Política global de protección de datos y privacidad de Ipsos

(en vigor a partir del 25 de mayo de 2018)

Política global de protección de datos y privacidad de Ipsos

Contenido

1. Introducción 4
2. Alcance 4
3. Aplicación de leyes nacionales y códigos de conducta 4
4. Principios del procesamiento de Datos Personales 5
   - 4.1. Licitud, lealtad y transparencia 5
   - 4.2. Limitación de la finalidad 5
   - 4.3. Minimización de datos 5
   - 4.4. Exactitud 6
   - 4.5. Limitación del periodo de conservación 6
   - 4.6. Integridad y confidencialidad 6
   - 4.7. Restricción de transferencia 6
   - 4.8. Medidas y consideraciones generales 6
5. Bases jurídicas para el procesamiento de datos 6
   - 5.1. Datos del respondiente 6
     - **5.1.1.** Consentimiento para el procesamiento de datos 6
     - **5.1.2.** Procesamiento de datos para una relación contractual 7
     - **5.1.3.** Procesamiento de datos de conformidad con la autorización legal 7
     - **5.1.4.** Procesamiento de datos de conformidad con el interés legítimo 7
     - **5.1.5.** Procesamiento de categorías especiales de Datos Personales 7
     - **5.1.6.** Datos del usuario e Internet 7
   - 5.2. Datos Personales proporcionados por clientes 8
   - 5.3. Datos de los empleados 8
     - **5.3.1.** Procesamiento de datos para la relación laboral 8
     - **5.3.2.** Procesamiento de datos de conformidad con la autorización legal 8
     - **5.3.3.** Convenios colectivos sobre procesamiento de datos 8
     - **5.3.4.** Consentimiento para el procesamiento de datos 8
     - **5.3.5.** Procesamiento de datos de conformidad con el interés legítimo 9
     - **5.3.6.** Procesamiento de categorías especiales de Datos Personales 9
     - **5.3.7.** Decisiones automatizadas 9
     - **5.3.8.** Telecomunicaciones e Internet 9
   - 5.4. Contactos de Mercadotecnia 10
6. Transferencias de Datos Personales 10
7. Terciarización/Procesamiento de datos por una tercera parte 11
8. Derechos del Interesado 12
9. Confidencialidad del procesamiento 12
10. Privacidad desde el diseño y por defecto 13
11. Seguridad de procesamiento 13
12. Auditoría de protección de datos 13
13. Incidentes de protección de datos 13
14. Responsabilidades y sanciones 14
    - 14.1. Gestión 14
    - 14.2. Data Protection Officers (DPO) 14
    - 14.3. Global Chief Privacy Officer 15

15. Derogación 15
16. Glosario 15
Controlador de datos/Controlador/Controlador adjunto 15
Usuarios de Datos 15
Procesador de Datos o Procesador 16
Interesados 16
Datos Personales 16
Procesamiento 16
Categorías especiales de datos (p/k/a datos personales sensibles) 16
Datos anónimos 17
Seudonimización 17
Información Personal Identificable (PII, por sus siglas en inglés) 17
Información de salud protegida (PHI, por sus siglas en inglés) 17
Datos personales sensibles (PSI, por sus siglas en inglés) 17

1. Introducción

Como parte de su responsabilidad social, Ipsos se compromete a cumplir a nivel internacional con las leyes, normas y los reglamentos de protección de datos. La política de protección de datos ("**Política**" o "**Política de Protección de Datos**") aplica mundialmente a Ipsos Group y se fundamenta en principios básicos de protección de datos globalmente aceptados. Asimismo, adopta los principios fundamentales de protección de datos del Reglamento General de Protección de Datos de la Unión Europea (*General Data Protection Regulation, "**GDPR**"*) como el estándar mínimo al cual tanto Ipsos Group como sus empleados y proveedores deberán adherirse.

Ipsos depende de la recopilación y el análisis de datos de particulares ("**Interesados**") para llevar a cabo sus investigaciones de mercados y negocios relacionados. Con el fin de seguir contando con la confianza de los respondientes y del público en general, es necesario que los respondientes no sufran consecuencias adversas, riesgos o daños al proporcionar su información o Datos Personales (consulte el Glosario para ver la definición y explicación de este término y otros marcados con mayúscula inicial) a Ipsos (para que este la procese con fines de negocios). La información puede obtenerse a través de cualquier tipo de individuo u organización.

Para dirigir su negocio, Ipsos también necesita recopilar y procesar información sobre las personas con quien opera, por ejemplo de empleados, proveedores, clientes actuales, anteriores y futuros, así como otros con quienes pueda comunicarse. Además, Ipsos está obligado por ley a procesar ocasionalmente algunos Datos Personales para cumplir con algunos requisitos legales.

Esta política describe los estándares básicos sobre cómo procesar, recopilar, manejar y almacenar los Datos Personales para cumplir con los estándares de protección de datos de Ipsos.

Los Usuarios de Datos están obligados a cumplir con esta Política al procesar los Datos Personales en representación de Ipsos. Cualquier violación de esta Política puede resultar en medidas disciplinarias e incluso despido.

2. Alcance

La Política se aplica globalmente a todas las empresas de Ipsos sin importar su sede, la cual sirve como el estándar mínimo al que todas las empresas, los empleados y proveedores de Ipsos deberán adherirse, sin importar si el *GDPR* aplica directamente a alguna actividad o territorio específico.

Todo aquél que trabaje para Ipsos tiene cierta responsabilidad de asegurar la adecuada recopilación y manejo de los Datos Personales.

El manejo y procesamiento de Datos Personales en cumplimiento con esta Política y sus principios de protección de datos es responsabilidad de todos.

Asimismo, Ipsos espera que sus proveedores/distribuidores cumplan con los principios establecidos en la presente.

3. Aplicación de leyes nacionales y códigos de conducta

La Política de Protección de Datos adopta principios de privacidad internacionalmente aceptados de acuerdo con las mejoras implementadas en el GDPR. Cabe mencionar que también depende de y complementa cualquier legislación nacional aplicable. Las leyes nacionales aplicables primarán en caso de suscitarse un conflicto con dicha Política o si aquellas establecen requerimientos más estrictos que ésta. Cualquier registro, notificación o requerimiento de reporte para el procesamiento de datos deberá cumplir con las leyes nacionales. En caso de no contar con una legislación nacional, deberá cumplirse con esta Política.

