Libro de Políticas y Procedimientos de Ipsos

Sección 8: Privacidad y Protección de Datos

8.1 Política Global de Privacidad y Protección de Datos

Fecha de Emisión	Septiembre 2018
Documento	8.1
Propietario	Rupert van Hullen
Revisión del Documento	
Última Fecha de Revisión	Septiembre 2024
Versión Revisada	Septiembre 2023
Cambios Propuestos (Indique el capítulo y breve descripción de los cambios)	Actualizado para reflejar la política actual de Ipsos
Comité de Revisión	Libro Global de Políticas y Procedimientos de Ipsos Equipo
Autoridad/Comité de Aprobación	Dan Levy
Próxima Fecha de Revisión	Será revisado de acuerdo con las políticas internas de Ipsos y/o los requisitos del sector
Nota: Los registros dentro de esta tabla no generarán un cambio en el número de versión.	

1. Índice

2. Introducción

Como parte de su responsabilidad social, Ipsos se compromete al cumplimiento internacional con las leyes, regulaciones y normas de protección de datos. Esta política de privacidad y protección de datos ("Política" o "Política de Protección de Datos") se aplica a nivel mundial a todas las empresas del Grupo Ipsos y se basa en principios básicos globalmente aceptados sobre la protección de datos. Esta Política adopta los principios fundamentales del RGPD ("GDPR") de la UE como el estándar mínimo al que deben adherirse las entidades del Grupo Ipsos, sus empleados y proveedores. Aunque esto debería ser obvio, no hace que el GDPR en sí mismo sea aplicable globalmente al Grupo Ipsos.General Data Protection Regulation

Ipsos depende de la recopilación y análisis de información sobre individuos identificables vivos ("Sujetos de Datos") para llevar a cabo su investigación de mercado, opinión y sociales y los negocios asociados. Mantener la confianza de los encuestados y del público requiere que los encuestados no sufran consecuencias adversas directas, riesgos o daños como resultado de proporcionar a Ipsos su información o sus Datos Personales (para una definición y explicación de este término y otros términos en mayúsculas, por favor vea el Glosario al final de este documento) o que estos sean procesados para los propósitos comerciales de Ipsos. La información puede obtenerse de cualquier tipo de individuo u organización.

Para llevar a cabo su negocio, Ipsos también necesita recopilar y procesar ciertos tipos de información, incluidos los Datos Personales, sobre las personas con las que Ipsos trata. Estos incluyen empleados actuales, pasados y potenciales, proveedores, clientes y otros con quienes pueda comunicarse. Además, ocasionalmente Ipsos puede ser requerido por ley para procesar ciertos tipos de Datos Personales para cumplir con ciertos requisitos legales.

Esta Política describe los estándares mínimos de cómo deben ser procesados, recopilados, manejados y almacenados 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 Datos Personales en nombre de Ipsos. Cualquier violación de esta Política puede resultar en acciones disciplinarias, hasta e incluyendo el despido de Ipsos.

3. Alcance

La Política es aplicable globalmente a todas las empresas de Ipsos, sin importar dónde estén basadas. Dentro de Ipsos, esta Política formará el estándar mínimo al cual todas las empresas de Ipsos, empleados y proveedores deben adherirse, sin importar si el GDPR se aplica directamente a cualquier actividad específica o territorio.

Todo el que trabaje para Ipsos tiene alguna responsabilidad en asegurar que los Datos Personales sean recopilados, almacenados y manejados apropiadamente.

Es responsabilidad de todos que los Datos Personales sean manejados y procesados en línea con esta Política y sus principios de protección de datos.

Ipsos también espera que sus proveedores/cumplan con los principios como se establece aquí.

4. Aplicación de Leyes Nacionales y Códigos de Conducta

Esta Política de Protección de Datos adopta principios de privacidad aceptados internacionalmente como los mejorados por el GDPR. Es subsidiaria y complementa cualquier legislación nacional aplicable. Las leyes nacionales relevantes tendrán precedencia si hay un

conflicto con esta Política o tiene requisitos más estrictos que esta Política. Por el contrario, donde el régimen local tenga requisitos menos estrictos, aún nos mantendremos a los requisitos de esta Política. Cualquier requisito de registro, notificación o reporte para el procesamiento de datos bajo leyes nacionales debe ser observado.
El contenido de esta Política también debe ser observado en ausencia de legislación nacional correspondiente o donde la legislación nacional tenga un estándar más bajo.

Cada compañía del Grupo Ipsos es responsable del cumplimiento de esta Política de Protección de Datos y las obligaciones legales aplicables. Si hay razón para creer que las obligaciones legales contradicen los deberes bajo esta Política de Protección de Datos, la Compañía relevante debe informar al DPO del país y al Oficial Principal de Privacidad Global. En caso de conflicto entre la legislación nacional y la Política de Protección de Datos, Ipsos trabajará con la compañía relevante para encontrar una solución práctica que cumpla con los requisitos y satisfaga los propósitos de esta Política así como la legislación aplicable.

Además de esta Política, para su negocio de investigación de mercado Ipsos se adhiere a los requisitos del Código Internacional ICC/Esomar sobre Investigación de Mercado, Opinión e Investigación Social y Análisis de Datos, que se puede encontrarhere.

5. Principios para el Procesamiento de Datos Personales

Todos los Datos Personales deben ser tratados correctamente, independientemente de cómo sean recolectados, registrados y procesados - ya sea en papel, en un archivo de computadora, base de datos, o registrados en otro material - y hay principios generalmente aceptados para salvaguardar esto, como se establece en las Guías de la OCDE sobre el así como salvaguardias relevantes en varios estatutos alrededor del mundo, incluyendo el GDPR.Protection of Privacy and Transborder Flows of Personal Data,

Ipsos considera el tratamiento legal y correcto de los Datos Personales y mantener la confianza de aquellos con quienes trata en el trato apropiado de Ipsos con los Datos Personales como un componente vital de sus operaciones de negocio y está comprometido a actuar ética y responsablemente en lo referente a estos Datos Personales y siempre proporcionar un alto grado de confidencialidad y seguridad.

Para demostrar estos compromisos, Ipsos se adhiere a los principios relacionados con el procesamiento de Datos Personales encontrados en el GDPR que son ellos mismos una personificación de los principios de la OCDE. Ipsos respeta los siguientes principios, que se explican con más detalle más adelante, concernientes a los Datos Personales. Los Datos Personales serán:

- Procesados de manera justa y lícita.
- Procesados para fines limitados y de una manera apropiada.
- Adecuados, relevantes y no excesivos para el propósito.
- Precisos.
- No se guardarán más tiempo del necesario para el propósito.
- Procesados en línea con los derechos de los Sujetos de los Datos.
- Seguros.
- No transferidos a personas u organizaciones situadas en otros países sin protección adecuada.

