Códigos y Directrices de Investigación Mundial

ESOMAR LISTA DE CONTROL DE PROTECCIÓN DE DATOS

ESOMAR, la Asociación Mundial para la Investigación de Mercados, Social y de la Opinión, reúne alrededor de 4.900 miembros en más de 130 países y es la organización esencial para el fomento, el avance y la exaltación de la investigación de mercados. Los Códigos y directrices están disponibles en www.esomar.org

ANEIMO, Asociación Nacional de Empresas de Investigación de Mercados y Opinión Pública, es la asociación que aglutina a las empresas **líderes del sector**, representándolas en los diferentes ámbitos sociales y profesionales, promoviendo su desarrollo y asegurando que sus trabajos se realizan con altos estándares de calidad y siguiendo los códigos de ética profesional. www.aneimo.com.

AEDEMO es la Asociación de los Profesionales que desarrollan su actividad en la Investigación de Mercados, el Marketing y los Estudios de Opinión. El objetivo fundamental de AEDEMO es la difusión y control de las técnicas empleadas en la Investigación Comercial.Las actividades se desarrollan en los campos de la formación, las publicaciones profesionales, los servicios a los asociados y las relaciones internacionales. www.aedemo.es

CONTENIDOS

1 INTRODUCCIÓN

El investigador que trabaja en un contexto mundial cada vez con más frecuencia se enfrenta a un mosaico de leyes nacionales diseñadas para asegurar el respeto a la privacidad de los individuos y a la protección de datos de carácter personal. El investigador tiene la responsabilidad de revisar y cumplir, no sólo los requisitos legales del país en el que opera, sino también los requisitos nacionales de protección de datos en todos los países donde lleva a cabo una investigación o tratamiento de datos.

Al mismo tiempo, la expansión incesante de nuevas tecnologías en todos los aspectos de nuestras vidas no sólo ha aumentado el volumen de los datos personales potencialmente disponibles para el investigador, sino también ha introducido nuevos tipos de información personal que deben ser protegidos.

Algo que no ha cambiado es la necesidad del investigador de proteger la reputación de la investigación de mercados, social y de la opinión a través de prácticas que aseguren la transparencia con entrevistados y clientes, que mantengan la confianza en la información que proporcionan y que muestren consideración con los participantes en una investigación.

2 ALCANCE

El propósito de este documento es proporcionar al investigador, especialmente al que trabaja en pequeñas organizaciones que podrían no disponer de suficientes recursos o experiencia en los requisitos relativos a la protección de datos, una orientación general sobre sus responsabilidades dentro de un marco global de protección de datos para asegurar que los participantes en una investigación mantienen el control sobre su información personal. El marco específico utilizado fue desarrollado por la Organización para la Cooperación y el Desarrollo Económico (OCDE). Este marco incluye un conjunto de ocho principios para su uso en el diseño de programas que aseguren la privacidad y la protección de datos de carácter personal:

- La limitación en la recogida
- La calidad de los datos
- La especificación de la finalidad
- La limitación del uso
- Las medidas de seguridad
- La transparencia
- La participación individual
- La responsabilidad

Estos principios generales se reflejan en la mayor parte de la legislación relativa a la privacidad y la protección de datos que existe o que está surgiendo en todo el mundo.

Sin embargo, el investigador debe tener presente que los principios de la OCDE están más estrechamente alineados con los requisitos de protección de datos de la UE, por lo que se insta al investigador que trabaja en otras regiones a consultar otros marcos que puedan ser de aplicación. Esto incluye el Asia-Pacific Co-operation (APEC) Privacy Framework, los US Safe Harbour Privacy Principles y los Generally Accepted Privacy Principles (GAPP) desarrollados por el American Institute of CPAs (AICPA) y el Canadian Institute of Chartered Accountants (CICA). Aunque estos marcos en general no tienen fuerza de ley, expresan principios básicos que el investigador debe adoptar cuando trabaje en la región apropiada.

Además, el investigador debe revisar y cumplir los requisitos de auto-regulación nacionales relativos a la protección de datos y a la investigación de mercados de cada país en el que planea hacer trabajo de campo o proceso de datos, ya que puede haber diferencias en cómo se aplican los principios básicos en cada país. La orientación incluida en este documento constituye un estándar mínimo y puede necesitar ser complementado con medidas adicionales en el contexto de un proyecto específico de investigación. El investigador puede considerar necesario contar con asesoría legal local en la jurisdicción donde la investigación va a realizarse con el fin de garantizar su pleno cumplimiento. También puede resultar útil consultar The Data Protection Laws of the World (Las Leyes de Protección de Datos del Mundo), un recurso en línea gestionado por DLA Piper que se actualiza anualmente.

