccionado o comentado sus publicaciones, así como información demográfica agregada y de otro tipo que les ayuda a comprender las interacciones con su página o cuenta.

(b) Anunciantes. FB proporciona a los anunciantes informes sobre el tipo de personas que ven sus anuncios y el rendimiento de los mismos, pero FB no comparte información que identifique personalmente al usuario (información como el nombre o la dirección de correo electrónico que por sí misma pueda utilizarse para ponerse en contacto con el usuario o que

identifique quién es el usuario) a menos que el usuario dé su permiso. Por ejemplo, FB proporciona información demográfica y de intereses generales a los anunciantes (por ejemplo, que un anuncio fue visto por una mujer de entre 25 y 34 años que vive en Madrid y le gusta la ingeniería de software) para ayudarles a entender mejor a su audiencia. FB también confirma qué anuncios de Facebook llevaron al usuario a realizar una compra o una acción con un anunciante.

c) Socios de medición. FB comparte información sobre los usuarios con empresas que la agregan para proporcionar informes de análisis y medición a los socios de FB.

(d) Socios que ofrecen bienes y servicios en Productos FB. Cuando el usuario se suscribe para recibir contenido premium, o compra algo a un vendedor en Productos FB, el creador de contenido o el vendedor pueden recibir la información pública del usuario y otra información que el usuario comparte con ellos, así como la información necesaria para completar la transacción, incluyendo los detalles de envío y contacto.

(e) Vendedores y proveedores de servicios. FB proporciona información y contenido a vendedores y proveedores de servicios que apoyan el negocio de FB, por ejemplo, proporcionando servicios de infraestructura técnica, analizando cómo se utilizan los Productos de FB, proporcionando servicio al cliente, facilitando los pagos o realizando encuestas.

(f) Investigadores y académicos. La FB también proporciona información y contenido a socios investigadores y académicos para que realicen investigaciones que avancen en la erudición y la innovación que apoyen el negocio o la misión de la FB, y mejoren el descubrimiento y la innovación en temas de bienestar social general, avance tecnológico, interés público, salud y bienestar.

(g) Solicitudes legales o de cumplimiento de la ley. FB accede, conserva y comparte la información de los usuarios con los reguladores, las fuerzas de seguridad u otros: (i) En respuesta a una solicitud legal, si la FB cree de buena fe que la ley le obliga a hacerlo. La FB también puede responder a solicitudes legales cuando cree de buena fe que la respuesta es requerida por la ley en esa jurisdicción, afecta a los usuarios en esa jurisdicción y es consistente con los estándares reconocidos internacionalmente. (ii) Cuando la FB crea de buena fe que es necesario para: detectar, prevenir y abordar el fraude, el uso no autorizado de los Productos, las infracciones de las condiciones o políticas de la FB o cualquier otra actividad perjudicial o ilegal; para proteger a la FB (incluidos sus derechos, propiedad o Productos), al usuario o a otros, incluso como parte de investigaciones o consultas reglamentarias; o para evitar la muerte o un daño corporal inminente. Por ejemplo, si es pertinente, la FB proporciona información y recibe información de terceros asociados sobre la fiabilidad de la cuenta del usuario para prevenir el fraude, el abuso y otras actividades perjudiciales dentro y fuera de los Productos de la FB.

(h) Se puede acceder a la información que FB recibe sobre los usuarios (incluidos los datos de las transacciones financieras relacionadas con las compras realizadas con Facebook) y conservarla durante un período prolongado cuando sea objeto de una solicitud u obligación legal, una investigación gubernamental o investigaciones sobre posibles infracciones de nuestras condiciones o políticas, o bien para evitar daños. También se conserva la información de las cuentas inhabilitadas por incumplimiento de las condiciones durante al menos un año para evitar que se repitan los abusos u otras infracciones de las condiciones.

Skype, Skype for Business y Poly.com

Skype y Skype for Business

Software operado por Microsoft. Skype está destinado al uso de los consumidores, mientras que Skype for Business, como su nombre indica, está destinado al uso profesional. Para ambos, el documento básico de privacidad es la Declaración de Privacidad de Microsoft. En ella se incluyen los términos generales del enfoque de Microsoft sobre el uso de datos y los detalles específicos de los productos, incluido Skype. La sección de productos para empresas y desarrolladores de la declaración de privacidad se aplica al uso de Skype for Business (véase también más abajo). A continuación, el Contrato de Servicios de Microsoft se aplica a las condiciones de uso de los productos de Microsoft, incluidas las condiciones específicas de Skype. Hay que tener en cuenta que "Microsoft® Teams sustituye a Skype for Business Online como solución profesional de reuniones en línea de Microsoft "2. Para Teams, se hace referencia al análisis anterior.

