45ª Sesión Cerrada de la Asamblea Global de Privacidad Octubre de 2023

Alcanzando estándares globales de protección de datos: principios para garantizar altos niveles de protección de datos y privacidad en todo el mundo

Esta Resolución es presentada por:

***PATROCINADORES***:

* Oficina del Comisionado de Información, Reino Unido

COPATROCINADORES:

* Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), México
* Comisionado de Protección de Datos, Consejo de Europa
* Supervisor Europeo de Protección de Datos, Unión Europea
* Comisión Nacional de Informática y Libertades (CNIL), Francia
* Comisionado Federal de Protección de Datos (BfDI), Alemania
* Autoridad de Protección de Datos, Bailía de Guernsey
* Garante per la protezione del dati personali, Italia
* Comisionado Federal de Protección de Datos e Información (FDPIC), Suiza
* Unidad Reguladora y de Control de Datos Personales, Uruguay

La 45ª Asamblea Global de la Privacidad 2023:

*DESTACANDO* la importancia de los altos estándares tanto para defender la protección de datos y la privacidad como un derecho fundamental como para proteger los derechos e intereses de las personas a través del tratamiento adecuado de los datos personales;

*RECONOCIENDO* que la interpretación coherente entre jurisdicciones es importante para mantener altos estándares y fomentar un entorno normativo claro. Que, a su vez, garantiza que los datos personales de las personas estén protegidos y se respeten sus derechos, que las organizaciones se ganen la confianza de las personas y que se puedan desarrollar productos y servicios innovadores para la economía digital.

*RECORDANDO* la Resolución de Madrid1 adoptada en 2009, que especifica un conjunto de principios y derechos que garantizan la protección efectiva de la privacidad con respecto al tratamiento de datos personales, y *RECONOCIENDO* su contribución e influencia global;

*RECONOCIENDO QUE* las jurisdicciones de todo el mundo han estado desarrollando sus propias leyes y regímenes de protección de datos que reflejan los valores, prioridades y necesidades de su cultura y sociedad, *y RECONOCIENDO* ADEMÁS la necesidad de que los esfuerzos internacionales continúen basándose en puntos en común, complementariedades y elementos de convergencia para fomentar la interoperabilidad futura entre ellos;

*SUBRAYANDO QUE* el contexto en el que deben aplicarse los principios y las leyes de protección de datos y privacidad ha cambiado, y continúa evolucionando a medida que los avances en la tecnología, la innovación y la digitalización conducen a nuevas actividades y modelos de negocio que se basan cada vez más en el tratamiento de grandes volúmenes de datos personales de formas nuevas y progresivamente complejas, y *RECONOCIENDO QUE* las leyes, los principios y la forma en que se aplican deben seguir proporcionando un alto nivel de protección;

*OBSERVANDO QUE* tales desarrollos van desde la digitalización generalizada de los servicios hasta el desarrollo y despliegue generalizados de la inteligencia artificial, el uso de decisiones automatizadas y las innovaciones que utilizan tecnologías biométricas;

*PREOCUPADOS PORQUE* tales desarrollos pueden plantear nuevos desafíos para la implementación y el cumplimiento de las leyes de protección de datos y privacidad, ya que presentan riesgos relacionados con la minimización de datos, la seguridad, la transparencia y la precisión, que pueden causar efectos negativos significativos, como resultados injustos, discriminatorios y sesgados para las personas, o afectar su capacidad para ejercer sus derechos de protección de datos y privacidad;

*PREOCUPADO PORQUE* este amplio contexto incluye inevitablemente un tratamiento más intrusivo de los datos personales, incluidos los datos personales sensibles, especialmente los de los niños y las personas vulnerables, donde la necesidad de garantizar que los derechos se respeten y puedan ejercerse es particularmente aguda / importante;

*OBSERVANDO QUE* estas preocupaciones han llevado a los miembros de la GPA en varias jurisdicciones a tomar medidas coercitivas, como emitir multas, exigir la eliminación de datos y algoritmos innecesarios y emitir órdenes para detener el procesamiento. Los miembros también han expresado su preocupación en relación con la transparencia, la equidad, los sesgos y la discriminación;