Por último, el investigador que realiza investigación en áreas especializadas (por ejemplo, la investigación farmacéutica) puede consultar guías específicas, como por ejemplo la EphMRA Adverse Event Reporting Guidelines 2014 (Guía sobre Comunicación de Eventos Adversos) para mayor orientación.

3 USO DE "DEBE" Y "DEBERÍA"

En este documento la palabra "debe" se usa para identificar los requisitos obligatorios. Usamos la palabra "debe" al describir un principio o una práctica que el investigador está obligado a seguir con objeto de cumplir con el Código Internacional ICC/ESOMAR Para la Práctica de la Investigación Social y de Mercados. La palabra "debería" se usa cuando se describe una implementación. Con este uso se acepta que el investigador puede optar por aplicar un principio o una práctica de diferentes maneras dependiendo del diseño de su investigación.

4 DEFINICIONES

Investigación business-to-business (B2B), significa la recogida de datos de personas jurídicas tales como empresas, escuelas, organizaciones sin ánimo de lucro y similares.

Investigación business-to-consumer (B2C), significa la recogida de datos de los individuos.

Consentimiento significa el acuerdo libre e informado dado por una persona para la recogida y tratamiento de sus datos personales. En la investigación de mercados, social y de la opinión este consentimiento se basa en proporcionar al participante en la investigación información clara acerca de la naturaleza de los datos que se recogen, la finalidad para la que se utilizarán dichos datos y la identidad de la persona u organización que mantiene los datos personales. El participante de la investigación puede retirar su consentimiento en cualquier momento.

Responsable del tratamiento significa una persona u organización responsable de decidir cómo se tratan los datos personales. Por ejemplo, un cliente de la investigación sería el responsable del tratamiento sobre sus clientes o consumidores; un organismo de seguridad social público sería el responsable del tratamiento de los datos recogidos de sus beneficiarios de la asistencia social; un proveedor de un panel de investigación sería el responsable del tratamiento de los datos recogidos de los miembros de su panel online; y un instituto de investigación sería el responsable del tratamiento de los datos recogidos de los participantes en un estudio omnibus.

Encargado del tratamiento significa un tercero que recibe, registra, mantiene o realiza operaciones (incluyendo el análisis) de datos de carácter personal en nombre y bajo la dirección del responsable del tratamiento. Como se señaló anteriormente, un instituto de investigación sería tanto el responsable del tratamiento como el encargado del tratamiento para un estudio ómnibus.

Legislación que protege la privacidad significa leyes o reglamentos nacionales, cuyo cumplimiento tiene el efecto de proteger los datos personales de forma consistente con los principios establecidos en este documento.

Investigación de mercados, que incluye la investigación social y de la opinión, es la recopilación e interpretación sistemática de información sobre personas u organizaciones utilizando métodos y técnicas estadísticas y de análisis de las ciencias sociales aplicadas para obtener conocimientos o apoyo en la toma de decisiones. La identidad de una persona que participa en la investigación no se dará a conocer al usuario de la información sin el consentimiento expreso de dicha persona y no se le realizará acción de venta como resultado directo de haber proporcionado información.

Recogida de datos pasiva significa datos recogidos sin emplear el sistema tradicional de preguntar y responder a preguntas.

Datos personales significa cualquier información relativa a una persona física identificada o identificable (es decir, un particular y no una persona jurídica u otra entidad asimilable). Una persona identificable es alguien que pueda ser identificado, directa o indirectamente, en particular mediante un número de identificación o mediante las características físicas, fisiológicas, psíquicas, económicas, culturales o sociales de dicha persona. En algunos tipos de investigación tales ficheros de datos podrían incluir situaciones en las que los individuos podrían ser identificados mediante fotografías, grabaciones de audio o video u otra información personal recogida durante la investigación.

Tratamiento de datos personales incluye, pero no se limita a, su recogida, registro, organización, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de comunicación, cotejo o interconexión, bloqueo, supresión o destrucción, ya sea por medios automatizados o de otro modo.

Participante en la investigación significa cualquier persona cuyos datos personales se recogen en un proyecto de investigación, ya sea por una entrevista activa o por medios pasivos.