5.1. Legalidad, Justicia y Transparencia

Los datos personales deben ser procesados y recopilados de manera lícita, justa y transparente en relación con el Sujeto de los Datos. Además, los Sujetos de Datos deben ser informados de cómo se están manejando sus datos, usualmente en forma de una política/aviso de privacidad o términos y condiciones. En general, los datos personales deben ser recopilados directamente del individuo concernido. Cuando este no sea el caso, la base

legal en la cual el procesamiento está justificado debe ser documentada. El DPO relevante tiene que ser consultado sobre si se debe realizar una Evaluación de Impacto de Protección de Datos (EIPD) (ver también la guía separada sobre EIPDs que se puede encontrar en el .intranet)

5.2. Limitación de propósito

Los datos personales solo deben ser recopilados para propósitos especificados, explícitos y legítimos y no procesados posteriormente de una manera que sea incompatible con esos propósitos. Cambios posteriores al propósito solo se permiten en una medida limitada y requieren sustentación y validación. El DPO relevante tiene que ser consultado sobre si se debe realizar una EIPD (ver también la guía separada sobre EIPDs que se puede encontrar en el . Las instancias obligatorias para el requisito de realizar una EIPD están establecidas en el párrafo 12 abajo.intranet)

5.3. Minimización de datos

Los datos personales deben ser adecuados, relevantes y limitados a lo que es necesario en relación para el propósito por el cual son procesados. Debe determinarse si y en qué medida la recopilación y procesamiento de datos personales es necesaria para alcanzar el propósito por el cual se lleva a cabo el procesamiento. Si es necesario, necesitamos resistirnos a que un cliente proporcione detalles innecesarios como parte de cualquier provisión de muestra. Donde el propósito lo permita, donde el gasto involucrado esté en proporción con los riesgos para los Sujetos de Datos y sea metodológicamente posible, se deben usar datos anonimizados en lugar de datos personales.

5.4. Precisión

Los datos personales deben ser precisos y, cuando sea necesario, mantenidos actualizados. Se deben tomar todas las medidas razonables para asegurar que los datos personales que son inexactos, teniendo en cuenta el propósito por el cual son procesados, sean borrados o rectificados sin demora.

5.5. Limitación del almacenamiento

Los datos personales no deben ser retenidos en una forma que permita la identificación de los Sujetos de Datos por más tiempo del necesario para el propósito por el cual los datos personales son procesados. Ipsos no mantendrá los datos personales por más tiempo del necesario para el propósito o propósitos para los cuales fueron recopilados. Ipsos tomará todas las medidas razonables para destruir, o borrar de sus sistemas, todos los datos personales que ya no sean requeridos. Esto no se aplica a los datos anonimizados.

Mientras que el Grupo Ipsos ha introducido políticas en línea con ISO 20252 sobre los períodos máximos de retención para los datos personales (como se puede encontrar en el , también es política de Ipsos reducir tales períodos de retención siempre que sea posible, ya sea eliminando o anonimizando los datos personales relevantes mucho antes de que se alcancen los períodos máximos (ver también abajo bajo 5.6).Information Management Policy)

5.6. Integridad y confidencialidad

Los datos personales deben ser procesados de una manera que asegure la seguridad apropiada de los datos personales de ser revelados, diseminados, accedidos o manipulados. Por lo tanto, donde sea metodológicamente posible y el gasto no sea desproporcionado a los riesgos del Sujeto de Datos, los datos personales deben ser pseudonimizados tan pronto como sea posible y ser usados para ningún otro procesamiento posterior – RECORDATORIO: ¡los datos pseudonimizados permanecen siendo y son datos personales!

Una vez que se haya alcanzado el propósito del procesamiento, usualmente una vez que se haya completado el control de calidad, los datos personales deben ser anonimizados o borrados.

5.7. Restricción en las transferencias

Los datos personales no deben ser transferidos a otros países (incluso a otras compañías de Ipsos en otros países) que no ofrezcan un nivel adecuado de protección. Ipsos ha introducido varias medidas para adjudicar tal nivel adecuado de protección de manera general (ver también el párrafo 7 para más detalle), sin embargo, varios países pueden tener requisitos más estrictos, adicionales y/o diferentes que deben ser adheridos.

5.8. Medidas y consideraciones generales

Adicionalmente, en relación con su negocio de investigación de mercado Ipsos cumple con el y con las de EsomarICC/ESOMAR International Code on Market, Opinion, and Social Research and Data Analytics Data Protection Checklist.

6. Bases legales para el procesamiento de datos

Ipsos estará recopilando, procesando y usando datos personales solo bajo las siguientes bases legales, siempre y cuando tal base legal exista bajo la ley nacional aplicable. Una de estas bases legales también es requerida si el propósito de recopilar, procesar y usar los datos personales se va a cambiar del propósito original, a menos que haya una compatibilidad clara entre el propósito original y el nuevo propósito. Ver también el párrafo 5.2 y cualquier posible requisito adicional de cumplimiento.

6.1. Datos del encuestado

Los encuestados son los sujetos de datos más comunes en el negocio de Ipsos. Consecuentemente, el tratamiento correcto de sus datos personales está en el corazón del negocio de Ipsos.

5.1.1Consentimiento para el procesamiento de datos

Los Datos Personales pueden ser procesados siguiendo el consentimiento del Sujeto de Datos. Antes de dar consentimiento, el Sujeto de Datos debe ser informado de acuerdo con el principio de transparencia establecido en el párrafo 5.1. La declaración de consentimiento debe obtenerse por escrito o electrónicamente para fines de documentación. En algunas circunstancias, como encuestas telefónicas, el consentimiento se puede dar verbalmente. En todos los casos, la concesión del consentimiento debe ser documentada.

Cualquier consentimiento solo será válido si constituye una indicación libremente dada, específica, informada y sin ambigüedades de los deseos del Sujeto de Datos por el cual da una declaración, por una clara acción afirmativa que significa acuerdo con el procesamiento de los Datos Personales relacionados con él/ella. En consecuencia, el consentimiento no puede basarse en el uso de casillas previamente marcadas. Para orientación respecto del consentimiento, por favor vea elintranet.

5.1.2 Procesamiento de Datos para una Relación Contractual

Aparte del consentimiento, los Datos Personales pueden ser procesados cuando esto es necesario en el contexto de un contrato con dichos Sujetos de Datos para cumplir las obligaciones y derechos relevantes del contrato. Esto también se aplica cuando dicho procesamiento es necesario para establecer o terminar un contrato, como los encuestados (incluyendo compradores misteriosos) que se inscriben en un panel de Ipsos.

Algunos países ven la entrada en un contrato como una forma de consentimiento.

5.1.3 Procesamiento de Datos conforme a Autorización Legal

El procesamiento de Datos Personales también está permitido si la legislación lo solicita, requiere o permite esto. El tipo y extensión del procesamiento de datos debe ser necesario para la actividad de procesamiento de datos legalmente autorizada y debe cumplir con las disposiciones legales relevantes. Ejemplos típicos para esta base legal son el reporte de eventos adversos, legislación fiscal, de empleo o de igualdad.

5.1.4 Procesamiento de Datos conforme a Interés Legítimo

Los Datos Personales también pueden ser procesados, si es necesario para los intereses legítimos del Grupo Ipsos (o un tercero) y donde la legislación nacional provee para esta base (por ejemplo, Artículo 6(1)(f) del GDPR). La base legal del interés legítimo para el procesamiento no es reconocida en todo país, y la legislación nacional relevante tomará precedencia. Generalmente, los Datos Personales de niños no pueden ser procesados basados en interés legítimo y esto también no se aplica a categorías especiales de Datos Personales!

En cualquier evento, los Datos Personales no pueden ser procesados en base a un interés legítimo si, en el caso individual, hay evidencia de que los intereses del Sujeto de Datos merecen protección y que esta protección tiene precedencia. Antes de que los Datos Personales sean procesados en base al interés legítimo, es necesario realizar una evaluación de interés legítimo (idealmente en la forma de un DPIA con un enfoque particular en el interés legítimo). No obstante, donde claramente el párrafo 12 no se aplica, se puede llevar a cabo una evaluación de interés legítimo simplificada. Se puede encontrar una plantilla relevante here.