Todas las empresas de Ipsos Group están obligadas a cumplir con la Política de Protección de Datos y con las obligaciones jurídicas aplicables. Si existen motivos para considerar que dichas obligaciones jurídicas contradicen las responsabilidades contenidas en esta Política de Protección de Datos, la empresa en cuestión deberá informar al *Data Privacy Officer* (DPO) y al *Global Chief Privacy Officer*. En caso de conflicto entre la legislación nacional y esta Política de Protección de Datos, Ipsos colaborará con la empresa en cuestión para encontrar una

solución práctica que cumpla con los requerimientos y propósitos de esta Política y de la legislación aplicable.

Además de esta Política, Ipsos se adhiere a los requerimientos del Código Internacional ICC/ESOMAR para la práctica de la Investigación de Mercados, Opinión y Social y del Análisis de Datos, que puede consultar aquí.

4. Principios del procesamiento de Datos Personales

Sin importar cómo se recopilaron, registraron y procesaron (en papel, archivo electrónico, base de datos, grabado o en otro tipo de material), el tratamiento de los Datos Personales deberá ser el apropiado. Existen principios generalmente aceptados para asegurar esto, como lo establece la OCDE en sus Directrices sobre la Protección de la Privacidad y Flujo de Datos Transfronterizos, así como salvoconductos contemplados en varios estatutos alrededor del mundo, incluyendo el GDPR.

El tratamiento legal y apropiado de los Datos Personales y mantener la confianza de aquellos con quienes trata son componentes clave de las operaciones de negocios de Ipsos. Además, Ipsos se compromete a actuar ética y responsablemente al respetar dichos Datos Personales y a siempre proporcionar un alto nivel de confidencialidad y seguridad.

Para demostrar su compromiso, Ipsos se adhiere a los principios relacionados con el procesamiento de Datos Personales del GDPR, los cuales derivan de los principios de la OCDE. Ipsos respeta los siguientes principios en materia de Datos Personales, mismos que se explican a detalle más adelante:

- Procesamiento lícito y justo
- Procesamiento con finalidad limitada y apropiadamente definida
- Deben ser adecuados, relevantes y no excesivos para la finalidad
- Exactitud
- Periodo de conservación no mayor al necesario para la finalidad
- Procesamiento de acuerdo con los derechos de los Interesados
- Seguridad
- No transferencia a personas u organizaciones ubicadas en otros países sin la protección adecuada

4.1. Licitud, lealtad y transparencia

Los Datos Personales deberán procesarse y recopilarse de manera lícita, leal y transparente en relación con el Interesado. Además, debe informársele sobre el tipo tratamiento y manejo que se le está dando a sus datos. En general, los Datos Personales deben obtenerse directamente del individuo en cuestión. Cuando este no sea el caso, deberá documentarse la base jurídica que justifique la obtención, así como consultarse con el DPO responsable sobre si debería llevarse a cabo una evaluación del impacto en la protección de datos (DPIA, por sus siglas en inglés). Consulte por separado la guía sobre DPIA en la intranet.

4.2. Limitación de la finalidad

Los Datos Personales deberán recopilarse solamente con propósitos lícitos, específicos y explícitos sin que haya un procesamiento posterior incompatible con dichos propósitos. Los cambios subsecuentes a la finalidad sólo serán posibles hasta cierto punto y requieren de una justificación y validación. Deberá consultarse con el DPO responsable sobre si debería llevarse a cabo una evaluación del impacto en la protección de datos (DPIA, por sus siglas en inglés). Consulte por separado la guía sobre DPIA en la Intranet.

4.3. Minimización de datos

Los Datos Personales deberán ser adecuados, aplicables y limitarse a lo necesario en relación con el propósito para el que se procesaron. Deberá determinarse si se procesan los Datos Personales y hasta qué punto es necesario dicho procesamiento para cumplir con el propósito por el que se procesan. Deberán usarse datos anónimos cuando el propósito así lo permita y cuando el gasto realizado sea proporcional al propósito establecido.

4.4. Exactitud

Los Datos Personales deberán ser precisos y, cuando sea necesario, mantenerse actualizados. Deberán tomarse las medidas pertinentes para asegurar que se eliminen o corrijan inmediatamente los Datos Personales que sean imprecisos y que no cumplan con el objetivo para el cual se procesaron.

4.5. Limitación del periodo de conservación

Los Datos Personales no deberán retenerse de manera que permitan la identificación de los Interesados por más tiempo del necesario, para cumplir con el propósito por el cual se procesaron. Ipsos conservará los Datos Personales solo el tiempo necesario para cumplir con el fin o fines para los cuales fueron recopilados y tomará todas las medidas pertinentes para destruir o eliminar de sus sistemas todos los Datos Personales que ya no se requieran.

4.6. Integridad y confidencialidad

Los Datos Personales deberán procesarse de forma que no sean susceptibles a revelarse, divulgarse, manipularse ni que terceros accedan a ellos. Por lo tanto, cuando sea metodológicamente posible y el gasto no sea excesivo en relación con los riesgos del Interesado, se usarán datos seudonimizados para el procesamiento. NOTA: los datos seudonimizados son y seguirán siendo Datos Personales.

4.7. Restricción de transferencia

Los Datos Personales no deberán transferirse a otros países (incluso a otras empresas de Ipsos en dichos países) que no cuenten con un nivel adecuado de protección. En general, Ipsos ha emprendido varias medidas para garantizar un nivel de protección adecuado (consulte el párrafo 6 para más detalles). Sin embargo, varios países pueden tener más o diferentes requisitos que cumplir.

4.8. Medidas y consideraciones generales

En lo referente a la investigación de mercados, Ipsos cumple con el Código Internacional ICC/ESOMAR para la práctica de la Investigación de Mercados, Opinión y Social y del Análisis de Datos y la Lista de Control de Protección de Datos de ESOMAR.

5. Bases jurídicas para el procesamiento de datos

Ipsos recopilará, procesará y usará los Datos Personales sólo bajo las siguientes bases jurídicas, siempre que éstas se contemplen en las leyes nacionales aplicables. Si el propósito original de recopilar, procesar y usar los Datos Personales cambia, se requerirá una base jurídica a menos que haya una compatibilidad clara entre el propósito original y el nuevo. Consulte el párrafo 4.2 y cualquier posible requerimiento de cumplimiento adicional.

5.1. Datos del respondiente

Los respondientes son los Interesados más comunes en el negocio de Ipsos; por lo tanto, el tratamiento correcto de sus Datos Personales es un elemento central en el negocio de la empresa.

5.1.1. Consentimiento para el procesamiento de datos

Los Datos Personales solo podrán procesarse una vez que se tenga el consentimiento del Interesado. Previo a éste, deberá informársele al Interesado conforme al principio de transparencia como se establece en el párrafo 4.1. La declaración de consentimiento deberá obtenerse por escrito o electrónicamente con fines de documentación. En algunos casos, como en las entrevistas telefónicas, puede darse el consentimiento verbal. En todos los casos, deberá documentarse el consentimiento.