Investigador significa cualquier individuo u organización que lleva a cabo, o que actúa como consultor, un proyecto de investigación de mercados, incluyendo a los que trabajan en la organización del cliente así como los subcontratistas utilizados, por ejemplo un proveedor de tecnología.

Cliente de la investigación o usuario de los datos significa cualquier persona u organización que solicita, comisiona, patrocina o suscribe la totalidad o parte de un proyecto de investigación.

Datos sensibles significa cualquier información de personas identificables relativa al origen racial o étnico, la salud o la vida sexual, antecedentes penales, opiniones políticas, creencias religiosas o filosóficas o afiliación sindical. Otro tipo de información puede ser considerada como sensible en diferentes jurisdicciones. En los EE.UU., por ejemplo, la información relativa a la salud personal, los ingresos u otra información financiera, identificadores financieros y documentos de identidad emitidos por el gobierno es también considerada como sensible.

Transferencia en relación a datos se refiere a cualquier divulgación, comunicación, copia o movimiento de datos de una entidad a otra, independientemente del medio, incluyendo pero no limitado al movimiento a través de una red, las transferencias físicas, las transferencias de un medio o dispositivo a otro, o por el acceso remoto a los datos.

Transferencia internacional de datos personales significa el movimiento de datos personales fuera de la frontera nacional por cualquier medio, incluyendo el acceso a los datos desde fuera del

país donde fueron recogidos y el uso de las tecnologías de almacenamiento en la nube de los datos.

5. LISTA DE CONTROL SOBRE LA POLÍTICA Y LOS PROCEDIMIENTOS DE PROTECCIÓN DE DATOS

Los usuarios de la siguiente lista de control pueden notar que los epígrafes y el orden de los temas no son los mismos que los utilizados por la OCDE. La intención aquí es expresar los principios en un lenguaje y en un orden que es más familiar para el investigador. Los usuarios también pueden ver que los temas están interrelacionados y a veces se superponen. **No obstante, es esencial que la lista de control sea vista como un todo y que los temas individuales sean vistos como complementarios y no excluyentes, prestando especial atención a las diferencias que dependen de si una organización está actuando como responsable del tratamiento o como encargado del tratamiento. Cualquier pregunta para la que la respuesta no sea un "sí", indica una brecha potencial en un esquema de protección de la privacidad y por lo tanto un riesgo potencial de violar una o más leyes de protección de datos.**

5.1 Impacto mínimo

1. *Cuando se diseña un proyecto de investigación, ¿limita usted la recogida de datos personales sólo a aquellos que sean necesarios para los fines de la investigación y se asegura de que no se utilizan en cualquier forma incompatible con estos fines?*

El investigador sólo debe recoger y/o mantener los datos personales necesarios para asegurar que se realizó una entrevista con una persona en concreto y/o que puedan ser necesarios por motivos de control de calidad, de muestreo y/o de análisis. En el caso de la investigación B2B, esto incluye datos personales relativos al puesto o nivel del participante dentro de una empresa, ya que pueden ser necesarios para la finalidad de la investigación.

Este mismo principio se aplica a los métodos de recogida de datos pasivos en los que los datos personales pueden ser recogidos sin emplear el método tradicional de preguntar y responder a preguntas. Por lo tanto, es responsabilidad del investigador asegurar que los únicos datos personales recogidos son aquellos que sean necesarios para la finalidad de la investigación. En el caso de que se reciban otros datos personales, éstos deben ser filtrados y eliminados.

2. *¿Implementa usted procesos que garanticen que los participantes de la investigación no se vean perjudicados o afectados negativamente como resultado directo de su participación en un proyecto de investigación de mercado?*

El investigador debe asegurarse de que los datos personales no puedan ser rastreados ni pueda inferirse la identidad de un individuo mediante análisis cruzados (divulgación deductiva), existencia de muestras pequeñas o por cualquier otra forma de los resultados de la investigación. Ejemplos de esto serían: fusionando información auxiliar, como por ejemplo: usando datos de la zona geográfica o la capacidad de identificar a un empleado específico en una encuesta de satisfacción del cliente.

