# Política de Protección de Datos Personales
## treble.ai

En treble.ai, inc nos comprometemos a procesar los datos personales de forma segura y a respetar la privacidad de las personas afectadas.

| | |
|---|---|
| Versión No. y fecha de la última | v. 1.0. 16 de diciembre de 2020 |
| Aprobado por: | Sebastián Valencia, CEO de treble.ai, inc |
| Esta política se revisará anualmente o cada vez que se produzcan cambios en nuestro tratamiento de datos. | |

# Tabla de contenidos

# 1. Ámbito de aplicación y definiciones

1. **Alcance**. La presente Política de Protección de Datos Personales (la "**Política**") describe las normas internas de treble.ai, inc. para el tratamiento y la protección de datos personales. La Política se aplica a todas las entidades del grupo treble.ai, inc, incluidas treble.ai, inc y todas las demás subsidiarias del grupo, empleados y contratistas de las entidades ("**Nosotros**", "**nos**", "**nuestro**", "**treble.ai**"). La dirección de cada entidad es responsable en última instancia de la aplicación de esta política, así como de garantizar, a nivel de la entidad, que existan procedimientos adecuados y eficaces para su aplicación y la supervisión continua de su cumplimiento. A los efectos de esta Política, los empleados y contratistas se denominan conjuntamente "**Empleados**".

2. **Gerente de Privacidad**. Privacy Manager es un empleado de treble.ai responsable del cumplimiento de la protección de datos personales dentro de treble.ai (el "**Gerente de Privacidad**"). El Gerente de Privacidad es el encargado de cumplir con las obligaciones impuestas por esta Política y supervisar a los demás empleados, que están sujetos a esta Política, en cuanto a su adhesión a esta Política. El Responsable de Privacidad debe participar en todos los proyectos en una fase temprana para tener en cuenta los aspectos de protección de datos personales ya en la fase de planificación.

   El Gerente de Privacidad designado en treble.ai, inc es Daniel Martínez.

3. **Representante de la UE**. Como entidad que procesa datos personales de acuerdo con la legislación de la UE, pero ubicada fuera de la Unión Europea, treble.ai debe designar al representante dentro de uno de los Estados miembros de la UE. La función del representante es ser un punto de contacto para, entre otros, las autoridades de control y los interesados, en todas las cuestiones relacionadas con el tratamiento, con el fin de garantizar el cumplimiento del presente Reglamento.

   El representante designado de treble.ai, inc. en la UE es Maetzler Rechtsanwalts GmbH & Co KG.

## 4. **Definiciones**.

| | |
|---|---|
| **Autoridad de Supervisión** | significa una autoridad pública responsable de regular y supervisar la protección de datos personales con respecto a las actividades de treble.ai. |
| **Violación de datos** | significa una violación de la seguridad y/o confidencialidad que conduzca a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal a los Datos Personales transmitidos, almacenados o procesados de otro modo.<br>Esto incluye, entre otros, correos electrónicos enviados a una lista de destinatarios incorrecta o divulgada, una publicación ilegal de los Datos personales, pérdida o robo de registros físicos y acceso no autorizado a la información personal. |
| **D a t a Controlador** | se refiere a la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determine (tome una decisión) los fines y medios del tratamiento de Datos personales. |
| **Datos Procesador** | se refiere a una persona física o jurídica, autoridad pública, agencia u otro organismo que procesa los Datos personales en nombre del controlador de datos. |
| **Leyes de protección de datos** | se refiere a cualquier ley y norma legal sobre el uso y la protección de datos personales aplicable a las actividades de treble.ai, incluido, entre otros, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por la que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD) |
| **Solicitud del interesado (DSR)** | se refiere a cualquier solicitud del Interesado y relativa a sus datos personales y/o derechos del Interesado. |
| **Titular de los datos** | se refiere a una persona física, cuyos Datos personales procesamos. Los interesados incluyen, entre otros, usuarios, visitantes del sitio web, empleados, contratistas y socios de treble.ai. |
| **Datos personales** | se refiere a cualquier información relacionada con un Sujeto de Datos identificado o identificable; un Sujeto de Datos puede ser identificado por referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o la combinación de factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de ese Sujeto de Datos. |

| | |
|---|---|
| **Tratamiento** | se refiere a cualquier operación o conjunto de operaciones realizadas por treble.ai sobre Datos personales, como la recopilación, el registro, la organización, la estructuración, el almacenamiento, la adaptación o la alteración, la recuperación, la consulta, el uso, la divulgación por transmisión, la difusión o cualquier otra forma de puesta a disposición, la alineación o combinación, la restricción, la eliminación o la |
| **Cláusulas contractuales tipo** | se refiere a la Decisión de la Comisión Europea, de 5 de febrero de 2010, sobre cláusulas contractuales tipo para la transferencia de datos personales a procesadores establecidos en terceros países en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo |
| **Terceros** | se refiere a una persona física o jurídica que accede a los Datos personales para su posterior procesamiento y que no es un empleado, miembro o afiliado corporativo de treble.ai. Esta definición no se aplica a las personas físicas que prestan servicios a treble.ai como |
| **Usuario** | se refiere a un Sujeto de datos que utiliza nuestros servicios proporcionados en treble.ai sitio web. |

# 2. Principios de tratamiento de datos

2.1. Las actividades de tratamiento de treble.ai deben estar en consonancia con los principios especificados en la presente sección. El Responsable de Privacidad debe asegurarse de que la documentación de cumplimiento de treble.ai, así como las actividades de tratamiento de datos, cumplan con los principios de protección de datos.

2.2. Debemos procesar los Datos Personales de acuerdo con los siguientes principios:

2.2.1. De manera lícita, leal y transparente (**Licitud, equidad y transparencia**). Siempre contaremos con una base legal para el procesamiento (descrita en la Sección 3 de esta Política), recopilaremos la cantidad de datos adecuada para el propósito y las bases legales, y nos aseguraremos de que los Interesados estén al tanto del procesamiento;

2.2.2. Recopilados para fines específicos, explícitos y legítimos y no procesados posteriormente de una manera que sea incompatible con dichos fines (**Limitación de la finalidad**). No debemos procesar los Datos personales para los fines no especificados en nuestra documentación de cumplimiento sin obtener la aprobación específica del Administrador de Privacidad;

2.2.3. Adecuados, pertinentes y limitados a lo necesario para los fines para los que se tratan (**Minimización de datos**). Siempre nos aseguramos de que los datos que recopilamos no sean excesivos y estén limitados por la estricta necesidad;

2.2.4. Exactos y, en su caso, actualizados (**precisión)**. Nos esforzamos por eliminar los datos inexactos o falsos sobre los interesados y nos aseguramos de actualizar los datos. Los interesados pueden solicitarnos una corrección de los datos personales;

2.2.5. Conservados en una forma que permita la identificación de los Interesados durante no más tiempo del

necesario para los fines para los que se procesan los Datos personales (limitación del **período de almacenamiento**). Los períodos de almacenamiento deben limitarse según lo prescrito por las Leyes de Protección de Datos y esta Política; y

2.2.6. Tratar de manera que se garantice la seguridad adecuada de los Datos personales, incluida la protección contra el procesamiento no autorizado o ilegal y la pérdida, destrucción o daño accidental, utilizando medidas técnicas u organizativas adecuadas (**Confidencialidad, integridad y disponibilidad**).