El consentimiento será válido solo si constituye la manifestación inequívoca, informada, específica y libre de los deseos del Interesado, quien mediante un acto afirmativo claro acepta que se procesen sus Datos Personales. Consulte la guía de consentimiento AQUÍ.

5.1.2. Procesamiento de datos para una relación contractual

Además del consentimiento, se procesarán los Datos Personales en un contrato cuando sea necesario. En dicho contrato se considerará a los Interesados como partes con derechos y obligaciones. Asimismo, esto se aplicará cuando el procesamiento sea necesario para establecer o terminar un contrato. Particularmente, aplicará a los respondientes (incluyendo a los *Mystery Shoppers*) que se registren en los paneles de Ipsos.

Algunos países entienden el establecimiento de un contrato como una forma de consentimiento.

5.1.3. Procesamiento de datos de conformidad con la autorización legal

Se permite el procesamiento de Datos Personales si la legislación nacional lo solicita, requiere o permite. Será necesario tener el tipo y extensión de procesamiento de datos para que dicha actividad sea legalmente autorizada y deberá cumplir con las disposiciones legislativas aplicables.

5.1.4. Procesamiento de datos de conformidad con el interés legítimo

Los Datos Personales también pueden procesarse si es necesario para el interés legítimo de Ipsos Group y cuando la legislación nacional así lo permita (ej., Artículo 6(1)(f) del GDPR). No todos los países reconocen la base jurídica del interés legítimo para el procesamiento, por lo que primará la legislación nacional relevante. En general, las categorías especiales de Datos Personales no pueden procesarse con base en el concepto de interés legítimo. En cualquier caso, los Datos Personales no pueden procesarse con base en el interés legítimo si, en el caso particular, existe evidencia de que los intereses del Interesado ameritan protección y que prima dicha protección. Antes de procesar los Datos Personales con base en interés legítimo, es necesario determinar si hay un interés que amerite protección. Además, la empresa de Ipsos Group en cuestión hará una evaluación del interés legítimo (por medio de una DPIA enfocada en el interés legítimo). El DPO o CPO correspondiente deberá validar cualquier evaluación.

5.1.5. Procesamiento de categorías especiales de Datos Personales

Es posible procesar las categorías especiales de Datos Personales solamente si la ley lo requiere o si el Interesado dio su consentimiento explícito. Consulte la guía sobre consentimiento AQUÍ. También es posible procesar categorías especiales de Datos Personales si es obligatorio para presentar, ejercer o defender reclamaciones jurídicas. De igual forma, dentro de la AEE se pueden procesar categorías especiales de Datos Personales con fines estadísticos y de investigación científica e histórica (Artículo 9(2)(j)), sujetas a las medidas adicionales adecuadas. Deberá solicitarle asesoramiento al DPO o CPO antes de remitirse a estas disposiciones.

5.1.6. Datos del usuario e Internet

Si se recopilan, procesan y usan Datos Personales en páginas web o aplicaciones, deberá informarse a los Interesados sobre la Política de Privacidad, incluyendo, si aplica, la información sobre *cookies* o medidas técnicas similares. La Política de Privacidad y cualquier información relacionada con las cookies deberán estar integradas para que sea de fácil identificación, directamente accesible, de fácil comprensión y esté constantemente disponible para el Interesado.

En caso de crearse perfiles de usuario (seguimiento) para evaluar el uso de las páginas web y aplicaciones, deberá informarse a los Interesados en el Aviso de Privacidad. El seguimiento en línea de los Interesados puede efectuarse solamente si las leyes nacionales o el consentimiento explícito de los Interesados lo permiten. Aun cuando se use un seudónimo para hacer el seguimiento del Interesado, en el Aviso de Privacidad, deberá dársele al Interesado la opción darse de baja (*opt-out*). En cuanto a la medición de audiencias en línea sin permiso previo de recibir información vía correo electrónico (*opt-in*), Ipsos se apega a los principios estipulados por researchchoices.com.

Si las páginas web o aplicaciones tienen acceso a los Datos Personales en un área restringida para usuarios/respondientes registrados, la identificación y autenticación de los Interesados deberá ofrecer la protección necesaria durante el acceso.

Como parte del compromiso de Ipsos de cumplir con el código de la ESOMAR, las leyes y el conjunto de requisitos establecidos en la Guía ESOMAR para la investigación en medios de

comunicación social, también se adhiere a las siguiente directrices: Guía ESOMAR para la investigación online y Guía ESOMAR sobre la investigación y análisis de datos con niños, jóvenes y otras personas vulnerables.

5.2. Datos Personales proporcionados por clientes

Comúnmente, los clientes de Ipsos hacen transferencias de Datos Personales. Esto generalmente sucede para proporcionarle a Ipsos una muestra o mejorar una muestra existente. En cuanto a los Datos Personales recibidos, Ipsos será el Procesador y solamente Procesará dichos Datos Personales de acuerdo con las instrucciones emitidas por el cliente, las cuales pueden incluir restricciones en materia de transferencia a terceros (incluyendo a otras empresas de Ipsos) o a otros países, así como requisitos de seguridad específicos. Deberán acatarse todas las restricciones. Es de suma importancia que dichas instrucciones se documenten por escrito y se llegue a un acuerdo antes de que Ipsos acepte cualquier acuerdo contractual. Lo anterior tiene el objetivo de asegurar que Ipsos puede cumplir con cualquiera de las restricciones o requisitos específicos del cliente.

Sin distinción de cuáles sean los requisitos de los clientes, cualquier Dato Personal proporcionado por alguno de ellos deberá cumplir con los siguiente:

a) Deberán procesarse exclusivamente para la finalidad con la que se recopilaron;
b) No deberán conservarse por más tiempo del necesario para cumplir con su finalidad
c) Estarán sujetos a los mismos requisitos de seguridad aplicables a los Datos Personales de Ipsos

5.3. Datos de los empleados

5.3.1. Procesamiento de datos para la relación laboral

De ser necesario, se pueden procesar los Datos Personales para iniciar, llevar a cabo o terminar relaciones laborales. Asimismo, se pueden procesar los Datos Personales de los solicitantes al iniciar una relación laboral. Si el candidato es rechazado, sus datos deben ser eliminados en cumplimiento con el periodo de conservación a menos que el solicitante haya aceptado permanecer registrado para un futuro proceso de selección. De igual manera, se necesita el consentimiento para usar los datos en futuros procesos de solicitud antes de compartir ésta con otras empresas de Ipsos.