5.1.5 Procesamiento de Categorías Especiales de Datos Personales

Las categorías especiales de Datos Personales solo pueden ser procesadas si la ley lo requiere, o el Sujeto de Datos ha dado su consentimiento explícito. Para orientación respecto del consentimiento y particularmente 'consentimiento explícito', por favor vea las Categorías especiales de Datos Personales también pueden ser procesadas si esto es obligatorio para la afirmación, ejercicio o defensa de reclamos legales. Dentro del Área Económica Europea (EEA), las categorías especiales de Datos Personales también pueden ser procesadas para la investigación científica y histórica y para fines estadísticos (Artículo 9(2)(j) GDPR), sujeto a medidas adicionales apropiadas. Antes de confiar en estas disposiciones, debe realizarse un DPIA (ve también la orientación separada sobre DPIAs que puede ser encontrada en el
‘consentimiento explícito’, por favor vea las categorías especiales de Datos Personales también pueden ser procesados si esto es obligatorio para afirmar, ejercer o defender reclamaciones legales. Dentro del Área Económica Europea (AEE), categorías especiales de Datos Personales también pueden ser procesados para investigaciones científicas e históricas y para fines estadísticos (Artículo 9(2)(j) GDPR), sujeto a medidas adicionales apropiadas. Antes de depender de estas disposiciones, se debe realizar un análisis de impacto de protección de datos (DPIA) (véase también la orientación separada sobre DPIAs que se puede encontrar en elintranet.intranet.

5.1.6 Datos de Usuario e Internet

Si los Datos Personales se recopilan, procesan y utilizan desde sitios web o en aplicaciones, se debe informar al Sujeto de los Datos de esto en una declaración de privacidad que incluya, si corresponde, información sobre cookies o medidas técnicas similares. La declaración de privacidad y cualquier información sobre cookies deben integrarse de manera que se identifiquen fácilmente, sean directamente accesibles, comprensibles y estén disponibles de manera consistente para el Sujeto de los Datos. Esto también significa que a menos que los Datos Personales recopilados sean estrictamente necesarios para el funcionamiento del sitio web o la aplicación, se requeriría el consentimiento del Sujeto de los Datos para la recolección de datos. Por lo tanto, cualquier cookie relevante solo puede decirse después de haber obtenido el consentimiento.

Si se crean perfiles de uso (seguimiento) para evaluar el uso de sitios web y aplicaciones, siempre se debe informar a los Sujetos de los Datos de esto en la declaración de privacidad. El seguimiento de los Sujetos de los Datos en línea solo puede llevarse a cabo, si está permitido bajo la ley nacional o con el consentimiento de los Sujetos de los Datos. Incluso si el seguimiento utiliza un pseudónimo para el Sujeto de los Datos, si se realiza utilizando cookies, balizas, etiquetas, píxeles o cualquier otra técnica de seguimiento, como mínimo se debe dar al Sujeto de los Datos la oportunidad de optar por no participar en la declaración de privacidad. Se debe tener especial cuidado dentro del EEE para adherirse a la Directiva ePrivacy y en su momento al Reglamento ePrivacy.

Si los sitios web o aplicaciones pueden acceder a Datos Personales en un área restringida a usuarios/respondentes registrados, la identificación y autenticación del Sujeto de los Datos debe ofrecer suficiente protección durante el acceso.

Como parte del compromiso de Ipsos de adherirse al Código de Esomar, las reglas y requisitos establecidos en otros como Esomar también se aplican a Ipsos como parte de esta Política. También se debe considerar la orientación adicional publicada por Esomar como parte de su proceso de quejas basado en la web en guidelines Guideline on Research and Data Analytics with Children, Young People, and Other Vulnerable Individuals www.trustinresearch.org.

6.2. Datos Personales Proporcionados por Clientes

La transmisión de Datos Personales a Ipsos por parte de sus clientes es un hecho común. Generalmente ocurre para proporcionarnos una muestra o para mejorar una muestra existente. Respecto a cualquier Dato Personal así recibido, Ipsos será el Procesador y solo puede Procesar estos Datos Personales de acuerdo con las instrucciones acordadas o recibidas del cliente. Estas instrucciones

pueden incluir restricciones sobre transferencias a otras partes (incluidas otras compañías o proveedores de Ipsos) o transferencias a otros países, así como requisitos específicos de seguridad. Cualquier restricción de este tipo debe cumplirse. Es imperativo que dichas instrucciones se documenten por escrito y se acuerden antes de que se acepten los arreglos contractuales relevantes por parte de Ipsos, para asegurar que Ipsos realmente pueda cumplir con dichas restricciones o requisitos específicos del cliente.
Independientemente de cualquier requisito del cliente, cualquier Dato Personal proporcionado por un cliente solo puede ser:

a) Procesado para el propósito para el que fueron proporcionados;
b) No ser conservados por más tiempo del requerido para el propósito; y
c) Sujeto a los mismos requisitos de seguridad aplicables a los Propios Datos Personales de Ipsos.

6.3. Datos de Empleados

5.3.1 Procesamiento de Datos para la Relación Laboral

En las relaciones laborales, los Datos Personales pueden ser procesados si se necesita para iniciar, llevar a cabo y terminar el acuerdo de empleo. Al iniciar o considerar una relación laboral, se pueden procesar los Datos Personales del solicitante. Si se rechaza al candidato, sus datos deben ser eliminados en observancia con el período de retención requerido a menos que el solicitante haya acordado (tal acuerdo debe documentarse) permanecer en archivo para un futuro proceso de selección. También se necesita consentimiento para usar los datos para procesos de solicitud adicionales antes de compartir la solicitud con otras empresas del Grupo Ipsos.

En una relación laboral existente, el procesamiento de datos siempre debe relacionarse con el propósito del acuerdo de empleo si no aplica ninguna de las siguientes circunstancias para el procesamiento de datos autorizado.

Si durante el procedimiento de solicitud fuera necesario recopilar información de un solicitante de un tercero, se deben observar los requisitos de las leyes nacionales correspondientes. En casos de duda, se debe obtener el consentimiento de los Sujetos de los Datos.

Debe haber una autorización legal para procesar Datos Personales que están relacionados con la relación laboral pero originalmente no eran parte del desempeño del contrato de trabajo. Esto puede incluir requisitos legales, regulaciones colectivas con representantes de empleados, consentimiento del empleado o el interés legítimo de la compañía.

5.3.2 Procesamiento de Datos conforme a Autorización Legal

Por favor vea arriba en el párrafo 5.1.3 para los requisitos adicionales. Esto típicamente se relaciona con impuestos u otros requisitos de informes estatutarios.

5.3.3 Acuerdos Colectivos sobre el Procesamiento de Datos

Si una actividad de procesamiento de datos excede los propósitos para cumplir un contrato, puede ser permisible si es autorizada a través de un acuerdo colectivo entre el empleador y representantes de empleados, dentro del alcance permitido bajo la ley de empleo relevante. Los acuerdos deben cubrir el propósito específico de la actividad de procesamiento de datos prevista y deben ser redactados dentro de los parámetros de la legislación nacional de protección de datos y de empleo.