**2.3. <u>Rendición de cuentas</u>**.

**2.3.1.** Podremos demostrar nuestro cumplimiento de las Leyes de Protección de Datos (**Principio de rendición de cuentas**). En particular, debemos garantizar y documentar todos los procedimientos, esfuerzos, consultas internas y externas pertinentes sobre la protección de datos personales, incluidos:

- el hecho de designar a una persona responsable del cumplimiento de la protección de datos de treble.ai;
- Desarrollos e implementación de avisos, políticas y procedimientos, tales como
  Aviso de Privacidad, esta política o el procedimiento de respuesta a la Violación de Datos;
- el hecho de la formación del personal sobre el cumplimiento de las leyes de protección de datos; y
- Evaluación, implementación y prueba de medidas de protección de datos organizativas y técnicas.

2.3.2. El Gerente de Privacidad debe mantener los Registros de actividades de procesamiento de treble.ai una vez que la empresa alcance un número de 250 empleados, hasta el día de hoy esto no se aplica. Es responsabilidad del Gerente de Privacidad actualizar este documento una vez que eso suceda. El Registro de actividades de tratamiento es un documento de responsabilidad que describe las actividades de tratamiento de datos personales de treble.ai, elaborado de conformidad con el art. 30 del RGPD (el "**Registros de actividades de tratamiento**"). Los Registros de actividades de tratamiento deberán mantener, al menos, la siguiente información sobre cada actividad de tratamiento:

- datos de contacto del treble.ai, del representante de la UE y, en su caso, del responsable de la protección de datos;
- el nombre de la actividad, sus fines y base jurídica junto con, en su caso, los intereses legítimos de treble.ai;
- los interesados y las categorías de datos personales afectados;
- plazos de conservación de los datos;
- descripción general de las medidas de seguridad aplicables;
- destinatarios, incluidos los corresponsables, encargados del tratamiento y contratistas implicados, así como el hecho de la transferencia internacional de datos con las garantías aplicadas a la transferencia;

- en su caso, una referencia a la evaluación de impacto del tratamiento de datos;
- en su caso, una referencia al registro de la violación de datos ocurrida en relación con los datos personales;
- Si treble.ai actúa como procesador de datos, la información que debe proporcionarse incluye los nombres y datos de contacto de los Controladores, el nombre y los datos de contacto del representante del Controlador (si corresponde), las categorías de procesamiento (actividades), los nombres de terceros países u organizaciones internacionales que

se transfieren datos personales a (si corresponde), salvaguardas para transferencias excepcionales de datos personales a terceros países u organizaciones internacionales (si corresponde) y descripción general de las medidas de seguridad técnicas y organizativas.

# 3. Acceso a los Datos Personales. Fundamentos y fines jurídicos

**3.1. <u>Fundamentos jurídicos</u>**.

3.1.1. Cada actividad de procesamiento debe tener uno de los motivos legales especificados en esta Sección para procesar los Datos personales. Si no contamos con ninguno de los descritos, no podemos recopilar ni seguir procesando los Datos Personales.

3.1.2. Si treble.ai tiene por objeto utilizar los datos personales para fines distintos de los especificados en la política de privacidad, el Responsable de Privacidad debe evaluar, determinar y, si es necesario, recopilar/registrar la base jurídica adecuada para ello.

3.1.3. **Ejecución del contrato**. Cuando treble.ai tenga un contrato con el interesado, p. ej. las condiciones de uso del sitio web o el contrato de trabajo, y el contrato requiere el suministro de datos personales por parte del interesado, la base jurídica aplicable será la ejecución del contrato.

3.1.4. **Consentimiento**. Para procesar los datos personales sobre la base del consentimiento, debemos obtener el consentimiento antes del Procesamiento y conservar la evidencia del consentimiento con los registros de los Datos Personales del Interesado. El Administrador de Privacidad debe asegurarse de que el consentimiento recopilado de los Interesados cumpla con los requisitos de las Leyes de Protección de Datos y esta Política. En particular, el Responsable de Privacidad debe asegurarse de que:

- el interesado debe ser libre de dar o negarse a dar su consentimiento.
- el consentimiento tiene la forma de una indicación activa del interesado, es decir, la casilla de verificación del consentimiento no debe estar premarcada para el usuario.
- la solicitud de consentimiento articula claramente los fines del procesamiento, y otra información especificada en la Subsección 6.2 está disponible para el Sujeto de datos.
- el interesado debe ser libre de dar su consentimiento o de revocarlo.

3.1.5. **Intereses legítimos**. Tenemos derecho a utilizar los datos personales en nuestro "interés legítimo". Los intereses pueden incluir los fines que estén justificados por la naturaleza de nuestras actividades comerciales, como el análisis de marketing de datos personales. Para que treble.ai utilizar los intereses legítimos como base jurídica para el tratamiento, el Responsable de Privacidad debe asegurarse de que:

- el interés legítimo en el tratamiento está claramente definido y registrado en la política de privacidad;

- se detectan los riesgos previstos para los derechos e intereses de los interesados. Los ejemplos de los riesgos se pueden encontrar en la Subsección 7.2.;
- los Interesados tienen expectativas razonables sobre el procesamiento y se toman medidas de protección adicionales para abordar los riesgos;
- sujeto a las condiciones de la Subsección 6.7 (Derecho de oposición al procesamiento), el Interesado tiene la oportunidad de optar por no participar en el procesamiento por los intereses legítimos descritos.

Si al menos una de las condiciones anteriores no es cumplida por treble.ai, el Responsable de Privacidad debe elegir y proponer un fundamento jurídico diferente para el tratamiento, como el consentimiento.

**3.1.6. Cumplimiento legal e interés público**. Además de los motivos especificados anteriormente, es posible que las leyes de la Unión Europea o las leyes de los Estados miembros de la UE nos soliciten el procesamiento de Datos personales de nuestros Usuarios. Por ejemplo, se nos puede exigir que recopilemos, analicemos y supervisemos la información de los Usuarios para cumplir con las leyes financieras o laborales.

Siempre que tengamos una obligación de este tipo, debemos asegurarnos de que:

- Tratamos los datos personales estrictamente de acuerdo con los requisitos legales pertinentes;
- no utilizamos ni almacenamos los Datos personales recopilados para otros fines que no sean el cumplimiento legal; y
- los Interesados son informados de manera adecuada y oportuna sobre nuestras obligaciones, alcance y condiciones del procesamiento de datos personales.

**Importante:** Cuando treble.ai tenga los requisitos legales de otro país para procesar datos personales, el Gerente de Privacidad debe proponer el uso de otro fundamento legal para el procesamiento en virtud de las Leyes de Protección de Datos, como los intereses legítimos o el consentimiento.

## 3.2. Acceso a los Datos Personales.

3.2.1. Los empleados deben tener acceso a los datos personales en función de la "necesidad de conocerlos". Solo se puede acceder a los datos si es estrictamente necesario para realizar una de las actividades especificadas en los Registros de actividades de procesamiento. Los empleados y contratistas tendrán acceso a los Datos Personales solo si tienen las credenciales necesarias para ello.

3.2.2. Los jefes de los departamentos de treble.ai son responsables del acceso y tratamiento de los datos personales por parte de sus empleados. Los jefes deben mantener la lista de los empleados que tienen derecho a acceder y procesar los datos personales. El Responsable de Privacidad tendrá derecho a revisar la lista y, cuando sea necesario, solicitar las modificaciones para cumplir con los requisitos de esta Política.

3.2.3. Los jefes de los departamentos de treble.ai deben asegurarse de que los empleados bajo su supervisión conozcan las Leyes de Protección de Datos y cumplan con las normas establecidas en esta Política. Para asegurarnos de que nuestros empleados puedan cumplir con los requisitos de protección de datos, debemos proporcionarles una formación adecuada en materia de protección de datos.