En caso de existir una relación laboral, el procesamiento de datos siempre debe alinearse con el propósito de la relación laboral si no aplica ninguna de las siguientes circunstancias para dicho procesamiento autorizado.

Si fuera necesario que una tercera parte recopile información del solicitante durante el procedimiento de solicitud, deberá apegarse a los requisitos de las leyes nacionales correspondientes. En caso de duda, deberá obtenerse el consentimiento de los Interesados.

Deberá haber una autorización legal para procesar los Datos Personales que estén vinculados con la relación laboral y que originalmente no estaban incluidas en el alcance original del contrato laboral. Esto puede incluir requisitos legales, reglamentaciones colectivas con representantes de empleados, el consentimiento del empleado o el interés legítimo de la empresa.

5.3.2. Procesamiento de datos de conformidad con la autorización legal

Para más información sobre los requisitos, consulte el párrafo anterior 5.1.3.

5.3.3. Convenios colectivos sobre procesamiento de datos

Se autoriza que el procesamiento exceda su propósito con el fin de cumplir con el contrato, siempre y cuando se autorice por medio de un convenio colectivo entre los representantes del patrón y del empleado y esté dentro del alcance permitido de la ley del trabajo aplicable. Los convenios deberán cubrir la finalidad específica del procesamiento de datos posterior y deberá elaborarse de acuerdo con los parámetros de las legislaciones nacionales en materia laboral y de protección de datos.

5.3.4. Consentimiento para el procesamiento de datos

Los datos del empleado pueden procesarse después de obtener el consentimiento de la

persona en cuestión. Las declaraciones de consentimiento deben enviarse voluntariamente. Dentro de la UE/AEE, el consentimiento no constituye una base jurídica válida para el procesamiento en el contexto laboral, ya que existe la presunción jurídica de que dicho consentimiento no se envía voluntariamente y cualquier procesamiento tendrá que basarse en alguna otra de las estructuras jurídicas disponibles. El consentimiento involuntario no tiene validez. Para saber hasta qué punto el consentimiento es un fundamento válido para el procesamiento, consulte el párrafo 5.1.1 sobre los requisitos. Una complicación posterior es que normalmente el consentimiento puede revocarse, lo que impediría cualquier procesamiento posterior.

5.3.5. Procesamiento de datos de conformidad con el interés legítimo

De ser necesario los Datos Personales pueden procesarse para cumplir con el interés legítimo de Ipsos Group y donde la ley aplicable permita que el procesamiento de Datos Personales se base en el interés legítimo. Dentro del contexto laboral, los intereses legítimos son generalmente de naturaleza financiera.

Para más información sobre los requisitos y limitaciones del interés legítimo, consulte el párrafo anterior 5.1.4.

Solamente se podrán tomar medidas de control o de supervisión que requieran el procesamiento de datos de los empleados cuando haya una obligación jurídica para hacerlo o exista una razón legítima. Incluso si existe una razón legítima, deberá examinarse la proporcionalidad de las medidas de control antes de que dichas medidas se apliquen. Los intereses justificados de la empresa que aplica las medidas de control (ej., cumplimiento con los lineamientos internos de la empresa o intereses de seguridad) deberán ponderarse con cualquier interés del empleado afectado que amerite protección y cuyo interés se afectaría con la exclusión de dicha protección. Además, dicha medida no puede aplicarse a menos que sea apropiada. Antes de aplicar cualquier medida, tanto los intereses legítimos de la empresa que ameriten protección como los del empleado, deberán identificarse y documentarse por medio de una evaluación de intereses legítimos. Asimismo, cualquier requisito adicional incluido en la legislación nacional deberá tomarse en cuenta (ej., los derechos de determinación conjunta de los representantes del empleado y los derechos de información de los Interesados).

5.3.6. Procesamiento de categorías especiales de Datos Personales

Es posible procesar las categorías especiales de Datos Personales solamente si la ley lo requiere o si el Interesado da su consentimiento explícito. Las categorías especiales de Datos Personales pueden procesarse si es obligatorio para presentar, ejercer o defender reclamaciones jurídicas.

5.3.7. Decisiones automatizadas

Si los Datos Personales se procesan automáticamente como parte de una relación laboral y los detalles personales específicos se evalúan para la toma de decisiones (ej., como parte de un proceso de selección de personal o evaluación de resultados), este procesamiento automático no puede ser la única base para las decisiones que puedan acarrear consecuencias negativas o crear problemas importantes para el empleado afectado. Para evitar decisiones erróneas, el proceso automatizado deberá asegurar que una persona física evalúe el contenido de la situación y que dicha evaluación sea la base para la decisión. Deberá informarse a los Interesados de los hechos y resultados de las decisiones automatizadas y de la posibilidad de responder.

5.3.8. Telecomunicaciones e Internet

Ipsos proporcionará equipo telefónico, direcciones de correo electrónico, Intranet e Internet junto con las redes sociales internas para fines relacionados al trabajo; todas son herramientas y recursos de la empresa y podrán usarse en el marco de las leyes aplicables y las políticas internas de la empresa, particularmente en el marco de la Política de Seguridad de la Información y Uso Aceptable. En caso de que se autorice su uso para fines privados, es necesario cumplir con la respectiva disposición de inviolabilidad de las telecomunicaciones privadas contemplada en las leyes nacionales de telecomunicaciones, en caso de que aplique.

Ipsos usa tecnología de filtro web para asegurar el cumplimiento con su Política de Uso Aceptable, hacer análisis y mediciones del tráfico en Internet, asegurar el cumplimiento con otras obligaciones jurídicas y defenderse de ataques en la infraestructura tecnológica informática o de usuarios individuales. Pueden implementarse medidas de seguridad en las conexiones de la red de Ipsos con el fin de bloquear contenido técnicamente dañino, así como

para analizar los patrones de ataque. Por motivos de seguridad, puede bloquearse temporal o permanentemente el uso del equipo telefónico, dirección de correo electrónico, Intranet/Internet y las redes sociales de algunas direcciones/ubicaciones de algunos individuos o tipos de conexión. Las evaluaciones de esta información que haga una persona específica, solo podrán realizarse en el caso justificado y concreto de que haya sospechas de violaciones a la ley o las políticas de Ipsos Group y debe ser autorizada por cualquier/cualesquiera de la(s) persona(s) que puedan autorizar un "derecho legal de retención" (consulte la Política de Gestión de la Información de TI). Es necesario cumplir tanto con la respectiva ley nacional como con las leyes grupales.

5.4. Contactos de Mercadotecnia

En general, en materia de la protección de privacidad otorgadas a los contactos de mercadotecnia son iguales a aquellas otorgadas a los respondientes. Sus detalles de contacto se consideran Datos Personales, aun cuando estén relacionado con la empresa. Solamente quedarán exentos de esta política aquellos contactos cuyos detalles son completamente genéricos (ej., contacto@acme.com).