5.3.4 Consentimiento para el Procesamiento de Datos

Los datos de los empleados pueden ser procesados con el consentimiento de la persona concernida. Las declaraciones de consentimiento deben ser presentadas voluntariamente. Sin embargo, dentro de la UE/Área Económica Europea, el consentimiento generalmente no constituye una base legal válida para el procesamiento en el contexto del empleo ya que existe una presunción legal de que dicho consentimiento no fue presentado voluntariamente y cualquier procesamiento tendrá que basarse en una de las otras bases legales disponibles (vea en particular 5.3.5 abajo y 5.3.2 arriba). El consentimiento involuntario es nulo. En la medida en que el consentimiento sea una base válida para el procesamiento, por favor vea arriba en el párrafo 1 para los requisitos adicionales. En cualquier caso el consentimiento normalmente puede ser retirado, evitando así cualquier procesamiento futuro, haciendo que otra base legal sea preferible de cualquier manera.

5.3.5 Procesamiento de Datos conforme a Interés Legítimo

Los Datos Personales también pueden ser procesados si es necesario para hacer valer un interés legítimo del Grupo Ipsos, siempre que la ley aplicable permita el procesamiento de Datos Personales basado en un interés legítimo. Dentro del contexto del empleo, los intereses legítimos son generalmente de naturaleza legal o financiera.

Por favor vea arriba en el párrafo 5.1.4 para los requisitos adicionales y limitaciones para la aplicación del interés legítimo.

Las medidas de monitoreo, control o supervisión que requieran el procesamiento de datos de empleados solo pueden tomarse si hay una obligación legal para hacerlo o existe una razón legítima. Incluso si hay una razón legítima, la proporcionalidad de las medidas de control también debe ser evaluada antes de que dichas medidas sean aplicadas. Los intereses justificados de la compañía en aplicar la medida de control (por ejemplo, cumplimiento de reglas internas de la compañía o intereses de seguridad) deben ser ponderados contra cualquier interés de privacidad que los empleados afectados por la medida puedan tener mereciendo protección y la medida no puede ser realizada a menos que se encuentre apropiada. Los intereses legítimos de la compañía y cualquier interés del empleado mereciendo protección deben ser identificados y documentados antes de que cualquier medida sea tomada realizando una evaluación de interés legítimo (en la forma de un DPIA con un enfoque particular en el interés legítimo). Además, cualquier requisito adicional bajo la ley nacional (por ejemplo, consejos de trabajo, derechos de codeterminación para los representantes de los empleados e derechos de información de los Sujetos de Datos) deben ser tomados en cuenta.

5.3.6 Procesamiento de Categorías Especiales de Datos Personales

Las categorías especiales de Datos Personales solo pueden procesarse si la ley lo requiere o si el Sujeto de los Datos ha dado su consentimiento explícito. Estos datos también pueden procesarse si es obligatorio para afirmar, ejercer o defender reclamos legales.

Como se mencionó, dentro de la UE/Área Económica Europea, el consentimiento como base legal para el procesamiento de categorías especiales de datos personales para fines de empleo puede descartarse. Sin embargo, podría haber obligaciones específicas bajo la ley de empleo, seguridad social o protección social que autoricen dicho procesamiento.

5.3.7Decisiones Automatizadas

Si los Datos Personales se procesan automáticamente como parte de la relación laboral y se evalúan detalles personales específicos para la toma de decisiones (por ejemplo, como parte del proceso de selección de personal o la evaluación de calificaciones), este procesamiento automático no puede ser la única base para decisiones que tendrían consecuencias negativas (como el rechazo de una solicitud) o que tendrían implicaciones significativas para el empleado afectado. Para evitar decisiones erróneas, el proceso automatizado debe asegurar que una persona natural evalúe el contenido de la situación, y que esta evaluación sea la base para la decisión real. Los Sujetos de los Datos también deben ser informados de los hechos y resultados de las decisiones automatizadas y se les debe dar la posibilidad de responder.

5.3.8Telecomunicaciones e Internet

El equipo telefónico, las direcciones de correo electrónico, el acceso a intranet e Internet junto con las redes sociales internas son proporcionados por Ipsos principalmente para tareas relacionadas con el trabajo. Son una herramienta y un recurso de la empresa. Pueden usarse dentro de las regulaciones legales aplicables y las políticas internas de la compañía, en particular la En caso de uso autorizado para fines privados, la ley sobre el secreto de las telecomunicaciones en las leyes nacionales de telecomunicación relevantes debe ser observada, si aplica.Information Security Policy.

Ipsos está utilizando tecnología de filtrado web, registro y otras tecnologías defensivas para garantizar el cumplimiento de su Política de Uso Aceptable, la medición y análisis del tráfico de Internet, otras obligaciones de cumplimiento legal y para defenderse contra ataques a la infraestructura de TI o usuarios individuales. Las medidas de protección pueden implementarse para las conexiones a la red de Ipsos que bloquean contenido técnicamente dañino y para analizar los patrones de ataque. Por razones de seguridad, el uso de equipo telefónico, direcciones de correo electrónico, la intranet/Internet y redes sociales internas puede bloquearse de manera permanente o temporal para direcciones/ubicaciones individuales o tipos de conexión. Las evaluaciones de estos datos de una persona específica solo pueden hacerse en un caso concreto y justificado de sospecha de violaciones de la ley o políticas del Grupo Ipsos o una amenaza inmediata para la infraestructura de TI y debe ser autorizado por cualquiera de las personas que puedan autorizar un "bloqueo legal" (ver también el . Las leyes nacionales relevantes deben observarse de la misma manera que las regulaciones del grupo.Information Management Policy)

6.4. Contactos de Marketing

Generalmente, los contactos de marketing no son diferentes de los encuestados en cuanto a las protecciones de privacidad que se les otorgan. Sus detalles de contacto constituyen Datos Personales, incluso si están relacionados con el negocio. Solo si los detalles de contacto son verdaderamente genéricos como “contact@acme.com”, no entrarán bajo esta Política.

Las comunicaciones de marketing a menudo están sujetas a requisitos legales específicos, particularmente si se envían electrónicamente o se realizan por teléfono.

Se tiene que asumir, que los contactos de marketing no han solicitado los materiales de marketing. En otras palabras, los destinatarios no han solicitado recibir comunicaciones de marketing de Ipsos. Para proceder legalmente, se aplican aquí también las condiciones relativas a la base legal, en particular, los requisitos de consentimiento establecidos en el párrafo 1.

Excepcionalmente, se puede aplicar un 'opt-in suave' si se cumplen las condiciones siguientes:

- donde los detalles del Sujeto de los Datos se obtuvieron en el curso de una venta o negociaciones para una venta de servicios de Ipsos;
- donde los mensajes son solamente marketing de servicios similares;
- donde a la persona se le da una oportunidad simple de rechazar el marketing cuando se recopilan sus detalles; y
- en el momento de la primera comunicación de marketing se llama la atención explícitamente sobre el derecho a oponer, presentándose de manera clara y separada de otra información, y se les proporciona una manera sencilla de hacerlo en todos los mensajes futuros.

7. Transmisión de Datos Personales

La transmisión de Datos Personales a destinatarios fuera o dentro del Grupo Ipsos está sujeta a los requisitos de autorización para el procesamiento de Datos Personales bajo el párrafo 5.7 Restricción de Transferencias. El destinatario de los datos (ya sea otra empresa de Ipsos o cualquier proveedor) debe estar obligado a usar los datos solo para los fines definidos. Para las transferencias externas a proveedores, los requisitos de este párrafo y los del párrafo 8 Procesamiento de Datos por Terceros/Subcontratados se aplican de manera acumulativa.