1 [14302 STANDARS.qxp:Maquetación 1 (globalprivacyassembly.org)](https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf)

*ACOGIENDO CON BENEPLÁCITO* los esfuerzos de los miembros del GPA en varias jurisdicciones para identificar las implicaciones de protección de datos y privacidad de las tecnologías emergentes y futuras;

*SEÑALANDO* la importancia de adoptar un enfoque ético y centrado en el ser humano para las tecnologías emergentes, y *ENFATIZANDO QUE* la protección de datos y la privacidad son fundamentales para fomentar la gobernanza de datos, con el fin de salvaguardar el reconocimiento de los derechos e intereses de las personas en el entorno digital;

*SUBRAYANDO QUE* el contexto de una economía digital global en rápido desarrollo también enfatiza la necesidad de enviar y recibir datos a través de las fronteras de una manera que proteja los derechos de protección de datos y privacidad de las personas;

*SUBRAYANDO ADEMÁS QUE* para permitir que los datos fluyan a través de las fronteras, existe la necesidad de marcos y mecanismos con estándares altos comparables para garantizar la protección coherente de los derechos de las personas al tiempo que se facilita el flujo internacional de datos personales necesarios en un mundo globalizado;

*DESTACANDO* la importancia de la cooperación para identificar y trabajar hacia la convergencia entre las protecciones en los marcos e instrumentos legales para lograr un alto nivel de protección de datos y privacidad, fomentar la interoperabilidad futura y facilitar el flujo libre de datos con confianza;

*AFIRMANDO* la capacidad de las autoridades miembros de la GPA para actuar como asesores expertos de confianza, y la importancia de que los responsables políticos, las autoridades y otras partes interesadas trabajen juntos para proteger los datos personales y defender los derechos de las personas en el contexto de la economía digital global actual;

La GPA reconoce el valor de los estándares globales con respecto a la protección de datos y la privacidad y, por lo tanto, reconoce y promueve los siguientes principios, derechos y otros elementos de alto nivel como importantes para lograr altos estándares de protección de datos personales y privacidad en el contexto de la economía digital global actual:

1. **Legalidad y equidad**

El tratamiento de los datos personales debe ser lícito de conformidad con la legislación nacional aplicable y los acuerdos internacionales. También destacamos el principio de equidad y enfatizamos que los datos personales no deben obtenerse por medios engañosos o fraudulentos, priorizando la protección de los intereses del interesado y la expectativa razonable de privacidad, asegurando que el procesamiento no resulte en resultados injustos, discriminatorios o sesgados.

## Especificación de propósito

El tratamiento debe limitarse al cumplimiento de fines específicos, explícitos y legítimos y no tratarse posteriormente de manera incompatible con dichos fines.

## Necesidad y proporcionalidad

Reafirmamos el principio de minimización de datos, según el cual los datos personales deben limitarse a lo que sea adecuado, relevante y no excesivo en relación con los fines del procesamiento. También enfatizamos la importancia de la proporcionalidad general y la necesidad en el contexto del objetivo general del procesamiento, en relación con los derechos de información de las personas, para permitir que se tomen las decisiones apropiadas sobre el uso de nuevos tipos de procesamiento y tecnologías, como las que procesan datos sensibles /de categoría especial o datos biométricos.

## Calidad de los datos

Se deben tomar todas las medidas razonables para garantizar que los datos personales procesados sean precisos y se mantengan actualizados según sea necesario para cumplir con los fines. Esto es particularmente importante cuando los riesgos de que se tomen decisiones importantes sobre las personas sobre la base de información incorrecta se ven exacerbados por el uso de decisiones automatizadas, algoritmos e IA, lo que a su vez puede tener graves implicaciones para las decisiones relacionadas, por ejemplo, con las finanzas, la investigación y los delitos penales. Las decisiones automatizadas deben basarse en información precisa y los sistemas deben estar entrenados con información precisa e imparcial.

## Limitación de retención / almacenamiento

Los datos personales deben conservarse solo el tiempo que sea necesario para cumplir con los fines para los que se procesan, y deben eliminarse o anonimizarse cuando ya no sean necesarios para esos fines.