3.2.4. Todos los empleados que accedan a los datos personales deberán mantener una estricta confidencialidad con respecto a los datos a los que accedan. Los empleados que accedan a los datos personales deben utilizar únicamente los medios (software, locales, etc.) para el tratamiento que hayan sido prescritos por

treble.ai. Los datos no deben divulgarse ni ponerse a disposición de otro modo fuera de las instrucciones de gestión.

3.2.5. Los empleados dentro de su competencia deben ayudar a los representantes de treble.ai, incluido el Gerente de Privacidad, en cualquier esfuerzo relacionado con el cumplimiento de las Leyes de Protección de Datos y/o esta Política.

3.2.6. Cuando un empleado detecta o cree que hay una actividad sospechosa, violación de datos,

el incumplimiento de las Leyes de Protección de Datos y/o esta Política, o si no se ha enviado una DSR al departamento competente dentro de treble.ai, el empleado debe informar de dicha actividad al Gerente de Privacidad.

3.2.7. Los empleados que no estén seguros de si pueden procesar o divulgar legítimamente Datos personales deben buscar asesoramiento del Gerente de Privacidad antes de tomar cualquier medida.

# 4. Terceros

4.1. Antes de compartir datos personales con cualquier persona fuera de treble.ai, el Responsable de Privacidad debe asegurarse de que este Tercero tenga un nivel de protección de datos adecuado y proporcione suficientes garantías de protección de datos de acuerdo con las Leyes de Protección de Datos, incluidos, entre otros, los requisitos de procesamiento (Art. 28 del GDPR) y el cumplimiento de transferencias internacionales (Sección 5 del GDPR). Cuando sea necesario, el Responsable de la Privacidad debe asegurarse de que treble.ai celebre el contrato de protección de datos adecuado con el tercero.

4.2. Un empleado puede compartir datos personales con terceros solo si y en la medida en que lo haya prescrito directamente el gerente y se especifique en la Política de privacidad

4.3. Si estamos obligados a eliminar, cambiar o detener el procesamiento de los Datos personales, debemos asegurarnos de que los Terceros, con los que compartimos los Datos personales, cumplan con estas obligaciones en consecuencia.

4.4. Siempre treble.ai sea contratado como procesador de datos en nombre de otra entidad, el Gerente de Privacidad debe asegurarse de treble.ai cumpla con la obligación de procesamiento. En particular, debe existir el acuerdo de procesamiento de datos adecuado de acuerdo con las Leyes de Protección de Datos. El Responsable de Privacidad debe supervisar el cumplimiento de las instrucciones de tratamiento de datos del responsable del tratamiento, en particular en lo que respecta al alcance de las actividades de tratamiento, la participación de los subencargados, las transferencias internacionales, el almacenamiento y la posterior eliminación de los datos personales tratados. Los datos personales tratados en el marco de la función de encargado del tratamiento no deben tratarse para ningún otro fin que no sea el especificado en las instrucciones, el acuerdo u otro acto jurídico pertinente que regule las relaciones con el responsable del tratamiento.

# 5. Transferencias internacionales

5.1. Si tenemos empleados, contratistas, filiales corporativas o procesadores de datos fuera del EEE y les transferimos datos personales para el procesamiento, el Administrador de privacidad debe asegurarse de treble.ai tome todas las medidas

de seguridad necesarias y apropiadas de acuerdo con las leyes de protección de datos.

5.2. El Responsable de Privacidad debe evaluar las garantías disponibles y proponer a la dirección de treble.ai la salvaguardia adecuada para cada

transferencia. Los siguientes regímenes se aplican a las transferencias de Datos Personales fuera de la UE:

- cuando la Comisión Europea decida que el país tiene un nivel adecuado de protección de datos personales, la transferencia no requiere la adopción de medidas de seguridad adicionales. La lista completa de jurisdicciones adecuadas puede consultarse en la página correspondiente del sitio web de la Comisión Europea1.
- para transferir Datos Personales a nuestros contratistas o socios (Procesadores de Datos o Controladores) en otros terceros países, debemos celebrar Cláusulas Contractuales Estándar con esa parte. La versión preliminar, junto con las orientaciones, se puede encontrar en la página correspondiente del sitio web de la Comisión Europea[2];
- si tenemos una filial corporativa o una entidad en otros países, podemos optar por adoptar Normas Corporativas Vinculantes de conformidad con el Artículo 47 del RGPD o un código de conducta aprobado de conformidad con el Artículo 40 del RGPD;
- también podemos transferir Datos personales a entidades que tengan una certificación aprobada de acuerdo con el artículo 42 del RGPD, que certifica un nivel adecuado de protección de datos de la empresa.

5.3. Como parte de las obligaciones de información, treble.ai deben informar a los Interesados de que sus Datos Personales se están transfiriendo a otros países, así como proporcionarles la información sobre las garantías utilizadas para la transferencia. La obligación de información se cumplirá de conformidad con la subsección 6.2.

5.4. En los casos excepcionales (el "**Derogación**"), cuando no podamos aplicar las salvaguardas mencionadas anteriormente y necesitemos transferir Datos personales, debemos obtener un consentimiento explícito (declaración activa) del Interesado o debe ser estrictamente necesario para la ejecución del contrato entre nosotros y el Interesado, o se aplican otras condiciones de derogación de acuerdo con las Leyes de Protección de Datos. El Administrador de Privacidad debe aprobar previamente cualquier transferencia de Derogación y documentar las Derogaciones aprobadas, así como la justificación de las mismas.

# 6. Derechos de los interesados

**6.1. <u>Nuestras responsabilidades</u>**.

6.1.1. El Administrador de Privacidad es el responsable último de entregar todas las DSR recibidas por treble.ai. En el caso de recibir cualquier DSR pendiente o inusual, el empleado debe buscar asesoramiento del Gerente de Privacidad antes de tomar cualquier acción.

6.1.2. El soporte técnico dentro de treble.ai es responsable de manejar las DSR de treble.ai usuarios a diario. El departamento de Recursos Humanos es responsable de:

[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en;

[2] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en;

manejo de la DSR de treble.ai empleados.

6.1.3. Todas las solicitudes de información sobre las solicitudes de información de los usuarios deben dirigirse y responderse desde la siguiente dirección de correo electrónico: privacy@treble.ai. La DSR de los empleados puede dirigirse directamente al responsable de RRHH o al privacy@treble.ai.

6.1.4. El empleado responsable debe responder a la DSR en el plazo de un (1) mes a partir de la recepción de la solicitud. En caso de que el cumplimiento de la DSR tarde más de un mes, el empleado responsable deberá solicitar el asesoramiento del Responsable de Privacidad y, en su caso, informar al Interesado sobre la prolongación del plazo de respuesta hasta dos (2) meses adicionales.

6.1.5. El empleado responsable debe analizar la DSR recibida para los siguientes criterios:

- **Identificación del interesado**. Antes de considerar el contenido de la DSR, el empleado responsable debe asegurarse de que el interesado sea la misma persona que afirma ser. Para ello, debe establecerse la conexión entre los registros de datos personales y el interesado.

  Para ello, se deben utilizar los siguientes métodos: comprobación de la dirección de correo electrónico del interesado: en general, la dirección de correo electrónico debe ser la misma que treble.ai tiene sobre el usuario en cuestión; si la dirección de correo electrónico es diferente del registro en la base de datos, se debe consultar al Gerente de Privacidad, tras cuya aprobación el empleado responsable puede solicitar detalles adicionales de la cuenta para la identificación, como la fecha de nacimiento, la dirección y la dirección de correo electrónico.