Frecuentemente, las comunicaciones de mercadotecnia están sujetas a requisitos legales específicos, particularmente si se envían electrónicamente o se realizan vía telefónica.

Debe asumirse que los contactos de mercadotecnia no solicitaron los materiales de mercadotecnia; en otras palabras, los destinatarios no pidieron recibir comunicación relacionada con mercadotecnia de Ipsos. Para proceder legalmente, las condiciones relacionadas con esta base jurídica, en particular los requisitos del consentimiento establecidos en el párrafo 5.1.1, son igualmente aplicables en este caso.

Excepcionalmente se puede aplicar la aceptación indirecta de mensajes vía correo electrónico si se cumplen las siguientes condiciones:

- Cuando los detalles del Interesado se hayan obtenido durante una venta o negociación de servicios de Ipsos
- Cuando los mensajes estén relacionados solamente con servicios similares de mercadotecnia
- Cuando a la persona se le dé solo una oportunidad de no autorizar correos de mercadotecnia cuando se recopilan sus datos de contacto y de no seleccionar la opción de rechazar en ese momento, se le dará la opción sencilla para seleccionarla en todos los futuros mensajes.

6. Transferencias de Datos Personales

La transferencia de Datos Personales a destinatarios fuera o dentro de Ipsos Group está sujeta a los requisitos de autorización para el procesamiento de Datos Personales establecidos en el párrafo 4.7 (Restricción de transferencias). Se les solicitará a los destinatarios de los datos (ya sea otra empresa de Ipsos o algún subcontratista) que usen los datos exclusivamente para los fines establecidos. Para transferencias externas, los requisitos del presente párrafo y aquellos establecidos en el párrafo 7 (Terciarización/Procesamiento de datos por una tercera parte) se aplicarán de forma acumulativa.

Si se transmiten los Datos Personales a un destinatario en un tercer país fuera de Ipsos Group, el destinatario deberá comprometerse por escrito mantener un nivel de protección de datos equivalente al de la presente Política de Protección de Datos o según lo requiera la ley aplicable. Por ejemplo, el GDPR estipula varios requisitos que deben cumplirse antes de llevar a cabo una transferencia, pero esto no aplica si la transmisión se basa en una obligación jurídica. Una obligación jurídica de esta naturaleza puede basarse en las leyes del país encargado de la transferencia de datos donde se ubique la empresa de Ipsos Group. Como alternativa, las leyes del país donde se ubique la empresa de Ipsos Group pueden reconocer la finalidad de la transferencia de datos basándose en las obligaciones jurídicas de un tercer país.

Cuando un tercero transmita los Datos Personales a una empresa de Ipsos Group (ej., un proveedor de muestras), deberá asegurarse de que los Datos Personales puedan usarse para dicho propósito.

Si una empresa de Ipsos Group con oficina registrada en un país transmite los Datos Personales a otra empresa de Ipsos Group con oficina registrada en otro país, la empresa importadora de los datos está obligada a cooperar con las investigaciones realizadas por la entidad reguladora aplicable del país en el cual la parte exportadora de datos tenga su oficina registrada. Asimismo, la parte importadora deberá cumplir con las observaciones realizadas por dicha entidad en relación con los datos transferidos.

Si un Interesado afirma que la presente Política de Protección de Datos fue violada por una empresa exportadora de datos de Ipsos Group ubicada en otro país, la empresa exportadora de Datos Personales de Ipsos Group se comprometerá a apoyar al Interesado en cuestión, estableciendo los hechos del asunto y haciendo valer los derechos del Interesado de acuerdo con la presente Política de Protección de Datos ante la empresa importadora de datos de Ipsos Group. Además, el Interesado está autorizado a hacer valer sus derechos ante la empresa exportadora de datos de Ipsos Group. En el supuesto de que haya reclamaciones de violación, la empresa exportadora deberá documentar ante los Interesados que la empresa importadora de Datos Personales no violó la Política de Protección de Datos.

Toda empresa de Ipsos Group que transfiera Datos Personales a una empresa de Ipsos Group ubicada en otro país será responsable de cualquier violación a la Política de Protección de Datos cometida por la empresa de Ipsos Group receptora de los datos, como si la violación la hubiese cometido la empresa de Ipsos Group que los transfirió.

Cualquier transferencia de Datos Personales dentro de Ipsos Group, solamente se realizará después de haya un registro aplicable en el JobBook del proyecto para el cual la transferencia se lleve a cabo. Dicho registro creará un contrato dentro del Convenio Maestro de Prestación de Servicios de Ipsos Intragroup, lo que automáticamente vuelve aplicables las respectivas cláusulas tipo de la UE a dicha transferencia.

7. Terciarización/Procesamiento de datos por una tercera parte

En muchos casos, Ipsos recurre a proveedores externos para el procesamiento de Datos Personales. En estos casos, deberá celebrarse un contrato de procesamiento de datos a nombre de Ipsos con dicho proveedor. Esto puede realizarse de dos formas: incluyendo las disposiciones necesarias en el acuerdo que rige la relación general con el proveedor o redactarlas por separado en un documento específico. En relación con el procesamiento a nombre de Ipsos, el proveedor deberá procesar los Datos personales de acuerdo con las instrucciones de Ipsos. Al dar instrucciones a un proveedor, deberá cumplirse con los siguientes requisitos:

- Cuando los Datos Personales en cuestión recaigan en el párrafo 5.2 (Datos del cliente), deberá proporcionársele al proveedor cualquiera de los requisitos aplicables del cliente
- Deberá elegirse al proveedor con base en su capacidad para cumplir con las medidas requeridas por Ipsos tanto técnicas como de protección y estar de acuerdo con el proceso de aprobación de proveedores de Ipsos
- El proveedor no deberá subcontratar el procesamiento sin el previo consentimiento por escrito de Ipsos
- Las instrucciones deberán presentarse por escrito mediante un contrato apropiado. Deberán documentarse las instrucciones sobre el procesamiento de datos, las responsabilidades de Ipsos y del proveedor
- Antes de procesar los datos, Ipsos deberá estar seguro de que el proveedor cumplirá con sus responsabilidades. Un proveedor puede documentar su cumplimiento con los requisitos de seguridad de datos, en especial si presenta una certificación adecuada. Dependiendo del riesgo del procesamiento de datos, deberán repetirse las revisiones constantemente durante la duración del contrato. Ipsos se reserva el derecho de auditar el cumplimiento del proveedor
- En caso de un contrato transfronterizo de procesamiento de datos, deberá cumplirse con los requisitos nacionales aplicables para revelar Datos Personales en el extranjero. Los datos personales del AEE pueden procesarse en un tercer país solamente si el proveedor comprueba que su Política de Protección de Datos cuenta con un estándar de protección de datos equivalente al del GDPR y a la presente Política de Protección de Datos. Los instrumentos adecuados pueden ser:

- Un contrato basado en las cláusulas estándar de la UE sobre el contrato de procesamiento de datos en otros países con el proveedor. Asimismo, se requerirán contratos similares para cualquier subcontratista del proveedor
- Que el proveedor cuente con un sistema de certificación aprobado por la UE para proporcionar un nivel suficiente de protección de datos

8. Derechos del Interesado

Todos los Interesados gozan de los derechos que a continuación se enuncian. La empresa correspondiente de Ipsos gestionará de inmediato la solicitud del Interesado y no generará ninguna desventaja para el mismo. Cuando Ipsos esté procesando los Datos Personales proporcionados por clientes de acuerdo con lo estipulado en el párrafo 5.2 (Datos Personales), deberá consultarse en el contrato del cliente sobre el proceso a seguir y deberá informársele de inmediato al cliente sobre dicha solicitud.

- **Derecho de acceso**:
  - El Interesado puede solicitar información sobre los Datos Personales suyos que se hayan almacenado, cómo se recopilaron y con qué finalidad
  - Si los Datos Personales se transfirieren a terceros, deberá proporcionarse información sobre la identidad o categoría de los destinatarios, incluyendo otras empresas de Ipsos
- **Derecho de rectificación**: Si los Datos Personales fueran incorrectos o estuvieran incompletos, los Interesados pueden exigir que se corrijan o completen.
- **Derecho de cancelación**: Cuando los Datos Personales se procesen basándose en el consentimiento (consulte la guía independiente sobre consentimiento), los Interesados pueden objetar el proceso en cualquier momento. Deberán bloquearse los Datos Personales objetados.
- **Derecho de supresión**: El Interesado puede solicitar que sus datos se eliminen si el procesamiento de dichos datos no tiene bases jurídicas o dichas bases ya no aplica. Lo mismo procede si la finalidad del procesamiento de datos es inválida o ya no aplican por otras razones. Deberán supervisarse los periodos de conservación y el conflicto de intereses que ameriten la protección.
- **Derecho de oposición**: En general, los Interesados tienen derecho a oponerse al procesamiento de sus datos y deberá tomarse en cuenta si la protección de sus intereses prima sobre los intereses del Controlador de Datos dada la situación personal del Interesado. Dicho derecho no aplica cuando el procesamiento de Datos Personales se requiere por disposición jurídicas. El contrato de trabajo con…
- **Derecho a la portabilidad de datos**: El Interesado tiene derecho a solicitar que los Datos Personales que proporcionó estén disponibles para su uso en un formato que sea fácil de leer como un documento de Word o Excel.

9. Confidencialidad del procesamiento

Los Datos Personales son confidenciales. Queda prohibida la recopilación, el procesamiento o uso de dichos datos por parte de los empleados. Asimismo, queda prohibido todo procesamiento de datos llevado a cabo por un empleado que no tenga autorización para efectuarlo como parte de sus tareas legítimas. Se aplica el principio de “necesidad de conocer”. Los empleados pueden tener acceso a los Datos Personales siempre y cuando apropiado para el tipo y alcance de la actividad en cuestión. Lo anterior requiere un desglose, una división cuidadosa y una delimitación de funciones y responsabilidades. Asimismo, se aplican los requisitos de la Política de Gestión de la Información.

Aqueda prohibido que los empleados usen Datos Personales para fines personales o comerciales propios, así como divulgarlos a personas no autorizadas o dar acceso a los datos de cualquier otra forma. Los supervisores deben informar a los empleados sobre la obligación de confidencialidad de datos desde el inicio de su relación laboral. Dicha obligación permanecerá vigente aun cuando la relación laboral haya finalizado. Los contratos laborales con el personal de Ipsos deberán contener las obligaciones de confidencialidad adecuadas.

10. Privacidad desde el diseño y por defecto

Ipsos usará un enfoque de Privacidad desde el diseño y por defecto en todo su trabajo, particularmente cuando:

- Construya nuevos sistemas de TI para almacenar o acceder a Datos Personales
- Desarrolle nuevas aplicaciones o enfoques de investigación
- Se involucre en iniciativas para compartir datos
- Use los datos con nuevas finalidades

La privacidad desde el diseño es un enfoque a los proyectos que promueve la privacidad de datos y el cumplimiento con la protección de datos desde un inicio. Es una consideración clave en las primeras etapas y posteriormente, a todo lo largo de cada proyecto.

Adoptar un enfoque de privacidad desde el diseño es una herramienta esencial para minimizar riesgos de privacidad, construir confianza y voluntad al diseñar proyectos, procesos, productos o sistemas teniendo en mente la privacidad desde el principio.

Con respecto a lo anterior, el instrumento requerido para el cumplimiento una evaluación del impacto en la protección de datos.

11. Seguridad de procesamiento

Los Datos Personales deberán salvaguardarse de cualquier acceso o divulgación no autorizados (interno o externo), de procesamiento ilegal, así como de la pérdida, modificación o destrucción accidental. Lo anterior aplica sin distinción entre datos procesados electrónica o físicamente. Además de asegurar que los Datos Personales existentes cumplan con las políticas aplicables de Ipsos (consulte el Capítulo 7 Políticas y procedimientos del manual de Ipsos al respecto), antes de introducir nuevos métodos de procesamiento de datos, en particular nuevos sistemas de TI, deberán definirse e implementarse las medidas técnicas u organizacionales para proteger datos personales. Dichas medidas deberán basarse en tecnología de punta, el riesgo del procesamiento y la protección de datos. Tales medidas técnicas y organizacionales deberán acordarse en colaboración con el Information Security Officer y el DPO a cargo. Las medidas técnicas y organizacionales para proteger los Datos Personales son parte de la Gestión de Seguridad de la Información Empresarial y deberán ajustarse continuamente al desarrollo técnico, a los avances y cambios organizacionales.

Como mínimo, Ipsos procesará todos los Datos Personales que conserva de acuerdo con su política de seguridad y tomará todas las medidas de seguridad pertinentes contra el procesamiento ilegal o no autorizado, la pérdida accidental o daño de Datos Personales.