## Transparencia

Hacemos hincapié en la importancia de la claridad, la accesibilidad y la facilidad de comprensión para que las personas estén debidamente informadas sobre cómo se procesan sus datos personales y puedan ejercer sus derechos. La información debe proporcionarse activamente para garantizar que las personas conozcan el procesamiento, lo que puede requerir diferentes mecanismos según el contexto.

## Rendición de cuentas

Hacemos hincapié en la importancia de acompañar los elementos prácticos para demostrar el cumplimiento de los principios de alto nivel y poner en práctica el principio de rendición de cuentas, tales como, pero no necesariamente limitados a, las medidas proactivas que se exponen a continuación.

## Seguridad

Los responsables y encargados del tratamiento deben contar con las medidas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. La seguridad es un requisito cada vez más importante, ya que los riesgos de seguridad pueden aumentar a medida que avanza la tecnología, aumenta la participación en el entorno digital y se incrementan los volúmenes de datos personales procesados en la economía digital global.

En particular, esto puede conducir a un aumento de los riesgos de ciberseguridad. Observando que la ciberseguridad cruza las esferas regulatorias, enfatizamos la importancia de leyes y enfoques claros y consistentes de la cooperación entre reguladores, organismos de ciberseguridad y otras partes interesadas relevantes para abordar de manera efectiva los riesgos de seguridad global.

## Legitimación y bases para el tratamiento

Hacemos hincapié en la importancia de proporcionar una gama de bases legales adecuadas y proporcionadas para el procesamiento, por ejemplo, contratos, interés público, obligación legal, interés legítimo, así como consentimiento, dependiendo de los fines y el contexto del procesamiento. Cuando el consentimiento está disponible como base, enfatizamos la importancia del requisito de que sea significativo y válido, que ofrezca una elección y control reales, y que debe ser la voluntad libre, específica, inequívoca e informada del interesado, con su acuerdo significado por declaración o clara acción afirmativa.

## Datos sensibles

Se deben establecer protecciones adicionales para los datos personales relacionados con aspectos y características específicos, tales como el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, así como los datos relativos a la salud y la vida sexual y los delitos penales. También enfatizamos la necesidad de revisar los tipos de datos personales incluidos en esta categoría, para mantenernos al día con los desarrollos tecnológicos que permiten la identificación de datos personales y pueden plantear riesgos relacionados con su naturaleza sensible (por ejemplo, datos relacionados con información biométrica o genética, y con neurotecnología). Además, observamos que los datos que no son sensibles por mérito propio pueden llegar a serlo cuando se combinan con otros datos. Esto puede incluir datos inferidos en los que, en determinadas circunstancias, los registros relacionados, por ejemplo, con los hábitos de navegación o visualización se pueden utilizar para inferir el origen étnico, las creencias, las opiniones políticas, el estado de salud o la orientación sexual de una persona.

## Protección para niños y personas vulnerables

Dado que los niños y las personas vulnerables pueden ser menos conscientes de los riesgos que implica el procesamiento de sus datos personales y, por lo tanto, podrían ser menos capaces de ejercer sus derechos de protección de datos y privacidad, enfatizamos la importancia de tomar medidas específicas para su protección. Apreciamos los esfuerzos de los miembros de la GPA y otros para complementar los requisitos legales con códigos de práctica y orientación.

## Responsables y encargados del tratamiento

Es importante que existan acuerdos claros entre los controladores y los procesadores/proveedores de servicios que actúan en nombre y bajo las instrucciones de los controladores, con las respectivas obligaciones y responsabilidades, detalles específicos sobre el procesamiento e instrucciones establecidas en un contrato.

## Transferencias internacionales de datos personales

Hacemos hincapié en la importancia de prever la protección de los datos personales a través de las fronteras con una serie de mecanismos de transferencia, como la adecuación, las cláusulas modelo, las certificaciones y los acuerdos administrativos, para garantizar que la protección viaje con los datos. Observamos los beneficios de aprovechar los puntos en común, las complementariedades y los elementos de convergencia para fomentar la interoperabilidad futura entre los enfoques y mecanismos regulatorios existentes que permitan flujos de datos transfronterizos seguros y confiables. Acogemos con beneplácito el trabajo del G7 y su Mesa Redonda de Autoridades de Protección de Datos y Privacidad sobre el desarrollo y la puesta en marcha del Flujo Libre de Datos con Confianza, y reconocemos la importancia de trabajar en este tema a medida que la economía digital global genera mayores flujos de datos.