  Si el Interesado no se sometió a la verificación, el Responsable de la Privacidad deberá negarse a realizar la solicitud e informar al Interesado al respecto sin demora indebida, pero a más tardar en el plazo de un (1) mes a partir de la recepción de la solicitud.
- **Datos personales**. El empleado responsable debe comprobar si treble.ai tiene acceso a los datos personales solicitados. Si treble.ai no tiene los datos personales bajo control, el empleado responsable debe informar al Interesado y, si es posible, instruir sobre los pasos posteriores sobre cómo acceder a los datos en cuestión;
- **Contenido de la solicitud**. Dependiendo del contenido de la DSR, el empleado responsable debe definir el tipo de solicitud y verificar si cumple con las condiciones prescritas por esta Política y las Leyes de Protección de Datos. Los tipos de solicitudes y las condiciones respectivas para cada una de ellas pueden consultarse en los subapartados 6.3-6.9. Si la solicitud no cumple con los criterios descritos, el empleado responsable debe negarse a cumplir con la DSR e informar al Interesado sobre los motivos de la negativa;
- **Gratuito.** En general, todas las solicitudes de los interesados y el ejercicio de sus derechos son gratuitos. Si el empleado responsable considera que el interesado ejerce los derechos de forma excesiva o infundada (por ejemplo, con la intención de dañar o interrumpir las actividades comerciales de treble.ai), el empleado debe solicitar el asesoramiento del Responsable de la

privacidad y, al recibir este último, puede cobrar al interesado una tarifa razonable o negarse a hacerlo

cumplir con la solicitud;

- **Documentar**. Siempre treble.ai reciba la DSR, el Responsable de Privacidad debe asegurarse de que los datos y la hora, el Interesado, el tipo de solicitud y la decisión tomada al respecto estén bien documentados. En el caso de negarse a cumplir con la solicitud, también se deben documentar las razones de la negativa;
- **Destinatarios**. Al abordar la DSR, el Administrador de Privacidad debe asegurarse de que todos los destinatarios afectados hayan sido informados de las acciones necesarias que se tomaron.

**6.2. <u>Derecho a ser informado</u>**.

6.2.1. treble.ai debe notificar a cada Interesado sobre la recopilación y el procesamiento posterior de los Datos personales.

6.2.2. La información que debe proporcionarse incluye: el nombre y los datos de contacto de treble.ai; los fines genéricos y la base legal para la recopilación de datos y el procesamiento posterior; categorías de Datos Personales recopilados; destinatarios/categorías de destinatarios; períodos de retención; información sobre los derechos de los interesados, incluido el derecho a presentar una reclamación ante la autoridad de control competente; las consecuencias de los casos en los que los datos sean necesarios para la ejecución del contrato y el interesado no proporcione los datos requeridos; detalles de las garantías cuando los datos personales se transfieren fuera del EEE; y cualquier fuente de terceros de los datos personales, sin especificación para el caso particular (excepto si recibimos la solicitud directa del Titular de los Datos).

6.2.3. Los Usuarios deben ser informados por la Política de Privacidad accesible en el sitio web de treble.ai y proporcionada durante el registro de usuario. Los empleados y contratistas deben ser informados por una declaración de privacidad del empleado independiente, que explique los detalles descritos en la p. 6.2.2 de manera basada en casos, describiendo los propósitos y actividades particulares.

6.2.4. treble.ai Deberá informar a los Interesados sobre el tratamiento de los datos, incluida cualquier nueva actividad de tratamiento introducida en treble.ai dentro del siguiente plazo:

- si los datos personales se recopilan directamente del interesado, el interesado debe ser informado en el momento en que recopilamos datos personales de los interesados mostrándole al interesado nuestra declaración de privacidad;
- Si los datos personales se recogen de otras fuentes: (a) en el plazo de un mes a partir de su recogida; b) si los datos personales se van a utilizar para la comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado; o (c) si se prevé una divulgación a otro destinatario, a más tardar cuando los datos personales se divulguen por primera vez.
- a petición del interesado; y
- dentro de un (1) mes después de cualquier cambio en nuestras prácticas de datos personales, cambio del controlador de datos personales o después de cambios significativos en nuestras declaraciones de privacidad.

**6.3. <u>Derecho de acceso a la información</u>**.

6.3.1. Al Titular de los Datos se le deben proporcionar únicamente los registros de datos personales especificados en la solicitud. Si el interesado solicita acceso a todos los datos personales

En lo que respecta a él, el empleado debe buscar primero el asesoramiento del Gerente de Privacidad, para asegurarse de que todos los datos personales del Sujeto de datos estén mapeados y proporcionados.

6.3.2. El interesado tiene derecho a:

- saber si procesamos los Datos personales del interesado;
- obtener información sobre aspectos del procesamiento, incluida información detallada y específica de cada caso sobre los propósitos, las categorías de datos personales, los destinatarios/categorías de destinatarios, los períodos de retención, información sobre los derechos de una persona, detalles de las garantías relevantes cuando los datos personales se transfieren fuera del EEE y cualquier fuente de terceros de los datos personales; y
- obtener una copia de los Datos Personales que se están procesando cuando se le solicite.

**6.4. <u>El derecho a verificar la información del Interesado y solicitar su rectificación</u>**.

La información que recopilamos puede ser inexacta o estar desactualizada (por ejemplo, errores de nacionalidad, fecha de nacimiento, información sobre deudas, actividades económicas). Si revelamos que los Datos personales son inexactos o el Interesado nos solicita que lo hagamos, debemos asegurarnos de corregir todos los errores y actualizar la información relevante.

**6.5. <u>Derecho a restringir el tratamiento</u>**.

6.5.1. La limitación del tratamiento permite a los Interesados detener temporalmente el uso de su información para prevenir los posibles daños causados por dicho uso.

**6.5.2.** Este derecho se aplica cuando el Interesado:

- impugna la exactitud de los Datos personales;
- cree que procesamos los Datos personales de manera ilegal; y
- se opone al procesamiento y desea que no procesemos Datos personales mientras estamos considerando la solicitud.

6.5.3. En el caso de recibir la solicitud de restricción, no debemos procesar los Datos personales en cuestión para ningún otro propósito que no sea almacenarlos o con fines de cumplimiento legal hasta que las circunstancias de restricción dejen de existir.

**6.6. <u>Derecho a retirar el consentimiento</u>**. Para las actividades que requieren consentimiento, el Titular puede revocar su consentimiento en cualquier momento. Si el interesado revoca el consentimiento, debemos registrar los cambios y no debemos procesar los datos personales con fines basados en el consentimiento. La retirada del consentimiento no afecta a la licitud del tratamiento realizado antes de la retirada.

**6.7. <u>Derecho de oposición al tratamiento</u>**.

6.7.1. Si procesamos la información en nuestro interés legítimo, por ejemplo, para correos electrónicos de marketing directo o para nuestros fines de investigación de mercado, el interesado puede oponerse al procesamiento.

6.7.2. En el caso de recibir el caso de solicitud de objeción, debemos considerar Datos solicitud del sujeto y, cuando no tengamos intereses imperiosos, detener la

tratamiento para los fines especificados. Si los datos personales aún deben procesarse para otros fines, el Administrador de Privacidad debe asegurarse de que la base de datos tenga un registro de que los datos no pueden ser procesados posteriormente para las actividades objetadas.