12. Auditoría de protección de datos

El cumplimiento con la presente Política de Protección de Datos y las leyes de protección aplicables se supervisa constantemente por medio de auditorías de protección de datos y otros controles. Vigilar el desempeño de estos controles es responsabilidad del CPO, DPO y del auditor interno/externo que se contrate. Varios clientes de Ipsos también tienen derechos de auditoría de acuerdo con los contratos con Ipsos. Deberán reportarse los resultados de las auditorías de protección de datos al CPO y al Responsable del Cumplimiento. Los resultados de las auditorías de protección de datos deberán ponerse a disposición de las autoridades responsables de protección de datos cuando así lo soliciten.

13. Incidentes de protección de datos

Todos los empleados deberán informar inmediatamente al DPO o CPO sobre violaciones a la presente política de protección de datos o a otras reglamentaciones sobre la protección de Datos Personales de conformidad con el Procedimiento de Gestión de Fugas de Información, disponible en la Sección 8 del Manual de Políticas y Procedimientos de Ipsos. Toda falta en la resolución de temas mencionados en esta Política puede reportarse en el sistema Ipsos Whistle-blowing.

Use dicho sistema en los siguientes casos:

- Cuando exista una transferencia indebida de Datos Personales a terceras partes
- Cuando exista una transferencia de Datos Personales transfronteriza indebida
- Acceso indebido a Datos Personales (incluyendo terceras partes) o
- Pérdida de Datos Personales (incluyendo cuando se hace pública por fallas internas)

Deberá notificarse inmediatamente sobre cualquier violación a la protección de datos para asegurar lo siguiente: a) que se cumplan todas las responsabilidades contempladas en la ley nacional; b) que se informe a todo cliente afectado; y c) que haya comunicación adecuada con los clientes. Toda violación a la protección de datos también constituirá un incidente de seguridad de la información dentro de la Política de Gestión de Incidentes de TI.

14. Responsabilidades y sanciones

14.1. Gestión

Los órganos ejecutivos de las respectivas empresas de Ipsos Group son responsables del procesamiento de información en su área de responsabilidad. Por lo tanto, tienen la obligación de asegurar el cumplimiento de los requisitos legales y aquellos contenidos en esta política de protección de datos (ej., informe nacional o cumplir las conforme a las leyes locales).

La administración es responsable de asegurar que las medidas organizacionales, de Recursos Humanos y técnicas se apliquen para que todo procesamiento de datos se realice de acuerdo con los requisitos de protección de datos aquí contenidos.

El cumplimiento con estos requisitos también es responsabilidad de los empleados en cuestión.

En caso de que algún organismo oficial realice auditorías de protección de datos, deberá informarse inmediatamente al CPO al respecto.

El país donde se encuentre la administración de Ipsos en cuestión deberá informar tanto al CPO como al DPO.

El procesamiento indebido de Datos Personales u otras violaciones a las leyes de protección de datos pueden acarrear acciones penales en muchos países y resultar en reclamaciones para la compensación de daños. Adicionalmente, las violaciones de las que cada empleado resulte responsable pueden implicar sanciones dentro del ámbito de las leyes laborales.

14.2. Data Protection Officers (DPO)

Cada país será responsable donde labore Ipsos deberá designar a uno o más Data Protection Officers ("**DPO**"). Los DPO son el contacto interno y externo en el país en materia de protección de datos. Los DPO pueden hacer revisiones y deben familiarizar a los empleados con los contenidos de esta Política de Protección de Datos y la legislación aplicable. La administración deberá asistir a los DPO en sus esfuerzos. A continuación, se enlistan las principales responsabilidades de los DPO son:

- *Informar y asesorar a la organización y a sus empleados sobre sus obligaciones de cumplir con las leyes aplicables de protección de datos y la Política de Protección de Datos.* Esta responsabilidad será secundada y guiada en grupo y por medio de la red de DPO y bajo el liderazgo y capacitación del CPO
- *Supervisar el cumplimiento con las leyes de protección de datos, incluyendo la gestión de actividades de protección de datos internos; asesorar (no realizar) sobre evaluaciones de impacto en la protección de datos; capacitar al personal y realizar auditorías internas.* Esta responsabilidad será apoyará y guiará en grupo. Las auditorías deberán coordinarse con el grupo de auditoría interna, excepto las revisiones aleatorias
- *Ser el primer contacto de las autoridades de control y de aquellos individuos cuyos datos sean procesados (empleados, clientes, etc.)*

Dentro de cada país donde labore Ipsos, el DPO deberá:

- Reportar al puesto administrativo más alto de la organización de Ipsos en el país. Por ejemplo, a nivel administrativo o entre miembros de la junta directiva local
- Operar independientemente de las órdenes profesionales y no ser destituido o penalizado por realizar dicha actividad
- Contar con todos los recursos adecuados para facilitarle al DPO cumplir con sus obligaciones dentro de las leyes aplicables de protección de datos y la presente Política de Protección de Datos

Los DPO deberán informar inmediatamente al CPO de cualquier riesgo en la protección de datos.

14.3. Global Chief Privacy Officer

El Global Chief Privacy Officer ("**CPO**") trabaja independientemente de las órdenes profesionales y en aras del cumplimiento con las leyes de protección de datos nacionales e internacionales. También es responsable de la política de protección de datos y de supervisar su cumplimiento.

Cualquier Interesado puede acercarse al CPO o al DPO en cuestión en cualquier momento para expresar sus inquietudes, solicitar información o presentar una queja sobre la protección de datos o problemas en la seguridad de datos. La gestión de las inquietudes y quejas será confidencial si así se solicita.

Si el DPO en cuestión no puede resolver una queja o solucionar una violación a la política de protección de datos, deberá consultar al CPO inmediatamente. La administración de la empresa en cuestión deberá apoyar las decisiones del CPO orientadas a solucionar la violación de la protección de datos. Las investigaciones de los organismos de control siempre deberán reportarse al CPO.

15. Derogación

En casos excepcionales, es posible derogar la presente política antes de procesar los Datos Personales del Interesado. Cualquier derogación, requerirá una evaluación completa del impacto en la protección de datos para establecer y evaluar los riesgos a los que cualquier Interesado podría estar sujeto; los riesgos jurídicos y el impacto en su reputación, y dicha derogación estará sujeta a la aprobación del Presidente de Servicios de Apoyo de Ipsos.

16. Glosario

Controlador de datos/Controlador/Controlador adjunto

Es la persona u organización encargada de determinar las finalidades y el modo en que se procesa cualquier Dato Personal. Asimismo, es responsable de establecer prácticas y políticas de acuerdo con los requisitos legales aplicables.

En la mayoría de los casos cuando Ipsos recibe una muestra del cliente, Ipsos será el Controlador Adjunto de los datos recopilados. Lo anterior incluye los datos recopilados por Ipsos, aun cuando se les haya asegurado a los respondientes sobre la confidencialidad de sus respuestas. Las responsabilidades y obligaciones de los Controladores Adjuntos deberán documentarse y aclararse en un contrato escrito.