3. *Si usted va a emplear subcontratistas u otros proveedores para prestar los servicios en su nombre, ¿les suministra la mínima cantidad de información personal que sea necesaria para que puedan llevar a cabo los servicios pactados? ¿Tiene usted establecidos contratos que garanticen un nivel similar de protección por parte de éstos?*

Cuando se emplee un subcontratista, proporcione sólo la mínima cantidad de datos personales que sean necesarios para prestar el servicio acordado, siempre dejando claro a través de contratos y de instrucciones cuáles son las responsabilidades del subcontratista mientras esté en posesión de esos datos. Todos los subcontratistas deben adherirse a las mismas normas y reglamentos que el instituto de investigación. Además, la transferencia de datos personales a un subcontratista u otro proveedor sólo debe realizarse con el previo consentimiento o por encargo del cliente del instituto de investigación.

Lo anterior supone que a los participantes en la investigación se les asegurará que todos los datos recogidos serán mantenidos de forma confidencial y sólo se analizarán y reportarán a nivel agregado. Si los participantes en la investigación dan su consentimiento para vincular sus respuestas a sus datos personales, entonces deben ser informados cómo se compartirá y utilizará esa información.

5.2 Información y consentimiento

4. ¿Obtiene usted el consentimiento de cada participante cuyos datos personales se recogen?

En virtud de los Principios de Privacidad de la OCDE los datos personales deberían ser obtenidos por medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del participante en la investigación.

En general, la legislación nacional establece una serie de medios legítimos y justos, pero en la mayoría de los casos el investigador estará obligados a obtener el consentimiento.

Hay casos en los que la responsabilidad de obtener el consentimiento recae en otros. Por ejemplo: el uso de paneles de terceros o el uso de una base de datos del cliente. En este tipo de circunstancias, el investigador debe obtener garantías de que el consentimiento fue obtenido correctamente.

El consentimiento debe ser:

- libre (voluntario y en condiciones de ser retirado en cualquier momento);
- específico (en relación a uno o más fines identificados); e
- informado (con pleno conocimiento de todas las consecuencias relevantes de dar el consentimiento).

El consentimiento también debe provenir claramente de una declaración o acción por parte del participante de la investigación que ha sido informado de lo siguiente: (a) el uso que se dará a sus datos personales; (b) los datos específicos que se recogerán; (c) el nombre, la dirección y la información de contacto de la empresa u organización que recoge los datos y, si no son para dicha organización, el responsable del tratamiento; y (d) si los datos serán cedidos a terceros.

El investigador debería decidir cuidadosamente el mecanismo utilizado para obtener el consentimiento, normalmente expresado como opt-out, opt-in, implícito, informado o explícito. El método específico elegido debería estar documentado.

En general, cuanto más sensible, intrusiva o no evidente sea la recogida de datos, mayor debe ser el requisito de consentimiento que se requiere. En algunas jurisdicciones existen tipos de "datos personales sensibles" que requieren el consentimiento expreso de las personas afectadas antes de que puedan ser recogidos.

Puede haber casos en los que el investigador recoja o reciba datos de carácter personal de forma no intencionada o de personas que no sean participantes. Por ejemplo: información ofrecida voluntariamente por los participantes; listas suministradas por el cliente que contienen más información que la necesaria para realizar la investigación; y personas que no son participantes que han sido capturadas en fotografías o en video. El investigador debe tratar dicha información de la misma manera que los otros datos personales. A estos datos se les debería eliminar cualquier identificación o ser destruidos de inmediato, sobre todo si no hay manera de informar a las personas cuyos datos se han recogido sobre su paradero, almacenamiento o uso. En algunas jurisdicciones es obligatorio borrar dicha información o tratarla exactamente de la misma manera que otra información que ha sido capturada intencionalmente.

5. *¿Es usted transparente en relación a la finalidad o finalidades para las que se han recogido y mantenido los datos?*

En el sector de la investigación se ha mantenido durante mucho tiempo una distinción entre la investigación de mercado y la recopilación de datos para otros fines tales como la publicidad, promoción de ventas, elaboración de bases de datos, marketing directo y venta directa. Esta distinción es un ingrediente crítico para la diferenciación de la finalidad y para la promoción de una imagen positiva de la investigación a los ojos de los reguladores y del público en general. En los últimos años, la aparición de nuevas tecnologías ha aumentado las oportunidades para recoger información personal a través de técnicas como el seguimiento online y aplicaciones descargables para móviles.

En todos los casos es esencial que, antes de recoger cualquier dato, los posibles participantes en la investigación sean informados sobre la finalidad para la que se utilizarán sus datos y las consecuencias potenciales que puedan resultar, incluyendo para la finalidad de un contacto de seguimiento con objeto de control de calidad.