¿Quién es el responsable del tratamiento de datos?

Para quienes se encuentran en el Espacio Económico Europeo, el Reino Unido y Suiza (véase la sección de contacto de la declaración de privacidad):

Microsoft Ireland Operations Limited One Microsoft Place,

South County Business Park, Leopardstown,

Dublin 18, Ireland. Telephone: +353 1 706 3117.

¿Dónde se almacenan los datos?

Declaración de privacidad: Los datos personales recogidos por Microsoft pueden ser almacenados y procesados en su región, en los Estados Unidos y en cualquier otro país donde Microsoft o sus filiales, subsidiarias o proveedores de servicios tengan instalaciones. Microsoft mantiene importantes centros de datos en Australia, Austria, Brasil, Canadá, Chile, Finlandia, Francia, Alemania, Hong Kong, India, Irlanda, Japón, Corea, Luxemburgo, Malasia, Países Bajos, Singapur, Sudáfrica, Reino Unido y Estados Unidos. Normalmente, la ubicación de almacenamiento principal se encuentra en la región del cliente o en Estados Unidos, a menudo con una copia de seguridad en un centro de datos de otra región. Las ubicaciones de almacenamiento se eligen para que funcionen de forma eficiente, para mejorar el rendimiento y para crear redundancias con el fin de proteger los datos en caso de interrupción u otro problema. Tomamos medidas para garantizar que los datos que recogemos en virtud de esta declaración de privacidad se procesan de acuerdo con las disposiciones de esta declaración y los requisitos de la legislación aplicable dondequiera que se encuentren los datos.

Transferimos datos personales desde el Espacio Económico Europeo, el Reino Unido y Suiza a otros países, algunos de los cuales todavía no han sido considerados por la Comisión Europea como países con un nivel adecuado de protección de datos. Por ejemplo, es posible que sus leyes no le garanticen

los mismos derechos, o que no haya una autoridad supervisora de la privacidad allí que sea capaz de atender sus quejas. Cuando realizamos este tipo de transferencias, utilizamos una serie de mecanismos legales, incluidos los contratos, para ayudar a garantizar que sus derechos y protecciones viajen con sus datos. Para obtener más información sobre las decisiones de la Comisión Europea sobre la adecuación de la protección de los datos personales en los países en los que Microsoft procesa datos personales, consulte este artículo en el sitio web de la Comisión Europea.

Microsoft Corporation cumple con el Marco del Escudo de Privacidad UE-EE.UU. y el Marco del Escudo de Privacidad Suiza-EE.UU. según lo establecido por el Departamento de Comercio de EE.UU. en relación con la recopilación, el uso y la retención de información personal transferida desde la Unión Europea, el Reino Unido y Suiza a los Estados Unidos. Microsoft Corporation ha certificado ante el Departamento de Comercio que se adhiere a los Principios del Escudo de Privacidad. Si los agentes de terceros procesan los datos personales en nuestro nombre de manera incompatible con los principios de cualquiera de los dos marcos del Escudo de Privacidad, seguimos siendo responsables, a menos que demostremos que no somos responsables del hecho que originó el daño. Las filiales estadounidenses controladas de Microsoft Corporation, identificadas en nuestra presentación de autocertificación, también se adhieren a los Principios del Escudo de Privacidad; para más información, consulte la lista de entidades o filiales estadounidenses de Microsoft que se adhieren a los Principios del Escudo de Privacidad.

Si hay algún conflicto entre los términos de esta política de privacidad y los Principios del Escudo de Privacidad, los Principios del Escudo de Privacidad prevalecerán. Para obtener más información sobre el programa del Escudo de Privacidad, y para ver nuestra certificación, visite el sitio web del Escudo de Privacidad.

Si tiene alguna pregunta o queja relacionada con la participación de Microsoft en el Escudo de Privacidad UE-EE.UU. o Suiza-EE.UU., le animamos a que se ponga en contacto con nosotros a través de nuestro formulario web. Para cualquier queja relacionada con los marcos del Escudo de Privacidad que Microsoft no pueda resolver directamente, hemos optado por cooperar con la Autoridad de Protección de Datos de la UE correspondiente, o con un panel establecido por las autoridades europeas de protección de datos, para resolver las disputas con los individuos de la UE, y con el Comisionado Federal de Protección de Datos e Información de Suiza (FDPIC) para resolver las disputas con los individuos de Suiza. Póngase en contacto con nosotros si desea que le indiquemos los contactos de su autoridad de protección de datos. Como se explica con más detalle en los Principios del Escudo de Privacidad, el arbitraje vinculante está disponible para abordar las quejas residuales que no se resuelven por otros medios. Microsoft está sujeta a los poderes de investigación y aplicación de la Comisión Federal de Comercio de Estados Unidos (FTC).