Si los Datos Personales se transmiten a un destinatario fuera del Grupo Ipsos, este destinatario debe acordar por escrito mantener un nivel de protección de datos equivalente a esta Política de Protección de Datos o como lo exija la ley aplicable. Por ejemplo, el GDPR estipula varios requisitos que deben cumplirse, antes de que pueda ocurrir cualquier transferencia. Esto no aplica si la transmisión se basa en una obligación legal. Una obligación legal de este tipo puede basarse en las leyes del país de domicilio de la empresa del Grupo Ipsos que transmite los datos. Alternativamente, las leyes del país de domicilio de la empresa del Grupo Ipsos pueden reconocer el propósito de la transmisión de datos basada en las obligaciones legales de un tercer país.

Cuando los Datos Personales sean transmitidos por un tercero (como un proveedor de muestras) a una empresa del Grupo Ipsos, se debe asegurar que los Datos Personales puedan ser utilizados para el propósito previsto.

Si los Datos Personales son transferidos de una empresa del Grupo Ipsos con su sede en un país a una empresa del Grupo Ipsos con su sede en otro país, la empresa que importa los datos está obligada a cooperar con las consultas realizadas por la autoridad supervisora relevante en el país en el que la parte que exporta los datos tiene su sede y a cumplir con cualquier observación realizada por la autoridad supervisora con respecto al procesamiento de los datos transmitidos.

Si un Sujeto de Datos afirma que esta Política de Protección de Datos ha sido violada por una empresa del Grupo Ipsos ubicada en otro país que está importando los datos, la empresa del Grupo Ipsos que exporta los Datos Personales se compromete a apoyar al Sujeto de Datos en cuestión, en el establecimiento de los hechos del asunto y también en hacer valer sus derechos de acuerdo con esta Política de Protección de Datos contra la empresa del Grupo Ipsos que importa los datos. Además, el Sujeto de Datos también tiene derecho a hacer valer sus derechos contra la empresa del Grupo Ipsos que exporta los datos. En caso de reclamaciones de una violación, es obligación de la empresa exportadora demostrar a los Sujetos de Datos que la empresa importadora de los Datos Personales no violó esta Política de Protección de Datos.

Cada empresa del Grupo Ipsos que transmite Datos Personales a una empresa del Grupo Ipsos ubicada en otro país, seguirá siendo responsable de cualquier violación de esta Política de Protección de Datos cometida por la empresa del Grupo Ipsos que recibió los Datos Personales, como si la violación hubiera sido cometida por la empresa del Grupo Ipsos que transmite los Datos Personales.

Todas las empresas del Grupo Ipsos están obligadas a firmar el Acuerdo Maestro de Servicios Intra-Grupo (y guardar una copia en la Base de Datos Corporativa). Cualquier transferencia de Datos Personales dentro del Grupo Ipsos solo se realizará después de que se haya hecho la entrada relevante en JobBook para el proyecto o servicios bajo los cuales ocurre la transferencia. Dicha entrada creará un contrato específico bajo el Acuerdo Maestro de Servicios Intragrupo de Ipsos y automáticamente hace aplicables las respectivas Cláusulas Contractuales Estándar de la UE a dicha transferencia, incluso si la transferencia no afecta a ninguna entidad de la UE/EEE. Como tal, las Cláusulas Contractuales Estándar se aplican a cada transferencia de datos personales dentro del Grupo Ipsos. Las Cláusulas Contractuales Estándar en sí mismas pueden encontrarse en elintranet.

8. Procesamiento de Datos por Terceros/Subcontratados

En muchos casos, Ipsos está utilizando proveedores externos para procesar Datos Personales. En estos casos, debe celebrarse un acuerdo sobre el procesamiento de datos en nombre de Ipsos con dicho proveedor. Esto se puede hacer ya sea mediante la inclusión de disposiciones apropiadas en el acuerdo que rige la relación general con el proveedor o en un documento específico y separado. Cualquiera de los enfoques cumple con la obligación de tener un “Acuerdo de Protección de Datos” en vigor. En lo que respecta al procesamiento en nombre de Ipsos, el proveedor solo puede procesar los Datos Personales según las instrucciones escritas de Ipsos. Cuando se instruya a un proveedor, se deben cumplir los siguientes requisitos:

- Donde los Datos Personales en cuestión caigan bajo el párrafo 6.2 (datos del cliente), cualquier requisito relevante del cliente debe transmitirse al proveedor.
- El proveedor debe ser elegido en función de su capacidad para cubrir las medidas protectoras técnicas y organizativas requeridas y en línea con el proceso de aprobación de proveedores de Ipsos.
- El proveedor no debe subcontratar el procesamiento adicional sin el consentimiento previo por escrito de Ipsos (que puede proporcionarse como parte del acuerdo con dicho proveedor Microsoft.
- Las instrucciones deben estar por escrito mediante un contrato apropiado. Las instrucciones sobre el procesamiento de datos y las responsabilidades de Ipsos y proveedor deben documentarse.
- Antes de que comience el procesamiento de datos, Ipsos debe estar seguro de que el proveedor cumplirá con sus deberes. Un proveedor puede documentar su cumplimiento con los requisitos de seguridad de datos en particular presentando la(s) certificación(es) adecuada(s). Dependiendo de los riesgos del procesamiento de datos, las revisiones deben repetirse de manera regular durante el término del contrato. Ipsos debe retener el derecho de auditar el cumplimiento del proveedor.
- En caso de procesamiento de datos contractuales transfronterizo, se deben cumplir los requisitos nacionales relevantes para transferir Datos Personales al extranjero. En particular, los Datos Personales del Área Económica Europea solo pueden procesarse en un tercer país, si el proveedor puede demostrar que tiene un estándar de protección de datos equivalente al GDPR y esta Política de Protección de Datos. Las herramientas adecuadas pueden ser:
    - Una decisión de adecuación de la Comisión de la UE respecto al país receptor, una lista de la cual se puede encontrarhere.
    - un acuerdo basado en cláusulas contractuales estándar de la UE para el procesamiento de datos contractuales en terceros países con el proveedor. Se requerirán acuerdos similares para cualquier subcontratista del proveedor.

- Participación del proveedor en un sistema de certificación acreditado por la UE para la provisión de un nivel suficiente de protección de datos.
- Para el Reino Unido, las Cláusulas Contractuales Estándar de la UE más el Addendum del Reino Unido a las mismas.

9. Derechos del Interesado

Todo Sujeto de Datos tiene los derechos establecidos en esta Sección, ya sean previstos o no por la legislación aplicable. Esto obviamente no afecta ningún derecho adicional o más extenso que el Sujeto de Datos pueda disfrutar bajo la legislación nacional, incluyendo el GDPR. Su solicitud de acuerdo a estos derechos debe ser atendida inmediatamente por la empresa de Ipsos relevante y no puede resultar en ninguna desventaja para el Sujeto de Datos. Donde los Datos Personales relevantes están siendo procesados por Ipsos bajo el párrafo 6.2 Datos Personales Proveídos por Clientes, el contrato de cliente relevante debe ser consultado respecto a cualquier proceso a seguir y el cliente tiene que ser informado sobre dicha solicitud inmediatamente.