6.7.3. La solicitud de objeción solo puede denegarse si los datos personales en cuestión se utilizan con fines de investigación científica/histórica o estadísticos y se han protegido adecuadamente, es decir, mediante técnicas de anonimización o seudonimización.

**6.8. <u>Derecho de supresión/olvido</u>**.

6.8.1. Los interesados tienen derecho a solicitarnos que borremos sus datos personales si se cumple una de las siguientes condiciones:

- Los datos personales ya no son necesarios para los fines de la recopilación. Por ejemplo, un usuario ha proporcionado datos personales para una actividad única, como la validación de datos o la participación en un concurso, y el propósito ya se ha cumplido;
- el interesado revoca su consentimiento o se opone al tratamiento (cuando proceda) y no existe ningún otro fundamento jurídico para el tratamiento; o
- procesamos los Datos personales de manera ilegal o su eliminación es requerida por la legislación aplicable de la Unión Europea o de uno de los países miembros de la Unión Europea.

6.8.2. Condiciones bajo las cuales tenemos derecho a rechazar la eliminación:

- Los datos personales se procesan con fines de investigación científica/histórica o estadísticos y se protegen adecuadamente, es decir, se seudonimizan o anonimizan;
- Los datos personales siguen siendo necesarios para el cumplimiento legal (por ejemplo, el cumplimiento de las leyes financieras o laborales).

6.8.3. Solo se deben eliminar los registros de datos personales que se especificaron en la solicitud. Si el Interesado solicita la eliminación de todos los datos personales que le conciernen, el empleado debe solicitar primero el asesoramiento del Responsable de Privacidad, para asegurarse de que todos los datos sobre el Interesado estén mapeados y puedan eliminarse.

6.8.4. Si el Usuario todavía tiene una cuenta con nosotros y solicita la eliminación de la información necesaria para mantener la cuenta, debemos informar al Usuario que la eliminación afectará la experiencia del usuario o puede conducir al cierre de la cuenta.

**6.9. <u>Portabilidad de los datos</u>**.

6.9.1. Los interesados pueden solicitarnos que transfiramos todos los datos personales y/o parte de ellos en un formato legible por máquina a un tercero. Este derecho se aplica en dos casos:

- Los datos personales se recopilaron con el fin de prestar nuestros servicios (ejecución del contrato); o
- Recopilados sobre la base del consentimiento.

6.9.2. Para determinar si se cumple una de las condiciones p.6.9.1, el empleado debe buscar asesoramiento del Gerente de Privacidad y verificar la base legal aplicable en los Registros de actividades de procesamiento. Si la respuesta es negativa, la solicitud puede ser rechazada por treble.ai, y el Responsable de Privacidad debe decidir si desea

cumplir con la solicitud de forma voluntaria.

6.9.3. Para cumplir con la solicitud, el empleado responsable debe consolidar los Datos personales solicitados y enviar los datos en el formato con el que trabajamos habitualmente a la organización solicitada. El interesado debe proporcionar los datos de contacto necesarios de la organización.

# 7. Nuevas actividades de tratamiento de datos

## 7.1. Notificación al Administrador de Privacidad

7.1.1. Antes de introducir cualquier nueva actividad que implique el tratamiento de datos personales, un empleado responsable de su implementación debe informar al Responsable de Privacidad.

7.1.2. Al recibir información sobre una nueva actividad, el Administrador de Privacidad debe:

- determinar la base jurídica del tratamiento y, en caso necesario, adoptar nuevas medidas para su fijación;
- asegurarse de que la actividad de procesamiento se realice de acuerdo con esta Política, otras políticas de treble.ai, así como con las Leyes de Protección de Datos;
- añadir la actividad de tratamiento a los Registros de actividades de tratamiento;
- modificar las declaraciones de información de privacidad y, cuando sea necesario, informar al interesado en consecuencia.

## 7.2. Evaluación de impacto del tratamiento de datos

7.2.1. El Responsable de Privacidad, en su caso, con la participación de los empleados competentes y/o asesores externos, deberá llevar a cabo un proceso si se cumple al menos una de las siguientes condiciones:

- el tratamiento implica el uso de nuevas tecnologías, como la Inteligencia Artificial, el uso de dispositivos conectados y autónomos, etc. que crea determinados efectos jurídicos, económicos o similares para el Interesado;
- evaluamos y evaluamos sistemáticamente los aspectos personales de los Interesados sobre la base de la elaboración automatizada de perfiles, asignando la puntuación/tasa personal, y creamos efectos legales o similares para el Interesado mediante esta actividad;
- tratamos a gran escala datos sensibles, que incluyen datos personales relacionados con condenas y delitos penales, los datos sobre sujetos de datos vulnerables, los datos personales que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos con el fin de identificar de forma única a una persona física, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física;
- recopilamos o procesamos datos personales de un área de acceso público o de fuentes públicas a gran escala, o combinamos o combinamos dos conjuntos de datos diferentes; y

# 8. Retención de datos

**8.1. <u>Regla general</u>**.

8.1.1. El Responsable de Privacidad debe asegurarse de que treble.ai claramente definidas las reglas de almacenamiento de datos. Asegurándose de que la información debe ser eliminada cada vez que el interesado ejerza sus derechos de supresión de sus datos.

# 9. Seguridad

9.1. Cada departamento dentro de treble.ai tomará todas las medidas técnicas y organizativas apropiadas que protejan contra el acceso no autorizado, ilegal y/o accidental, la destrucción, la modificación, el bloqueo, la copia, la distribución, así como contra otras acciones ilegales de personas no autorizadas con respecto a los datos personales bajo su responsabilidad.

9.2. El empleado responsable de la supervisión de la seguridad de los datos personales dentro de treble.ai será un especialista en informática. Esta persona implementa las directrices y otras especificaciones sobre protección de datos y seguridad de la información en su área de responsabilidad. Asesora a la dirección de treble.ai en la planificación e implementación de la seguridad de la información en treble.ai, y debe participar en todos los proyectos en una fase temprana para tener en cuenta los aspectos relacionados con la seguridad ya en la fase de planificación.

# 10.Procedimiento de respuesta a la violación de datos

**10.1. <u>Equipo de respuesta</u>**.

10.1.1. En caso de revelar la Violación de Datos, el CEO de treble.ai formará urgentemente el Equipo de Respuesta a la Violación de Datos (el "Equipo de **Respuesta**"), que se encargará de la Violación de Datos, notificará a las personas adecuadas y mitigará sus riesgos.

10.1.2. El Equipo de Respuesta debe ser un grupo multidisciplinario encabezado por el CEO de treble.ai y compuesto por el Gerente de Privacidad, el especialista en leyes de privacidad (ya sea interno o externo) y especialistas en seguridad de la información con conocimientos y habilidades dentro de treble.ai o profesionales de subcontratación, si es necesario. El equipo debe asegurarse de que todos los empleados y contratistas/procesadores comprometidos se adhieran a esta Política y proporcionen una respuesta inmediata, eficaz y hábil a cualquier violación de datos sospechosa/supuesta o real que afecte a treble.ai.