Reafirmamos la Resolución de la GPA sobre el acceso del gobierno a los datos, la privacidad y el estado de derecho: Principios para el acceso gubernamental a los datos personales en poder del sector privado para fines de seguridad nacional y seguridad pública, y acogemos con beneplácito la Declaración de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre el acceso del gobierno a los datos personales en poder de entidades del sector privado.

## Derecho a la información

Hacemos hincapié en la importancia del derecho de las personas a estar informadas sobre qué datos personales se procesan, cómo, por quién y con qué fines, y sobre los derechos que tienen en relación con ese procesamiento. Tomamos nota del vínculo con el principio de transparencia y enfatizamos la creciente importancia de que las personas estén debidamente informadas, ya que las operaciones de procesamiento automatizado pueden ser cada vez más complejas y opacas.

## Ejercicio de derechos de acceso, rectificación, cancelación y oposición

Hacemos hincapié en la importancia de los derechos de acceso, rectificación, cancelación y oposición de los interesados y, en particular, destacamos la importancia del derecho de acceso, como un habilitador clave de los demás derechos de protección de datos de las personas.

## Restricción

También destacamos la importancia de un derecho a la restricción del tratamiento, para limitar el uso de datos personales y proteger a las personas del riesgo de decisiones inexactas, discriminatorias e injustas tomadas cuando esos datos son inexactos, tratados ilegalmente, objetados o en disputa.

## Portabilidad de datos

Observamos la importancia de que los interesados puedan obtener de un controlador una copia de sus datos personales en un formato electrónico estructurado y de uso común, para permitirles reutilizar sus datos en diferentes servicios y transferirlos a otro controlador según sea necesario.

## Derechos relacionados con la elaboración de perfiles y decisiones automatizadas

Destacamos la importancia de garantizar que se proporcionen derechos a los interesados cuando se lleva a cabo la elaboración de perfiles o se toman decisiones que los afectan significativamente, mediante medios automatizados sin intervención humana. Estos derechos pueden incluir, por ejemplo, derechos para obtener información sobre la lógica involucrada en el procesamiento, para obtener intervención humana o para impugnar una decisión.

## Capacidad para ejercer derechos

También destacamos la importancia de proporcionar **formas simples y eficientes para que las personas ejerzan sus derechos**. Esto es especialmente importante a medida que los tipos de datos personales evolucionan y las operaciones de procesamiento se vuelven más complejas. Cualquier restricción o limitación de derechos debe estar prevista por la ley y debe aplicarse en la medida necesaria y proporcionada para salvaguardar un objetivo de interés público o los derechos y libertades de los demás.

## Medidas proactivas

Hacemos hincapié en la necesidad de implementar medidas proactivas para implementar la protección de datos y la privacidad a nivel práctico. En estrecha relación con el **principio de rendición de cuentas**, destacamos la importancia de la implementación práctica y el cumplimiento de los requisitos de protección de datos y privacidad, y de demostrar el cumplimiento tanto a los reguladores como a las personas cuyos datos se procesan.

En particular, destacamos la importancia de:

* + **La** **privacidad y la protección de datos personales desde el diseño**, a medida que se desarrollan productos, tecnologías y formas de procesamiento de datos personales nuevos e innovadores, es vital incorporar la protección de datos y la privacidad desde el inicio de dichos proyectos para identificar, prevenir y mitigar los daños, y garantizar que los derechos puedan ser respetados y ejercidos. Esto podría incluir elementos como tecnologías que mejoran la privacidad y el uso de espacios regulatorios controlados;
  + **La privacidad y la protección de datos personales por defecto** deben aplicarse en programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que procese datos personales;
  + **Medidas proactivas de cumplimiento**, tales como:
    - **Evaluaciones de impacto de privacidad /protección de datos** para identificar y mitigar los riesgos de protección de datos y privacidad
    - **Auditorías independientes** para identificar y tomar las medidas adecuadas en caso de incumplimiento, según sea necesario para proteger los derechos de protección de datos de las personas