- **Derecho de acceso:**
  - Los Sujetos de Datos pueden solicitar información sobre qué Datos Personales relacionados con él/ella han sido almacenados, cómo los datos fueron recopilados y para qué propósito.
  - Si los Datos Personales son transmitidos a terceras partes, se debe proporcionar información sobre la identidad del recipiente o las categorías de recipientes, incluyendo otras empresas de Ipsos.
- **Derecho a la rectificación: Si los Datos Personales son incorrectos o incompletos, el Sujeto de Datos puede demandar que sean corregidos o complementados.**
- **Derecho a retirar el consentimiento: Cuando los Datos Personales son procesados sobre la base del consentimiento (ver también la guía separada sobre , el Sujeto de Datos puede objetar el procesamiento en cualquier momento. Estos Datos Personales deben ser bloqueados del procesamiento al que se ha objetado.**Consent)
- **Derecho al borrado. El Sujeto de Datos puede solicitar que sus datos sean borrados si el procesamiento de dichos datos no tiene base legal, o si la base legal ha dejado de aplicarse. Lo mismo aplica si el propósito detrás del procesamiento de datos ha caducado o ha dejado de ser aplicable por otras razones. Se deben observar los períodos de retención existentes y los intereses en conflicto que merecen protección.**
- **Derecho a objetar: El Sujeto de Datos generalmente tiene el derecho a objetar que sus datos sean procesados y esto debe tenerse en cuenta si la protección de su interés precede sobre los intereses del controlador de datos debido a la particular situación personal. Esto no aplica, si una disposición legal requiere que los Datos Personales sean procesados.**
- **Derecho a la portabilidad de los datos. El Sujeto de Datos tiene el derecho de solicitar que los Datos Personales mantenidos por Ipsos sean provistos por él/ella y estén disponibles para dicho Sujeto de Datos en un formato fácilmente legible, como un documento de Word o Excel.**

Para más detalles sobre cómo manejar cualquier solicitud del sujeto de datos conforme a la cual se ejerzan derechos, por favor vea nuestro como publicado en el intranet. Data Subject Request Policy

10. Confidencialidad del Procesamiento

Los Datos Personales están sujetos al secreto de datos. Cualquier recolección, procesamiento o uso no autorizado de tales datos por parte de Usuarios de Datos o cualquier otro empleado está prohibido. Cualquier procesamiento de datos llevado a cabo por un empleado que no ha sido autorizado para realizar como parte de sus deberes legítimos es no autorizado. El principio de "necesidad de conocer" aplica. Los empleados pueden tener acceso a Datos Personales solo en la medida que es apropiado para el tipo y alcance de la tarea en cuestión. Esto requiere una cuidadosa desglose y separación, así como en limitación, de roles y

responsabilidades, con derechos de acceso correspondientes. Además, se aplican los requisitos del . Information Management Policy

Se prohíbe a los empleados usar Datos Personales para sus propios fines privados o comerciales, divulgarlos a personas no autorizadas, o hacerlos disponibles de cualquier otra manera. Los supervisores deben informar a los empleados al inicio de la relación laboral sobre la obligación de mantener el secreto de los datos. Esta obligación permanecerá en vigor incluso después de que el empleo haya terminado. Los acuerdos de empleo con el personal de Ipsos deben contener obligaciones de confidencialidad apropiadas.

11. Privacidad por Diseño y por Defecto

Ipsos utilizará un enfoque de Privacidad por Diseño y por Defecto en todo su trabajo, pero en particular cuando:

- construyendo nuevos sistemas de TI para almacenar o acceder a Datos Personales;
- desarrollando nuevas aplicaciones o enfoques de investigación;
- emprendiendo una iniciativa de compartir datos; o
- usando Datos Personales para propósitos diferentes a los que habían sido recopilados.

La privacidad por diseño no es solo un enfoque para proyectos que promueve la privacidad y el cumplimiento de protección de datos desde el inicio y como tal una consideración clave en las primeras etapas de cualquier proyecto, y luego a lo largo de su ciclo de vida. También es una de las obligaciones de cumplimiento más fundamentales.

Tomar un enfoque de privacidad por diseño es una herramienta esencial en minimizar los riesgos de privacidad y construir confianza y diseñará proyectos, procesos, productos o sistemas con la privacidad en mente desde el principio

En cuanto a los ejemplos dados anteriormente, la herramienta requerida para el cumplimiento es realizar un DPIA de acuerdo con la orientación adicional que se puede encontrar en elintranet.

12. Evaluación de Impacto sobre la Protección de Datos

Antes de realizar cualquiera de las actividades de procesamiento descritas a continuación, se deberá completar un DPIA de acuerdo con la orientación adicional que se puede encontrar en el Esto es además de las otras instancias ya mencionadas en esta Política ya que el negocio de Ipsos se basa en el procesamiento a gran escala de Datos Personales.intranet.

Tipo de operación(es) de procesamiento	**Descripción**
Tecnología innovadora	Procesamiento que involucra el uso de nuevas tecnologías, o la aplicación novedosa de tecnologías existentes (incluyendo IA). Cualquier operación de procesamiento prevista que involucre el uso innovador de tecnologías (o aplicando nuevas soluciones tecnológicas y/o organizativas).

Denegación de servicio	Decisiones sobre el acceso de un individuo a un producto, servicio, oportunidad o beneficio que se basan en cualquier medida en la toma de decisiones automatizada (incluyendo el perfilado) o involucra el procesamiento de datos de categoría especial.
Perfilado a gran escala	Cualquier perfilado de individuos a gran escala
Datos biométricos	Cualquier procesamiento de datos biométricos con el propósito de identificar de manera única a un individuo. Cualquier operación de procesamiento prevista que involucre datos biométricos con el propósito de identificar de manera única a un individuo
Datos genéticos	Cualquier operación de procesamiento prevista que involucre datos genéticos.
Emparejamiento de datos (base)	Combinar, comparar o emparejar Datos Personales obtenidos de más de una fuente.
Procesamiento invisible	Procesamiento de Datos Personales que no se han obtenido directamente del Sujeto de Datos en circunstancias donde el controlador considera que cumplir con el principio de transparencia (ver párrafo 5.1) sería imposible o implicaría un esfuerzo desproporcionado. Cualquier operación de procesamiento prevista donde el controlador considera que cumplir con el principio de transparencia (ver párrafo 5.1) sería imposible o implicaría un esfuerzo desproporcionado.
Seguimiento	Procesamiento que implica el seguimiento de la geolocalización de un individuo o comportamiento, incluyendo pero no limitado al entorno en línea. Cualquier operación de procesamiento prevista que involucre datos de geolocalización.
Riesgo de daño físico	Cuando el procesamiento es de tal naturaleza que una violación de Datos Personales podría poner en peligro la salud o la seguridad de los individuos.

13. Seguridad del Procesamiento

Los Datos Personales deben ser protegidos contra el acceso o divulgación no autorizados (ya sea causados interna o externamente), procesamiento ilegal así como pérdida accidental, modificación o destrucción. Esto aplica independientemente de si los datos se procesan electrónicamente o en forma de papel. Aparte de asegurar los Datos Personales existentes en línea con las políticas relevantes de Ipsos (por favor, vea el Libro de Ipsos de el cual es aplicable en ese respecto), antes de la introducción de nuevos métodos de procesamiento de datos, sistemas IT nuevos o enfoques de investigación, medidas técnicas u organizativas para proteger los Datos Personales deben ser definidas e implementadas. Estas medidas deben basarse en el estado del arte, el riesgo de procesamiento y la necesidad de proteger los datos. Esta información también será requerida para el DPIA relevante.Policies and Procedures Chapter 7,

Estas medidas técnicas y organizativas deberían ser acordadas en consulta con el Oficial de Seguridad de la Información relevante y el DPO. Las medidas técnicas y organizativas para proteger los Datos Personales son parte de la gestión de la Seguridad de la Información

Corporativa y deben ser ajustadas continuamente al desarrollo técnico y avance así como a los cambios organizacionales.