Algunas jurisdicciones usan otras expresiones para el mismo concepto: **Encargado**, **Organización**, **Operador**[1], etc.

Usuarios de Datos

Son aquellos empleados de Ipsos cuyo trabajo implica procesar Datos Personales. Los Usuarios de Datos deberán proteger los datos y los Datos Personales que manejan de acuerdo con esta política y cualquier procedimiento de seguridad de datos aplicable en todo momento.

[1] Singapur

Procesador de Datos o Procesador

Es la persona u organización no es Usuaria de Datos y que se encarga de procesar Datos Personales a nombre del Controlador y por instrucciones del Controlador. Se excluye de esta definición a los empleados de Controladores de Datos, pero puede incluirse a los proveedores que manejan Datos Personales. Ipsos será un Controlador en diversas ocasiones (ej., en el caso de los panelistas o muestras ad-hoc que Ipsos reclute para una encuesta) o un Procesador (ej., en el caso de las muestras proporcionadas por clientes). Algunas jurisdicciones usan otras expresiones para el mismo concepto: **Tercera Parte**, **Intermediario**, **Operador**[2], etc.

Interesados

Para fines de la presente política, esto incluye a todos los individuos vivos de quienes una Empresa de Ipsos conserva Datos Personales. Un Interesado no necesariamente es un nativo o residente del país. Todos los Interesados tienen derechos legales sobre su información personal.

Datos Personales

La definición del GDPR de Datos Personales (Artículo 4 (1) del GDPR) aclara el concepto de Datos Personales y muestra que debe interpretarse ampliamente:

"…toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

Una persona física es un individuo vivo y el GDPR no es aplicable a individuos fallecidos. Sin embargo, cada estado miembro puede crear normas relacionadas con el procesamiento de Datos Personales incluso para personas fallecidas.

La información relacionada con una empresa no formará parte de los Datos Personales.

Debe reconocerse que no siempre es posible determinar con absoluta certeza si cierta información específica constituye Datos Personales. Será necesario revisar la información general que se conserva sobre la persona en cuestión o los medios razonablemente similares para identificar a una persona. Con los medios tecnológicos en constante mejora, más datos se considerarán Datos Personales.

Procesamiento

Es una actividad que requiere el uso de datos; incluye recopilar, registrar, conservar los datos o realizar una operación o conjunto de operaciones con los datos incluyendo la organización, la rectificación, la recopilación, el uso, la divulgación y la supresión o eliminación de esta. El procesamiento también incluye la transferencia de Datos Personales.

Categorías especiales de datos (p/k/a datos personales sensibles)

"Categorías especiales de Datos Personales" es la nueva expresión usada en el GDPR, la cual anteriormente se refería a "datos sensibles". Actualmente se define en el Artículo 9 del GDPR como datos relacionados con:

El origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos [ver abajo], datos biométricos [ver abajo] dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud [ver abajo] o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

El GPDR detalla algunas de estas expresiones y las define:

"Datos genéticos" datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

[2] Sudáfrica

"Datos biométricos": datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

"Datos relativos a la salud": datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

Datos anónimos

Se define como información que no se relaciona con una persona física identificada o identificable o a Datos Personales en función de los anónimos, de manera que el Interesado no sea o deje de ser identificable (GDPR Razón 26). Debe distinguirse de la información que junto con la información adicional (ej., una clave), puede usarse para identificar una persona física cuando los datos sean meramente seudonimizados.

Los datos seudonimizados quedan dentro de la definición de Datos Personales y, por lo tanto, se les aplican los principios y requisitos completos del GDPR.

Seudonimización

Seudonimización se refiere "al tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable" (Artículo 4 (5) del GDPR).

Los datos seudonimizados define refieren a los datos identificadores de un conjunto de información que son remplazados con identificadores artificiales, o seudónimos, que se conservan a parte y están sujetos a una salvaguarda técnica. Los datos seudonimizados siguen siendo Datos Personales; por lo tanto, siguen siendo aplicables todos los demás requisitos de protección de datos.

Información Personal Identificable (PII, por sus siglas en inglés)

Este término proviene de la legislación de privacidad de EE. UU. Pese a que, vistos desde la perspectiva aplicable al trabajo del día a día en Ipsos, los términos Datos Personales y PII pueden considerarse como sinónimos, el uso de la expresión PII en el contexto de la GDPR debe evitarse, pues impacta negativamente nuestra obligación para demostrar cumplimiento. Los organismos reguladores se apegan mucho a la consistencia y precisión en el uso de expresiones.

Información de salud protegida (PHI, por sus siglas en inglés)

Este término también proviene de la legislación de privacidad de EE. UU., particularmente de la *Health Insurance Portability and Accountability Act* (*HIPAA*). Pese a que desde la perspectiva aplicable al trabajo del día a día en Ipsos, las expresiones de Datos Personales y PII pueden considerarse como sinónimos, el uso de la expresión PII en el contexto de la GDPR debe evitarse.

El principal problema por considerar es que ciertos Datos Personales que se considerarían dentro de la definición legal de PHI, en el GDPR forman parte de los Datos Personales en vez incluirse en las categorías especiales de datos. Por ejemplo, el HIPPA consideraría como PHI toda la información de un conjunto de datos que contiene el nombre y la orientación sexual, mientras que el GDPR solamente consideraría que la orientación sexual forma parte de las categorías especiales de Datos Personales.

Datos personales sensibles (PSI, por sus siglas en inglés)

Actualmente, esta expresión es obsoleta, pues proviene de la legislación anterior. En buena medida, es sinónimo de categorías especiales de Datos Personales, como las definen en el Artículo 9 del GDPR y esa es la expresión que debe usarse. Los organismos reguladores esperan que Ipsos use correctamente la terminología para demostrar cumplimiento como una parte del deber de Ipsos de rendir cuentas.

Control de Documentos (Art 25 GDPR)

Versión	Fecha	Resumen de cambios	Autores	Aprobado por
1.0	12.04.2018	Versión aprobada para publicación	Rupert van Hullen	**Laurence Stoclet**

Revisión del documento	
Fecha de última revisión	12.04.2018
Versión revisada	1.0
Cambios propuestos (Enlistar el No. de capítulo y una breve descripción de los cambios)	N/A
Comité de revisión	CPO, GC, CIO, MarCom
Comité/Autoridad de aprobación	Deputy CEO & CFO
Próxima fecha de revisión	12.04.2019
Nota: los registros de esta tabla, no cambiarán el número de la versión.	