3. ¿Cuáles son los aspectos más importantes en los términos y condiciones de la plataforma?

Los datos pueden ser almacenados en EE.UU. y accedidos por LEA

4. ¿En qué medida los proveedores de la plataforma venden o comparten los datos personales?

Declaración de privacidad: Sección "Razones por las que compartimos los datos personales": Compartimos sus datos personales con su consentimiento o según sea necesario para completar cualquier transacción o proporcionar cualquier producto que haya solicitado o autorizado. Por ejemplo, compartimos tu contenido con terceros cuando nos lo indicas, como cuando envías un correo

electrónico a un amigo, compartes fotos y documentos en OneDrive o vinculas cuentas con otro servicio. Si utiliza un producto de Microsoft proporcionado por una organización a la que está afiliado, como un empleador o una escuela, o utiliza una dirección de correo electrónico proporcionada por dicha organización para acceder a los productos de Microsoft, compartimos ciertos datos, como los datos de interacción y los datos de diagnóstico, para permitir que su organización gestione los productos. Cuando proporcione datos de pago para realizar una compra, compartiremos los datos de pago con los bancos y otras entidades que procesan las transacciones de pago o proporcionan otros servicios financieros, y para la prevención del fraude y la reducción del riesgo crediticio.

Además, compartimos datos personales entre las filiales y subsidiarias controladas por Microsoft. También compartimos datos personales con proveedores o agentes que trabajan en nuestro nombre para los fines descritos en esta declaración. Por ejemplo, las empresas que hemos contratado para que proporcionen asistencia al servicio de atención al cliente o ayuden a proteger y asegurar nuestros sistemas y servicios pueden necesitar acceso a los datos personales para realizar esas funciones. En estos casos, estas empresas deben respetar nuestros requisitos de seguridad y privacidad de datos y no pueden utilizar los datos personales que reciben de nosotros para ningún otro fin. También podemos revelar datos personales como parte de una transacción corporativa, como una fusión o venta de activos.

Por último, retendremos, accederemos, transferiremos, divulgaremos y conservaremos los datos personales, incluido su contenido (como el contenido de sus correos electrónicos en Outlook.com, o los archivos de las carpetas privadas en OneDrive), cuando creamos de buena fe que es necesario hacerlo para

- Cumplir con la ley aplicable o responder a un proceso legal válido, incluso de las fuerzas del orden u otras agencias gubernamentales.

- Proteger a nuestros clientes, por ejemplo, para evitar el spam o los intentos de estafa a los usuarios de nuestros productos, o para ayudar a prevenir la pérdida de vidas o lesiones graves de cualquier persona.

- Operar y mantener la seguridad de nuestros productos, incluso para prevenir o detener un ataque a nuestros sistemas informáticos o redes.

- Proteger los derechos o la propiedad de Microsoft, incluida la aplicación de los términos que rigen el uso de los servicios; sin embargo, si recibimos información que indique que alguien está utilizando nuestros servicios para traficar con propiedad intelectual o física robada de Microsoft, no inspeccionaremos el contenido privado de un cliente nosotros mismos, pero podemos remitir el asunto a las autoridades.

Declaración de privacidad - Detalles específicos del producto - Servicios de Internet para empresas (relevante para Skype for Business)

Para proporcionar los Servicios de Internet para Empresas, Microsoft utiliza los datos que usted proporciona (incluidos los Datos del Cliente, Datos Personales, Datos del Administrador, Datos de Pago y Datos de Soporte) y los datos que Microsoft recopila o genera asociados con su uso de los Servicios de Internet para Empresas. Procesamos los datos tal y como se describe en las Condiciones de los servicios en línea (OST) y en el Centro de confianza de Microsoft. Datos personales. El Cliente es el controlador de los Datos Personales y Microsoft es el procesador de dichos datos, excepto cuando (a) el Cliente actúa como procesador de los Datos Personales, en cuyo caso Microsoft es un

subprocesador, (b) Microsoft está procesando los Datos Personales para sus operaciones comerciales legítimas, en cuyo caso Microsoft es un controlador, o (c) se establece lo contrario en las CSO.