## La adopción e implementación de políticas internas de protección de datos

que el personal debe cumplir

* + - **Capacitación, educación y sensibilización**, según corresponda, al personal que procesa datos personales, y la existencia de oficiales de protección de datos o personal responsable equivalente para supervisar el cumplimiento
    - **Medidas de prevención, detección y respuesta en caso de filtración**, incluida la **notificación** a las autoridades reguladoras y a las personas afectadas, según corresponda
    - **Programas de gestión de la privacidad** y otros enfoques similares para proporcionar y demostrar salvaguardas efectivas y el cumplimiento de los requisitos de protección de datos y privacidad
    - **Códigos de práctica o conducta,** para desarrollar directrices específicas dentro de los sectores que aborden de manera efectiva los principales problemas de protección de datos y privacidad dentro de esos sectores
    - **Certificación** para que las organizaciones demuestren su cumplimiento con los requisitos de protección de datos y privacidad a través de esquemas aprobados
    - **Mecanismos para ayudar a los interesados a presentar consultas y quejas** sobre el tratamiento de sus datos personales.

## Autoridades de control

Destacamos la importancia de la existencia de una autoridad de control independiente. Las autoridades deben ser independientes, contar con poderes suficientes para investigar y tomar medidas, contar con recursos suficientes para poder desempeñar eficazmente sus funciones, y sus líderes y personal deben tener niveles adecuados de experiencia y competencia técnica. Reconocemos la importancia de que las autoridades tengan jurisdicción suficiente para supervisar los sectores público y privado, para garantizar la aplicación coherente de la legislación sobre protección de datos y privacidad. Reafirmamos el análisis y reporte del Grupo de Trabajo de Marcos y Estándares Globales de la GPA sobre las características clave de las autoridades independientes de protección de datos/privacidad.2

También enfatizamos la importancia de las autoridades, además de monitorear y verificar el cumplimiento, realizar actividades de concientización y participación proactiva y preventiva con los controladores cuando sea posible y según corresponda, por ejemplo, mediante la producción de orientación, la realización de consultas con las partes interesadas y proyectos para promover el cumplimiento, como espacios regulatorios controlados.

## Cooperación

Hacemos hincapié en la importancia de la cooperación de las autoridades de supervisión, **tanto con otras autoridades de protección de datos y privacidad, como con otros reguladores sectoriales,** como los de competencia, consumo, finanzas y ciberseguridad. Reconocemos la importancia de las disposiciones para autorizar a las autoridades de protección de datos y privacidad a compartir la información necesaria con las autoridades de otras jurisdicciones para fortalecer la cooperación entre ellas.

2 [1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org)](https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf) (Anexo B, página 28)

Destacamos los beneficios de la cooperación en términos de desarrollo de capacidades, intercambio de conocimientos, eficiencia, prevención de la duplicación del trabajo, decisiones regulatorias mejores y más consistentes, particularmente en relación con las investigaciones de las mismas empresas y problemas en diferentes jurisdicciones globales, y en relación con diferentes aspectos regulatorios de las acciones de las organizaciones en la economía digital global.

Destacamos que los enfoques comunes de los reguladores, siempre que sea posible, pueden comunicar un mensaje más fuerte a las organizaciones y obtener mejores resultados regulatorios y mejores resultados para los ciudadanos del mundo.

## Responsabilidad y compensación

También destacamos la importancia de contar con **marcos de responsabilidad adecuados** y la capacidad de los interesados para **hacer valer sus derechos directamente a través de los tribunales.**

Por lo tanto, la 45ª Asamblea Global de la Privacidad resuelve:

* Abogar por, promulgar y promover los principios, derechos y otros elementos establecidos en esta resolución, para garantizar que puedan implementarse y aplicarse de manera efectiva en todos los contextos, particularmente en el procesamiento de datos con tecnologías e innovaciones nuevas y emergentes; e
* Instar a los responsables de la legislación y las políticas que consulten a las autoridades de protección de datos y privacidad como asesores expertos de confianza al promulgar y modificar las leyes de protección de datos, privacidad y leyes relacionadas.