10.1.3. Los miembros potenciales del Equipo de Respuesta deben estar preparados para responder a una Violación de Datos. El Equipo de Respuesta cumplirá con todas las responsabilidades de treble.ai mencionadas en esta Política. Las funciones del Equipo de Respuesta son:

- comunicar la Violación de Datos a la(s) Autoridad(es) de Control competente(s);
- en caso de alto riesgo para los derechos y libertades de los Interesados, comunicar la Violación de Datos al Interesado;

- si treble.ai obtener datos de cualquier tercero como procesador, y una Violación de Datos involucra datos obtenidos, informar a los terceros sobre la Violación de Datos;
- para comunicar a los contratistas de treble.ai o a cualquier otro tercero que procese los Datos Personales involucrados en la Violación de Datos; y
- Adoptar todas las medidas técnicas y organizativas apropiadas para poner fin a la Violación de datos y mitigar sus consecuencias;
- registrar el hecho de la Violación de Datos en los Registros de actividades de procesamiento y presentar un informe interno de violación de datos que describa el evento.

10.1.4. El Equipo de Respuesta desempeñará sus funciones hasta que se tomen todas las medidas necesarias requeridas por esta Política.

**10.2. <u>Notificación a la Autoridad de Control</u>**.

10.2.1. treble.ai informará a la Autoridad de Control Competente sobre la Violación de Datos sin demora indebida y, cuando sea posible, a más tardar 72 horas después de haber tenido conocimiento de la Violación de Datos.

10.2.2. La Autoridad de Control Competente será determinada por la residencia de los Interesados, cuya información estuvo involucrada en la Violación de Datos. Si la violación de datos se refiere a los datos personales de los interesados de más de un país, treble.ai informará a todas las autoridades de control competentes.

10.2.3. Para dirigir la notificación a la autoridad, el Equipo de Respuesta debe utilizar el Anexo 1 de esta Política. El anexo 1 contiene toda la información de contacto necesaria de las autoridades de supervisión de la UE. Si la violación de datos afecta a interesados de países distintos de la UE, el equipo de respuesta solicitará asesoramiento a un especialista en privacidad competente.

10.2.4. La notificación a la autoridad de control competente contendrá, como mínimo, la siguiente información:

- **la naturaleza de la violación de datos** incluyendo, cuando sea posible, las categorías y un número aproximado de Interesados y registros de Datos Personales afectados;
- el nombre y los datos de contacto de la **Equipo de Respuesta, Gerente de Privacidad o, en su defecto, del CEO**;
- las consecuencias probables de la violación de datos. Explique el punto de vista de treble.ai sobre los fines y los posibles riesgos adicionales de la violación de datos. Por ejemplo, los datos personales pueden ser robados para fines posteriores **actividades de venta, fraude o chantaje a los interesados en cuestión**; y
- **Las medidas adoptadas o propuestas** que deben adoptar treble.ai para hacer frente a la violación de datos, incluidas, en su caso, las medidas para mitigar sus posibles efectos adversos.

10.2.5. Para presentar una notificación, el Equipo de Respuesta debe utilizar la Violación de Datos de treble.ai

Formulario de notificación a la autoridad de control.

**10.3. <u>Notificaciones a los interesados</u>**.

10.3.1. Cuando es probable que la violación de datos resulte en un alto riesgo para los derechos y libertades de los sujetos de datos (por ejemplo, robo de fondos, activos, información confidencial),

también debe comunicar la violación de datos a los interesados interesados en cuestión sin demora indebida. El Administrador de Privacidad debe determinar si existe un alto riesgo en función de los factores de riesgo especificados en la Subsección 7.2.3 de esta Política.

10.3.2. La notificación contendrá la siguiente información:

- descripción de la violación de datos: qué sucedió y qué condujo a la violación de datos, como **una violación de seguridad, negligencia del empleado, error en el trabajo del sistema.** Si el Equipo de Respuesta decidió no revelar las causas de la Violación de Datos, entonces esta cláusula no debe mencionarse;
- las medidas adoptadas por treble.ai en relación con la violación de datos, incluidas las siguientes: **Medidas de seguridad, investigaciones internas y aviso a la autoridad supervisora**;
- recomendaciones para los interesados en cuestión sobre cómo mitigar los riesgos y las posibles consecuencias, tales como **Directrices sobre cómo restaurar el acceso a una cuenta, medidas de prevención (cambio de contraseña)**; y
- la información de contacto del Equipo de Respuesta o de uno de sus miembros.

10.3.3. La notificación a los Interesados debe realizarse por **correo electrónico** o, cuando sea imposible utilizar el correo electrónico, por otros medios de comunicación disponibles.

**10.3.4. Exenciones**. No estamos obligados a enviar la notificación a los interesados si se cumple alguna de las siguientes condiciones:

- treble.ai ha implementado medidas de protección técnicas y organizativas adecuadas, y dichas medidas se aplicaron a los Datos Personales afectados por la Violación de Datos, en particular, aquellas que dejan los Datos Personales inaccesibles a cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
- treble.ai ha adoptado medidas posteriores que garanticen que ya no sea probable que se materialice el alto riesgo para los derechos y libertades de los Interesados a que se refiere esta sección; o
- supondría un esfuerzo desproporcionado para comunicarse con todos los interesados interesados. En tal caso, en su lugar, habrá una comunicación pública o una medida similar mediante la cual se informe a los interesados de manera igualmente eficaz.

En el caso de que apliquemos una de las exenciones, debemos **documentar** las circunstancias, el motivo por el que no informamos y las acciones tomadas para cumplir con una de las exenciones.

**10.4. <u>Comunicación con terceros</u>**.

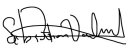
10.4.1. En el caso de que una violación de datos se refiera a los datos personales compartidos con nosotros o procesados por nosotros en nombre de un tercero, también debemos notificarlo al tercero dentro de las 24 horas. Si procesamos los Datos Personales como Procesador de Datos, la notificación al Tercero no nos

exime del deber de mitigar las consecuencias de la Violación de Datos, pero no debemos informar a la Autoridad de Control Competente y a los Interesados.

10.4.2. En caso de recibir la notificación sobre la Violación de Datos por parte del Procesador de Datos u otros Terceros que tengan acceso a los Datos Personales, el CEO de treble.ai deberá, de acuerdo con esta Sección:

- formar el Equipo de Respuesta;
- solicitar al Tercero que envíe la información mencionada en las Subsecciones 10.2-3 de esta Política;
- en caso necesario, informar a la(s) autoridad(es) de control competente(s) y Titulares de los datos; y
- realizar otros pasos del procedimiento de respuesta a la violación de datos.

# Lista de personas informadas sobre la política de protección de datos personales

| No | Nombre completo | Estado | Fecha | Firma |
|---|---|---|---|---|
| 1. | Daniel Martínez | Empleado | 16/12/20 |  |
| 2. | Sebastian Valencia | Empleado | 16/12/20 | |

# ANEXO 1 DE LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

## Autoridades Nacionales Europeas de Protección de Datos

## Austria

**Autoridad Austriaca de Protección de Datos**
Hohenstaufengasse 3
1010 Viena
Tel. +43 1 531 15 202525
Fax +43 1 531 15 202690 e-
mail: dsb@dsb.gv.at Sitio
web: http://www.dsb.gv.at/

Art 29 WP Miembro: **Dr. Andrea JELINEK**, Director, Austriaco
Dpa

## Bélgica

**Comisión de Privacidad**
**Comisión para la Protección de la Vida Privada** , Rue de la Presse, 35 / Drukpersstraat, 35, 1000 Bruselas / 1000 Bruselas, Tel. +32 2 274 48 00
Fax +32 2 274 48 35
Correo electrónico: commission@privacycommission.be
Sitio web: http://www.privacycommission.be/

Art 29 WP Vicepresidente: **Willem DEBEUCKELAERE,** Presidente de la República Belga
Comisión de privacidad