Microsoft es un controlador de Datos Personales cuando procesa Datos Personales para sus operaciones comerciales legítimas asociadas con la prestación del servicio, como la facturación y la preparación de facturas; la gestión de cuentas; la compensación; los informes financieros; la planificación empresarial y la estrategia de productos; la mejora de la funcionalidad básica para la accesibilidad, la privacidad y la eficiencia energética; y la lucha contra el fraude, la ciberdelincuencia y los ciberataques a los productos de Microsoft. Por lo general, agregamos los datos personales antes de utilizarlos para nuestras operaciones comerciales legítimas, eliminando la posibilidad de identificar a personas concretas. Utilizamos los datos personales en la forma menos identificable que permita el procesamiento necesario para las operaciones comerciales legítimas. Datos del administrador. Los Datos del Administrador son la información proporcionada a Microsoft durante el registro, la compra o la administración de los Servicios Online para Empresas.

Utilizamos los Datos del administrador para proporcionar los Servicios de empresa en línea, completar las transacciones, dar servicio a la cuenta, detectar y prevenir el fraude y cumplir con nuestras obligaciones legales. Los Datos del Administrador incluyen el nombre, la dirección, el número de teléfono y la dirección de correo electrónico que usted proporciona, así como los datos de uso agregados relacionados con su cuenta, como los controles que selecciona. Los Datos del administrador también incluyen la información de contacto de sus colegas y amigos si usted acepta proporcionársela a Microsoft con el propósito limitado de enviarles una invitación para utilizar los Servicios en línea para empresas; nos ponemos en contacto con esas personas con comunicaciones que incluyen información sobre usted, como su nombre y la foto de su perfil.

Según sea necesario, utilizamos los Datos del administrador para ponernos en contacto con usted y proporcionarle información sobre su cuenta, suscripciones, facturación y actualizaciones de los Servicios Enterprise Online, incluyendo información sobre nuevas características, seguridad u otros problemas técnicos. También nos ponemos en contacto con usted en relación con las consultas de terceros que recibimos sobre el uso de los Servicios de Empresa en Línea, tal y como se describe en su acuerdo. Usted no puede darse de baja de estas comunicaciones no promocionales. También podemos ponernos en contacto con usted en relación con información y ofertas sobre otros productos y servicios, o compartir su información de contacto con los socios de Microsoft. Cuando dicho socio disponga de servicios o soluciones específicas para satisfacer sus necesidades, o para optimizar su uso de los Enterprise Online Services, podremos compartir con el socio información limitada y agregada sobre la cuenta de su organización. Microsoft no compartirá su información confidencial o de contacto con el socio autorizado a menos que tengamos derechos suficientes para hacerlo. Puede gestionar sus preferencias de contacto o actualizar su información en el perfil de su cuenta.

Datos de pago. Utilizamos los datos de pago para completar las transacciones, así como para detectar y prevenir el fraude. Datos de soporte técnico.

Los clientes proporcionan o autorizan a Microsoft a recopilar datos en relación con la obtención de asistencia técnica para los Enterprise Online Services. Procesamos los datos de soporte para proporcionar soporte técnico y como se describe en el TSO. Algunos Servicios de Empresa en Línea requieren, o son mejorados por, la instalación de software local (por ejemplo, agentes, aplicaciones de administración de dispositivos) en un dispositivo.

Bajo su dirección, el software local puede transmitir (i) datos, que pueden incluir Datos del cliente, desde un dispositivo o aparato hacia o desde los Servicios de Empresa en Línea; o (ii) registros o

informes de errores a Microsoft para la resolución de problemas. Los Servicios Enterprise Online, incluido el software local, recopilan datos de dispositivos y de uso que se transmiten a Microsoft y se analizan para mejorar la calidad, la seguridad y la integridad de nuestros productos. Los Servicios de búsqueda de Bing, tal y como se definen en el TSO, utilizan datos como las consultas de búsqueda, tal y como se describe en la sección de Bing de esta declaración de privacidad.

Poly.com

Poly es un proveedor de hardware y servicios de herramientas de telefonía y videoconferencia. Por ejemplo, el Servicio de Tribunales, Fiscales y Prisiones de la República Checa utiliza Poly.com para sus necesidades de videoconferencia, incluidas las audiencias judiciales. Para cuestiones de privacidad se aplica la política general de privacidad y los libros blancos específicos de cada producto.