Como mínimo, Ipsos procesará todos los Datos Personales que posee de acuerdo con su Política de Seguridad y tomará medidas de seguridad apropiadas contra el procesamiento ilegal o no autorizado de Datos Personales, y contra la pérdida accidental de, o daño a, Datos Personales.

14. Auditoría de Protección de Datos

La conformidad con esta Política de Protección de Datos y las leyes de protección de datos aplicables se verifica regularmente con auditorías de protección de datos y otros controles. La realización de estos controles es la responsabilidad del CPO, los DPO, Auditoría Interna y/o auditores contratados externamente. Varios clientes de Ipsos también tienen derechos de auditoría bajo sus acuerdos con Ipsos. Los resultados de todas las auditorías de protección de datos deben ser reportados al CPO y al Jefe de Cumplimiento. A petición, los resultados de las auditorías de protección de datos serán puestos a disposición de las autoridades de protección de datos responsables.

15. Incidentes de Protección de Datos

Todos los empleados deben informar a su DPO o al CPO inmediatamente sobre casos de violaciones de esta Política de Protección de Datos u otras regulaciones sobre la protección de Datos Personales, de acuerdo con la cual también se puede encontrar en la Sección 8 del Libro de Políticas y Procedimientos de Ipsos. Cualquier fallo en abordar fallos serios bajo esta Política también puede ser reportado bajo el sistema.Personal Data Breach Management Procedure Ipsos Whistle-blowing

A modo de ejemplo solamente, en caso de:

- transmisión indebida de Datos Personales a terceros;
- transmisión indebida de Datos Personales a través de fronteras;
- acceso indebido, incluyendo por terceros, a Datos Personales, o
- pérdida de Datos Personales (incluyendo luego volverse públicos debido a fallos internos) se debe hacer una notificación de violación de protección de datos inmediatamente para asegurar que a) cualquier deber de informar respecto a los Sujetos de Datos, así como a las autoridades de protección de datos bajo la ley nacional se pueda cumplir, b) cualquier cliente afectado pueda ser informado y c) cualquier comunicación con stakeholders pueda ser gestionada. Cualquier violación de Protección de Datos también constituirá un incidente de seguridad de la información bajo la política de Gestión de Incidentes de TI, activando así un requerimiento de reporte separado.

16. Responsabilidades y Sanciones

16.1. Gestión

Los órganos ejecutivos de las respectivas empresas del Grupo Ipsos son responsables del procesamiento de datos en su área de responsabilidad. Por lo tanto, se requiere que aseguren que no solo los requerimientos bajo la ley nacional sino también aquellos contenidos en esta Política de Protección de Datos sean cumplidos (p.ej. obligaciones nacionales de informar).

La gestión es responsable de asegurar que las medidas organizativas, de RRHH y técnicas estén en lugar para que cualquier procesamiento de datos se lleve a cabo de acuerdo con estos requisitos de protección de datos.

El cumplimiento de estos requisitos es también responsabilidad de los empleados relevantes.

Si los organismos oficiales realizan auditorías de protección de datos, se debe informar inmediatamente al CPO.

La gestión del país de Ipsos relevante debe informar al CPO sobre el nombre del DPO.

El procesamiento inadecuado de Datos Personales, u otras violaciones de las leyes de protección de datos, pueden ser perseguidos penalmente en muchos países y resultar en reclamos por compensación de daño. Además, las violaciones por las cuales los empleados individuales son responsables pueden llevar a sanciones bajo la ley de empleo.

16.2. Oficiales de Protección de Datos

Cada país de Ipsos estará obligado a nombrar uno o más Oficiales de Protección de Datos ("DPO").
Los DPO son las personas de contacto internas y externas en el país para la protección de datos. Pueden realizar chequeos y deben familiarizar a los empleados con los contenidos de esta Política de Protección de Datos y la legislación aplicable. La gestión relevante está obligada a asistir a los DPO en sus esfuerzos. Las tareas principales de los DPO son:

- *Informar y asesorar a la organización y sus empleados sobre sus obligaciones de cumplir con las leyes de protección de datos aplicables y esta Política de Protección de Datos. Esta tarea será apoyada y guiada por el Grupo y a través de la red de DPO bajo el liderazgo del CPO y entrenamiento.*
- *Monitorear el cumplimiento de las leyes de protección de datos, incluyendo gestionar las actividades internas de protección de datos, asesorar (no realizar) sobre las evaluaciones de impacto de protección de datos; entrenar al personal y realizar auditorías internas. Esto será apoyado y guiado por el Grupo. Las auditorías, aparte de las comprobaciones puntuales, deberían ser coordinadas con la función de auditoría interna del Grupo.*
- *Proporcionar asesoramiento con respecto a las DPIAs. Bajo el proceso de DPIA, se debe buscar y considerar el asesoramiento del DPO responsable como parte de las evaluaciones a realizar en la DPIA.*
- *Ser el primer punto de contacto para las autoridades supervisoras y para las personas cuyos datos son procesados (empleados, clientes, etc.).*

Dentro de cada país de Ipsos, el DPO tendrá:

- Informar al nivel más alto de gestión de la organización de Ipsos country – es decir, al nivel de la junta de gestión local o miembro.
- Operar independientemente de las órdenes profesionales, y no ser despedido o penalizado por realizar su tarea.
- Ser proporcionado con recursos adecuados para permitir al DPO cumplir con sus obligaciones bajo las leyes de protección de datos aplicables y esta Política de Protección de Datos.

Los Oficiales de Protección de Datos deberán informar al CPO de cualquier riesgo de protección de datos de manera pronta.

16.3. Oficial Principal de Privacidad Global

El Oficial Principal de Privacidad Global ("CPO"), siendo internamente independiente de las órdenes profesionales, trabaja hacia el cumplimiento de las reglas de protección de datos nacionales e internacionales. Él/ella es responsable de esta Política de Protección de Datos y supervisa su cumplimiento.

Cualquier Sujeto de Datos puede acercarse al CPO o al DPO relevante en cualquier momento para expresar preocupaciones, hacer preguntas, solicitar información o hacer quejas relacionadas con problemas de protección de datos o seguridad de datos. Si se solicita, las preocupaciones y quejas serán tratadas confidencialmente.

Si el DPO relevante no puede resolver una queja o remediar una violación de la Política de Protección de Datos, el CPO debe ser consultado inmediatamente. Las decisiones del CPO para remediar violaciones de protección de datos deben ser mantenidas por la gerencia de la compañía en cuestión. Las consultas por autoridades supervisoras siempre deben ser reportadas al CPO.

17. Derogación

En casos excepcionales, puede ser posible obtener una derogación de esta Política, previo a cualquier procesamiento intencionado de los Datos Personales afectados. Cualquier derogación de este tipo solo puede ser concedida siguiendo una DPIA completa para establecer y evaluar los riesgos para cualquier Sujeto de Datos afectado, riesgos legales e impacto reputacional y está sujeta a la aprobación por el Presidente de Servicios de Soporte de Ipsos.

18. Glosario

Varias expresiones a continuación tienen definiciones más detalladas que se pueden accesar siguiendo los enlaces. Los casos relevantes están indicados por títulos en cursiva.

Controlador de Datos/Controlador/Controlador Conjunto

Esta es la persona u organización que determina los propósitos y la manera en que cualquier Dato Personal es procesado. Es responsable de establecer prácticas y políticas en línea con los requisitos legales aplicables.