# Bulgaria

**Comisión de Protección de Datos Personales**
2, bulevar Prof. Tsvetan Lazarov. Sofía 1592
Tel. +359 2 915 3580
Fax +359 2 915 3525 e-mail:
kzld@cpdp.bg Sitio web:
http://www.cpdp.bg/

Artículo 29 WP Miembro: **Sr. Ventsislav KARADJOV,** Presidente de la Comisión de Protección de Datos Personales

Art 29 WP Miembro suplente: **Sra. Mariya MATEVA**

# Croacia

**Agencia Croata de Protección de Datos Personales**
Martićeva 14
10000 Zagreb
Tel. +385 1 4609 000
Fax +385 1 4609 099
Correo electrónico: azop@azop.hr o info@azop.hr
Sitio web: http://www.azop.hr/

Miembro del GT Art 29**: Sr. Anto RAJKOVAČA**, Director de la Protección de Datos de Croacia
Agencia

# Chipre

**Comisario de Protección de Datos Personales**
Calle Iasonos, 1,
1082 Nicosia
P.O. Box 23378, CY-1682 Nicosia Tel. +357 22 818 456
Fax: +357 22 304 565
Correo electrónico: commissioner@dataprotection.gov.cy
Sitio web: http://www.dataprotection.gov.cy/

Art 29 WP Miembro: **D.ª Irene LOIZIDOU NIKOLAIDOU**

Art 29 WP Miembro Suplente: **Sr. Constantinos GEORGIADES**

# República Checa

**La Oficina de Protección de Datos Personales**
Oficina de Protección de Datos Personales Pplk. Sochora 27
170 00 Praga 7
Tel. +420 234 665 111
Fax +420 234 665 444 e-
mail: posta@uoou.cz Sitio
web: http://www.uoou.cz/

Art 29 WP Miembro: **Sra. Ivana JANŮ**, Presidenta de la Oficina de Datos Personales Protección

Artículo 29 WP Suplente: **Sr. Ivan PROCHÁZKA**, Consejero del Presidente de la Oficina

# Dinamarca

**La Autoridad Noruega de Protección de Datos**
Borgergade 28, 5
1300 Copenhague K
Tel. +45 33 1932 00
Fax +45 33 19 32 18
Correo electrónico: dt@datatilsynet.dk
Sitio web: http://www.datatilsynet.dk/

Miembro del WP Art 29: **Sra. Cristina Angela GULISANO,** Directora de Protección de Datos de Dinamarca
Agencia (Datatilsynet)

Art 29 WP Miembro Suplente: **Sr. Peter FOGH KNUDSEN**, Jefe de la Comisión Internacional
División de la Agencia Danesa de Protección de Datos (Datatilsynet)

# Estonia

**Inspección de Protección de Datos de Estonia (Andmekaitse Inspektsioon)**
Pequeña América 19
10129 Tallin
Tel. +372 6274 135
Fax +372 6274 137
e-mail: info@aki.ee
Sitio web: http://www.aki.ee/en

Miembro del WP del artículo 29**: Sr. Viljar PEEP,** Director General de Protección de Datos de Estonia
Inspectoría

Art 29 WP Miembro suplente: **Sra. Maarja Kirss**

# Finlandia

**Defensoría del Pueblo en materia de Protección de Datos**
Apartado Postal 315
FIN-00181 Helsinki Tel. +358 10 3666 700
Fax: +358 10 3666 735
Correo electrónico: tietosuoja@om.fi
Sitio web: http://www.tietosuoja.fi/en/

Miembro del WP del artículo 29: **Sr. Reijo AARNIO**, Defensor del Pueblo de la Protección de Datos de Finlandia
Autoridad

Art 29 WP Suplente Vocal **: Sra. Elisa KUMPULA**, Jefa de Departamento

# Francia

**Comisión Nacional de Informática y Libertades - CNIL**
8 rue Vivienne, CS 30223 F-75002 Paris, Cedex 02 Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Sitio web: http://www.cnil.fr/

Miembro del WP Art 29**: D.ª Isabelle FALQUE-PIERROTIN,** Presidenta

de la CNIL Miembro suplente del WP Art 29**: D.ª Florence RAYNAL**

# Alemania

**El Comisionado Federal para la Protección de Datos y la Libertad de Información**
Husarenstraße 30
53117 Bonn
Tel. +49 228 997799 0; +49 228 819950
Fax +49 228 997799 550; +49 228 81995 550
e-mail: poststelle@bfdi.bund.de
Sitio web: http://www.bfdi.bund.de/

La competencia para presentar reclamaciones se reparte entre las diferentes autoridades de supervisión de la protección de datos en Alemania.
Las autoridades competentes pueden identificarse con arreglo a la lista que figura en el https:// www.bfdi.bund.de/bfdi_wiki/index.php/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

Art 29 WP Miembro: **Sra. Andrea VOSSHOFF**, Comisionada Federal para la Libertad de Información

Art 29 WP Miembro suplente: **Prof. Dr. Johannes CASPAR,** representante de los estados federados

# Grecia

**Autoridad Helénica de Protección de Datos**
Kifisias de. 1-3, PC 11523 Ampelokipi Atenas
Tel. +30 210 6475 600
Fax +30 210 6475 628 e-mail: contact@dpa.gr Sitio web: http://www.dpa.gr/

Miembro del GT Art 29**: Sr. Konstantinos Menoudakos,** Presidente de la DPA

Helénica Miembro suplente del WP Art 29: **Dr. Vasilios ZORKADIS,** Director

# Hungría

**Autoridad Nacional de Protección de Datos y Libertad de Información**
Szilágyi Erzsébet fasor 22/C H-1125 Budapest
Tel. +36 1 3911 400
Correo electrónico: peterfalvi.attila@naih.hu
Sitio web: http://www.naih.hu/

Artículo 29 Miembro del WP: **Dr. Attila PÉTERFALVI,** Presidente de la Autoridad Nacional de Datos
Protección y libertad de información

Art 29 WP Suplente Vocal: **Sr. Endre Győző SZABÓ** Vicepresidente de la Comisión Nacional
Autoridad para la Protección de Datos y la Libertad de Información

# Irlanda

**Comisario de Protección de Datos**
Canal House, Estación Road, Portarlington Co., Laois
Fecha de llamada: 1890 25 22 31
Tel. +353 57 868 4800
Fax: +353 57 868 4757
Correo electrónico: info@dataprotection.ie
Sitio web: http://www.dataprotection.ie/

Art 29 WP Miembro: **Sra. Helen DIXON,** Comisionada de Protección de Datos

Art 29 WP Miembros suplentes: **Sr. John O'DWYER,** Comisionado Adjunto; **Sr. Dale SUNDERLAND,** Comisario Adjunto

# Italia

**Garante de la protección de datos personales**
Piazza di Monte Citorio, 121 00186 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
correo electrónico: garante@garanteprivacy.it
Sitio web: http://www.garanteprivacy.it/

Art 29 WP Miembro: **Sr. Antonello SORO,** Presidente de Garante per la protezione dei dati personali

Art 29 WP Suplente Vocal: **Sra. Giuseppe BUSIA,** Secretaria General de Garante per la protezione dei dati personali

# Letonia

**Directora de la Inspección Estatal de Datos: Sra. Daiga Avdejanova**
Calle Blaumana. 11/13-15
1011 Riga
Tel. +371 6722 3131
Fax: +371 6722 3556
Correo electrónico: info@dvi.gov.lv
Sitio web: http://www.dvi.gov.lv/