1. **¿Quién es el controlador de datos?**
   Plantronics, Inc.,
   345 Encinal Street Santa Cruz,
   California 95060 USA

2. **¿Dónde se almacenan los datos?**
   Usted acepta que toda la información personal recopilada por Poly puede ser transferida, procesada y almacenada en cualquier parte del mundo, incluyendo, pero sin limitarse a, los Estados Unidos, Australia, Singapur o Irlanda, así como la Unión Europea, en la nube, en nuestros servidores, en los servidores de nuestras filiales o en los servidores de nuestros proveedores de servicios, las empresas de nuestro grupo y los socios que puedan operar en todo el mundo

3. **¿Cuáles son los aspectos más importantes en los términos y condiciones de la plataforma?**

En lo que respecta a la plataforma Polycom RealPresence DMA, que es la que utilizan las autoridades judiciales checas, véase el libro blanco sobre seguridad y privacidad. La página 4-6 se refiere al tratamiento de datos, su finalidad, el almacenamiento y la protección de los mismos. En resumen, RealPresence DMA no accede a los datos de ningún cliente, excepto cuando es necesario para habilitar las funciones que ofrece la aplicación. Dado que estos sistemas se despliegan en el entorno del cliente, es responsabilidad de éste proteger la privacidad de los datos. RealPresence DMA recopila y procesa registros que contienen la siguiente información: Datos del dispositivo, Datos de llamadas y conferencias.

Poly recopila datos para entender cómo los clientes utilizan el sistema RealPresence DMA. El sistema envía los datos de uso una vez por hora a través de una conexión segura (TLS) (puerto 8443) a un punto de recogida de Poly. El administrador puede desactivar o activar la recogida de datos. Todos los datos se anonimizan antes de ser enviados y, por lo tanto, se eliminan los datos de identificación. Poly no carga ningún dato personal. La analítica excluye toda información que identifique a personas individuales o los hábitos de un individuo.

Los datos analíticos se almacenan en Amazon Web Services (AWS). Actualmente, utilizamos centros de datos sólo en los Estados Unidos. Para transferir los datos personales de los clientes de la UE a los Estados Unidos, Poly utiliza un acuerdo de transferencia de datos intragrupo que incorpora las

cláusulas contractuales estándar de la UE como mecanismo de transferencia. Sólo el personal autorizado de Poly tiene acceso directo a los datos.

4. **¿En qué medida los proveedores de la plataforma venden o comparten los datos personales?**

De acuerdo con la política general de privacidad, Poly: Podemos compartir sus datos tal y como se describe en esta política de privacidad; por ejemplo, con terceros o proveedores de servicios, para cumplir con las obligaciones legales, para proteger y defender nuestros derechos y propiedad, o con su permiso.

Proveedores de servicios. De vez en cuando, podemos revelar sus datos personales a organizaciones que prestan servicios. Por ejemplo, para proporcionar un servicio de atención al cliente, entregar productos, enviar artículos, procesar tarjetas de crédito, para la investigación, el marketing, las valoraciones y reseñas de productos, el procesamiento de datos y para medir el uso de nuestros sitios. Sólo compartiremos la información personal necesaria para que estas empresas realicen el trabajo en nuestro nombre. Su información personal se proporcionará a estas organizaciones en virtud de un acuerdo escrito que les impida retener, utilizar o revelar la información personal por cualquier motivo que no sea el propósito de prestar servicios bajo las instrucciones de Poly, y con respecto a esa información, para mantenerla segura y actuar de manera coherente con los principios pertinentes articulados en esta política de privacidad.

Cumplimiento de la ley. Podemos revelar sus datos a cualquier organismo competente de aplicación de la ley, regulador, agencia gubernamental, tribunal u otro Tercero cuando creamos que la revelación es necesaria, por ejemplo, (i) como cuestión de ley o reglamento aplicable, (ii) para ejercer, establecer o defender nuestros derechos legales, o (iii) para proteger sus intereses vitales o los de cualquier otra persona. Socios de Poly. Si usted ha optado por recibir contactos de marketing directo de un socio de Poly, Poly revelará su información personal a los socios de Poly. Su información personal se proporcionará al socio de Poly sólo si éste se compromete a actuar de forma coherente con los principios pertinentes articulados en esta política de privacidad. Sin embargo, Poly le recomienda que revise la política de privacidad del socio, ya que sus prácticas de privacidad no son supervisadas ni controladas por Poly.

Fusiones y adquisiciones. Podemos revelar sus datos a un posible comprador (y a sus agentes y asesores) en relación con cualquier propuesta de compra, fusión o adquisición de cualquier parte de nuestro negocio, siempre que informemos al comprador de que debe utilizar sus Datos Personales únicamente para los fines expuestos en esta Política de Privacidad. Si Poly se ve involucrada en una fusión, adquisición o venta de todos o parte de sus activos, se le notificará por correo electrónico y/o mediante un aviso destacado en nuestros Sitios sobre cualquier cambio de propiedad.