En la mayoría de los casos donde Ipsos está recibiendo muestra de un cliente, será controlador conjunto de los datos recolectados. Esto se extiende a los datos que recolectamos, incluso cuando hemos asegurado a los encuestados la confidencialidad de sus respuestas. Las responsabilidades y obligaciones de los controladores conjuntos tienen que ser documentadas y aclaradas en un acuerdo escrito.
Algunas jurisdicciones usan otras expresiones para el mismo concepto, como Persona Responsable, Organización, Operador etc.[1]

Usuarios de Datos

Estos son aquellos de nuestros empleados cuyo trabajo involucra el procesamiento de Datos Personales. Los usuarios de datos deben proteger los datos y Datos Personales que manejan de acuerdo con esta Política y cualquier procedimiento de seguridad de datos aplicable en todo momento.

Procesador de datos o Procesador

Esta es la persona u organización que no es un Usuario de Datos que procesa Datos Personales en nombre y bajo las instrucciones del Controlador. Los empleados de los controladores de datos están excluidos de esta definición, pero incluye a proveedores que manejan Datos Personales. Ipsos será variadamente un Controlador (p.ej., en respeto de nuestros panelistas o muestra ad-hoc Ipsos recluta para una encuesta) o un Procesador (p.ej.,

[1] Singapore

en respeto de muestra proporcionada por clientes). Algunas jurisdicciones usan otras expresiones para el mismo concepto, como Tercera Parte, Intermediario, Operador etc.[1]

Sujetos de Datos

Para el propósito de esta Política incluye a todos los individuos vivos sobre los cuales una Compañía Ipsos mantiene Datos Personales. Un Sujeto de Datos no necesita ser un nacional o residente de un país. Todos los Sujetos de Datos tienen derechos legales en relación con sus Datos Personales.

Personal Data

La definición de Datos Personales del GDPR (Artículo 4 (1) del GDPR) clarifica qué son Datos Personales y muestra que esto debe ser interpretado de manera amplia:

"…cualquier información relacionada con una persona natural identificada o identificable ('sujeto de datos'); una persona natural identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona natural".

Es importante notar que todos los datos sobre un Sujeto de Datos son Datos Personales, no solo los datos que lo identifican.

Una persona natural es un individuo vivo y el propio GDPR no se aplica a individuos fallecidos. Sin embargo, los estados miembros individuales pueden establecer normas relativas al tratamiento de Datos Personales incluso en lo que respecta a personas fallecidas.

La información sobre una empresa no constituirá Datos Personales.

No siempre es posible determinar con absoluta certeza si un elemento de información individual constituiría Datos Personales. Será necesario mirar la información general que se tiene sobre la persona

en cuestión o los medios razonablemente probables de ser utilizados para identificar a una persona. Con los medios tecnológicos en constante mejora, más datos se convertirán en Datos Personales.

Tratamiento

El tratamiento generalmente es cualquier actividad que involucra el uso de los datos. Más específicamente en relación con la protección de datos, es cualquier operación o conjunto de operaciones que se realiza sobre o sobre conjuntos de Datos Personales. Incluye recopilar, organizar, estructurar, almacenar, adaptar o alterar, obtener, grabar, mantener organizando, enmendar, recuperar, usar, divulgar, borrar o destruir Datos Personales. El tratamiento también incluye transferir Datos Personales o acceder a ellos, independientemente de dónde esto pueda ser.Personal Data

Categorías especiales de datos (anteriormente conocidos como datos personales sensibles)

"Categorías especiales de Datos Personales" es la nueva expresión utilizada en el GDPR y anteriormente se refería como "datos sensibles". Ahora esto está definido en el Artículo 9 del GDPR como datos concernientes a:
el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o afiliación sindical, datos genéticos [ver abajo], datos biométricos [ver abajo] con el propósito de

[1] South Africa

identificar de manera única a una persona natural, datos concernientes a la salud [ver abajo] o datos concernientes a la vida sexual o la orientación sexual de una persona natural

Para algunas de estas expresiones se han proporcionado definiciones más detalladas en el GDPR:

'datos genéticos' significa Datos Personales relacionados con las características genéticas heredadas o adquiridas de una persona natural que dan información única sobre la fisiología o la salud de esa persona natural y que resultan, en particular, de un análisis de una muestra biológica de la persona natural en cuestión;

'datos biométricos' significa Datos Personales resultantes de un procesamiento técnico específico relativo a las características físicas, fisiológicas o de comportamiento de una persona natural, que permiten o confirman la identificación única de esa persona natural, como imágenes faciales o datos dactiloscópicos;

'datos concernientes a la salud' significa Datos Personales relacionados con la salud física o mental de una persona natural, incluida la prestación de servicios de atención médica, que revelan información sobre su estado de salud;

Datos Anónimos

Esto ha sido definido como información que no se refiere a una persona natural identificada o identificable o a Datos Personales hechos anónimos de tal manera que el Sujeto de los Datos no es o ya no es identificable (Considerando 26 del GDPR). Esto debe distinguirse de los datos que, junto con el uso de información adicional (por ejemplo, una clave), podrían utilizarse para identificar a una persona natural, entonces los datos fueron meramente pseudonimizados.
Los datos pseudonimizados todavía caen bajo la definición de Datos Personales y todos los principios y requisitos completos del GDPR todavía se aplican a ellos.

Pseudonymisation

Pseudonimización significa el tratamiento de Datos Personales de tal manera que los Datos Personales ya no pueden atribuirse a un Sujeto de Datos específico sin el uso de información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas para asegurar que los Datos Personales no se atribuyan a una persona natural identificada o identificable. (Artículo 4(5) del GDPR)
Datos pseudónimos se refiere a datos de los cuales los identificadores en un conjunto de información son reemplazados con identificadores artificiales, o pseudónimos, que se mantienen por separado y sujetos a salvaguardas técnicas. ¡Los datos pseudonimizados permanecen siendo Datos Personales y, por lo tanto, todos los demás requisitos de protección de datos siguen aplicándose a ellos!

PII or Personally Identifiable Information

Este término deriva de la legislación sobre privacidad de EE. UU. Solo cubre un elemento estrecho de Datos Personales ya que se centra en aquellos datos que identifican a un Sujeto de Datos, mientras que Datos Personales se aplica a todos los datos relacionados con el sujeto de datos. El uso de la expresión PII debe evitarse, ya que denota un entendimiento incorrecto de nuestras obligaciones bajo la legislación de privacidad y protección de datos. Incluso dentro de los EE. UU., el creciente cuerpo de legislación estatal generalmente ahora se refiere a "Datos Personales. O

PHI o Información de Salud Protegida

Este término también deriva de la legislación sobre privacidad de EE. UU., en particular HIPAA en los EE. UU. Aunque desde una perspectiva práctica aplicable al trabajo diario de Ipsos las expresiones categorías especiales de Datos Personales y PHI deberían tratarse como sinónimos, el uso de PHI en el contexto de esta Política debe evitarse.

El principal problema a considerar es que ciertos Datos Personales que caerían bajo la definición legal de PHI, bajo GDPR constituirían Datos Personales en lugar de categorías especiales de datos. Por ejemplo, HIPPA consideraría toda la información en un conjunto de datos que contuviera el nombre y la orientación sexual como PHI, mientras que el GDPR solo consideraría la orientación sexual como parte de las categorías especiales de Datos Personales.

PSI o Información Personal Sensible

Esta expresión está ahora desactualizada, habiendo derivado de legislación anterior. Esto es en gran medida sinónimo de “categorías especiales de Datos Personales”, y se debería usar esta última expresión. Los reguladores esperarán que Ipsos utilice la terminología correcta para demostrar nuestro cumplimiento como parte de nuestra obligación de responsabilidad.