## Nota explicativa:

Los miembros actuales de la GPA reconocen la contribución y la influencia global de la Resolución de Madrid, que fue adoptada por la GPA en 2009, y que especificaba un conjunto de principios y derechos de protección de datos y privacidad, muchos de los cuales siguen siendo familiares hoy en día. Sin embargo, en el contexto actual de creciente digitalización, innovación y desarrollo tecnológico, de una economía digital global que ve más datos procesados a través de las fronteras, esta resolución establece a un alto nivel las expectativas actuales de los principios, derechos y otros elementos importantes que son importantes para garantizar altos estándares de protección de datos y privacidad en 2023, y que abogaríamos por que los responsables políticos consideren incluir a medida que se introducen y revisan las leyes de sus jurisdicciones.

A las autoridades miembros de la GPA les complace observar que las jurisdicciones de todo el mundo están promulgando crecientemente nuevas leyes de privacidad y protección de datos, y revisando las más antiguas, a menudo construyendo sobre elementos similares. Esto incluye el desarrollo creciente de regímenes específicos de transferencia internacional. Acogemos favorablemente los marcos y enfoques globales existentes, como el Convenio 108 del Consejo de Europa, un instrumento internacional jurídicamente vinculante abierto a la ratificación de todos los países y ahora modernizado en el Convenio 108+, las Directrices de la OCDE sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales, la Declaración de la OCDE sobre el Acceso Gubernamental a los Datos Personales en Posesión de Entidades del Sector Privado y la Recomendación de la OCDE sobre Cooperación Transfronteriza en el Cumplimiento de las Leyes de Protección de la Privacidad, las Directrices de la ONU para la Regulación de los Archivos Computarizados de Datos de Personal y las Normas para la protección de datos personales para los Estados Iberoamericanos, y acogemos con beneplácito los esfuerzos para aprovecharlos para implementar altos estándares de protección de datos y privacidad a nivel mundial.

El trabajo de la GPA bajo su actual Plan Estratégico 2021-233 ha fomentado la cooperación entre las autoridades de todas sus regiones para garantizar altos estándares de datos a nivel mundial. Nuestro trabajo en los últimos años ha señalado, y ha tratado de resaltar, la amplia similitud en los marcos globales en términos de principios básicos, derechos y otros elementos, como en el análisis de 2020 del Grupo de Trabajo de Marcos y Estándares Globales de diez marcos globales4, y el análisis de 2021 de los mecanismos de transferencia5.

Aunque las diferentes jurisdicciones tienen diferentes sistemas legales, por lo que el enfoque y el detalle de sus leyes de privacidad y protección de datos difieren, se pueden ver similitudes y convergencias, especialmente en los principios y derechos fundamentales. En esta resolución, la GPA tiene como objetivo resaltar la importancia de los principios y estándares generales y el beneficio que pueden aportar para fomentar la convergencia y la interoperabilidad, y a su vez apoyar la cooperación internacional para proteger los datos personales de las personas a nivel mundial.

3 [2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf](https://globalprivacyassembly.org/wp-content/uploads/2021/10/2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf) [(globalprivacyassembly.org)](https://globalprivacyassembly.org/wp-content/uploads/2021/10/2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf)

4 [Day-1-1\_2a-Day-3-3\_2b-v1\_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-](https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf) [Report-Final.pdf (globalprivacyassembly.org)](https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf)

5 [1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org)](https://globalprivacyassembly.org/wp-content/uploads/2021/10/1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf)

También destacamos la contribución positiva que pueden aportar a este fin organizaciones internacionales y multilaterales como la OCDE y el Consejo de Europa, el G7 y el G20, otras organizaciones y redes de protección de datos como la Red Iberoamericana de Protección de Datos (RIPD), la Asociación de Naciones del Sudeste Asiático (ASEAN), la Cooperación Económica Asia-Pacífico (APEC), el Consejo Europeo de Protección de Datos (EDPB), la Red de Autoridades Africanas de Protección de Datos (NADPA/RAPDP), la Association francophone des autorités de protection des données personnelles (AFAPDP) y organismos de normalización como la Organización Internacional de Normalización (ISO).