Art 29 WP Miembro suplente: **Sra. Aiga BALODE**

# Lituania

**Protección de Datos del Estado**
Žygimantai str. 11-6a 011042 Vilnius
Tel. +370 5 279 1445
Fax +370 5 261 94 94 e-
mail: ada@ada.lt Sitio
web: http://www.ada.lt/

Art 29 WP Miembro: **Sr. Raimondas Andrijauskas**, Director de la Comisión Estatal de Datos
Inspección de Protección

Art 29 WP Suplente Vocal **: Sra. Neringa KAKTAVIČIŪTĖ-MICKIENĖ**, Jefa de División de Investigación de Denuncias y Cooperación Internacional

# Luxemburgo

**Comisión Nacional de Protección de Datos**
1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette Tel. +352 2610 60 1
Fax +352 2610 60 29 e-
mail: info@cnpd.lu Sitio web:
http://www.cnpd.lu/

Artículo 29 WP Miembro: **Sra. Tine A. LARSEN,** Presidenta de la Comisión Nacional de Protección de Datos

Art 29 WP Suplente: **Sr. Thierry LALLEMANG**, Comisario

# Malta

**Oficina del Comisionado de Protección de Datos Comisionado de Protección de Datos: Sr.**
**José Ebejer**
2, Casa de las Vías Aéreas
High Street, Sliema SLM 1549 Tel. +356 2328 7100
Fax: +356 2328 7198
Correo electrónico: commissioner.dataprotection@gov.mt
Sitio web: http://www.dataprotection.gov.mt/

Art 29 WP Miembro: **Sr. Saviour CACHIA**, Información y Protección de Datos Comisionado

Art 29 WP Miembro Suplente: **Sr. Ian DEGUARA,** Director de Operaciones y Ejecución del programa

# Países Bajos

**Autoridad holandesa de protección de datos**
Boulevard Prince Clau 60
Apartado de correos 93374
2509 AJ Den Haag/La Haya Tel. +31 70 888 8500
Fax: +31 70 888 8501
Correo electrónico: info@autoriteitpersoonsgegevens.nl
Sitio web: https://autoriteitpersoonsgegevens.nl/nl

Miembro del GT Art 29**: Sr. Aleid WOLFSEN,** Presidente de la Autoridad Holandesa de Protección de Datos

# Polonia

**La Oficina del Inspector General para la Protección de Datos Personales - GIODO**
Stawki 2
00-193 Varsovia
Tel. +48 22 53 10 440
Fax +48 22 53 10 441
Correo electrónico: kancelaria@giodo.gov.pl; desiwm@giodo.gov.pl
Sitio web: http://www.giodo.gov.pl/

Miembro del WP Art 29**: Sra. Edyta BIELAK-JOMAA**, Inspectora General de Protección de Datos Personales

# Portugal

**Comisión Nacional de Protección de Datos - CNPD**
R. de São. Bento, 148-3° 1200-821 Lisboa
Tel.+351 21 392 84 00
Fax +351 21 397 68 32 e-
mail: geral@cnpd.pt Sitio
web: http://www.cnpd.pt/

Miembro del GT Art 29: **Sra. Filipa CALVÃO,** Presidenta de la Comisión Nacional de Protección de Datos

Art 29 WP Miembro Suplente: **Isabel CRUZ**, Secretaria General de la DPA

# Rumania

**La Autoridad Nacional de Control del Tratamiento de Datos Personales Presidenta: Sra.**
**Ancuţa Gianina Oprah**
28-30 Magheru Blvd.
Sector 1, BUCUREŞTI
Tel. +40 21 252 5599
Fax: +40 21 252 5757
Correo electrónico: anspdcp@dataprotection.ro
Sitio web: http://www.dataprotection.ro/

Art 29 WP Miembro: **Sra. Ancuţa Gianina OPRE,** Presidenta de la Comisión Nacional de Supervisión
Autoridad para el Tratamiento de Datos Personales

Art 29 WP Miembro Suplente: **Sra. Alina SAVOIU,** Jefa de la Comisión de Asuntos Jurídicos y
Departamento de Comunicación

# Eslovaquia

**Oficina de Protección de Datos Personales de la República Eslovaca**
Hraničná 12
820 07 Bratislava 27
Tel.: +421 2 32 31 32 14
Fax: + 421 2 32 31 32 34
Correo electrónico: statny.dozor@pdp.gov.sk
Sitio web: http://www.dataprotection.gov.sk/

Art 29 WP Miembro: **Sra. Soňa PŐTHEOVÁ,** Presidenta de la Oficina de Datos Personales
Protección de la República Eslovaca

Artículo 29 WP Suplente: **Sr. Anna VITTEKOVA**, Vicepresidenta

# Eslovenia

**Comisario de Información**
MS Mojca Prelesnik Zaloška 59
1000 Liubliana
Tel. +386 1 230 9730
Fax +386 1 230 9778 e-mail:
gp.ip@ip-rs.si Sitio web:
https://www.ip-rs.si/

Art 29 WP Miembro: **Sra. Mojca PRELESNIK,** Comisaria de Información de la República de Eslovenia

# España

**Agencia de Protección de Datos**
C/Jorge Juan, 6
28001 Madrid
Tel. +34 91399 6200
Fax +34 91455 5699
correo electrónico: internacional@agpd.es
Sitio web: https://www.agpd.es/

Art 29 WP Miembro: **D.ª María del Mar España Martí**, Directora de la Comisión Española de Datos
Agencia de Protección

Art 29 WP Suplente Vocal: **D. Rafael GARCIA GOZALO**

# Suecia

**Datainspektionen**
Drottninggatan 29 5th Floor
Box 8114
104. 20 Estocolmo
Tel. +46 8 657 6100
Fax: +46 8 652 8652
Correo electrónico: datainspektionen@datainspektionen.se
Sitio web: http://www.datainspektionen.se/

Art 29 WP Miembro: **Sra. Kristina SVAHN STARRSJÖ**, Directora General de la Comisión de Datos
Junta de Inspección

Artículo 29 WP Suplente Vocal: **Sr. Hans-Olof LINDBLOM**, Consejero Jurídico Principal

# Reino Unido

**La Oficina del Comisionado de Información**
Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF Tel. +44 1625 545 745 e-mail: international.team@ico.org.uk
Sitio web: https://ico.org.uk

Art 29 WP Miembro: **Sra. Elizabeth DENHAM,** Comisaria de Información

Art 29 WP Miembro suplente: **Sr. Steve WOOD,** Comisionado Adjunto

# ZONA EUROPEA DE LIBRE COMERCIO (AELC)

## Islandia

Agencia islandesa de protección de datos Rauðarárstíg 10
105. Reikiavik
Tel. +354 510 9600; Fax +354 510 9606 e-mail:
postur@personuvernd.is

## Liechtenstein

Oficina de Protección de Datos Kirchstrasse 8, P.O. Box 684
9490 Vaduz
Principado de Liechtenstein Tel. +423 236
6090 e-mail: info.dss@llv.li

## Noruega

La Autoridad Noruega de Protección de Datos
La Inspección de Datos
P.O. Box 8177 Dep 0034 Oslo
Tel. +47 22 39 69 00; Fax +47 22 42 23 50 e-mail:
postkasse@datatilsynet.no

Autoridad de Protección de Datos: **D. Bjørn Erik THORN**

## Suiza

Comisionado de Protección de Datos e Información de Suiza Eidgenössischer
Responsable de Protección de Datos e Información **: Sr. Adrian Lobsiger**
Feldeggweg 1
3003 Berna
Tel. +41 58 462 43 95; Fax +41 58 462 99 96 e-mail: contact20@edoeb.admin.ch