Cuando el investigador recoja datos personales de un participante en una investigación para ser usados con fines de investigación de mercados, la transparencia hacia el participante de la investigación es un elemento crítico en la comunicación. Al participante en una investigación se le debe dar suficiente información sobre el uso previsto de los datos personales recogidos y cualquier comunicación de los mismos a terceros. A modo de ejemplo, si el uso previsto de los datos personales es vincular la respuesta a una encuesta con el perfil del cliente, el participante en la investigación debe ser informado de esto en el momento de la recogida de los datos de carácter personal.

Los avisos de privacidad deben ser revisados de forma regular para asegurarse de que el tipo de datos recogidos y los usos previstos no han cambiado, y el investigador debe asegurarse de que las prácticas de negocio y las tecnologías que se utilizan dentro del instituto de investigación son consistentes con los compromisos asumidos con los participantes en la investigación y cumplen con los requisitos reglamentarios vigentes en cada momento.

Cada uso propuesto de datos personales debe ser analizado para garantizar el cumplimiento de la legislación local sobre privacidad, del Código CCI/ESOMAR y las Guías de ESOMAR, y la coherencia con los compromisos de privacidad asumidas con los participantes en la investigación.

6. *¿Es usted transparente acerca de los datos específicos que se recogen?*

Dada la amplia definición de datos personales en algunas jurisdicciones, se deben considerar todos los posibles elementos de datos personales que pueden ser recogidos a la hora de redactar la información a los participantes en la investigación.

Los datos personales pueden incluir: nombre, dirección, correo electrónico, número de teléfono, número de móvil, fecha de nacimiento, identificador de dispositivo móvil, dirección IP, fotografías, grabaciones de audio y video, número de identificación nacional (permiso de conducir, tarjeta de seguridad social, etc.), identificador de usuario asignado por su organización, nombre de usuario en medios sociales, datos almacenados en una cookie o píxel/etiqueta de seguimiento.

Recuerde también que un solo elemento de dato, por sí mismo, puede no ser considerado como dato personal identificable conforme a la legislación local, pero cuando se combina con otros datos (por ejemplo, código postal, sexo, lugar de trabajo o escuela, puesto y sueldo) puede permitir a una persona ser identificada individualmente.

Además, tenga en cuenta todos los posibles destinatarios de los datos personales. Los investigadores, las agencias de investigación, los proveedores de servicios y/o los clientes finales pueden tener la capacidad de recoger y/o utilizar los datos personales en el curso de un proyecto de investigación.

7. *¿Deja usted claro cómo serán recogidos los datos, incluyendo cualquier recogida pasiva de datos de la que el participante puede no ser consciente?*

Históricamente la investigación se ha basado en la entrevista como método principal para la recogida de datos personales. Como se señaló en el punto 5 anterior, las nuevas tecnologías han hecho posible recoger una gama más amplia de datos de carácter personal sin el conocimiento de las personas cuyos datos se recogen. Todos los participantes en la investigación deben ser informados acerca de qué datos específicos se recogen y el método de recogida utilizado, ya sea por un medio activo como puede ser una entrevista, por un medio pasivo, por medio de una aplicación para móvil o mediante un seguimiento del comportamiento online a través de cookies.

El investigador debe tener en cuenta qué elementos de los datos recogidos y/o método de recogida de datos podría no ser previsto por un participante en la investigación y proporcionarle una información suficiente en relación con tales métodos de recogida. Considere el uso de avisos "de formato abreviado" que remiten a una información más detallada sobre privacidad para describir una recogida o uso de datos que podría ser inesperado o invasivo. Las aplicaciones para móviles, en particular las que incluyen la geo-localización, "escucha pasiva" y/o la medición del sistema operativo del dispositivo móvil, requieren una descripción detallada y el consentimiento explícito del participante en la investigación a tales actividades.

5.3 Integridad/Seguridad

8. *¿Cuenta con procedimientos para garantizar que todos los datos personales recogidos son exactos, completos y actualizados?*

Los controles de calidad se deberían realizar en cada etapa del proceso de investigación. En el diseño de cuestionarios o aplicaciones de investigación, deberían realizarse pruebas antes del inicio del trabajo de campo para minimizar el riesgo de errores en la recogida de datos. Durante la fase de trabajo de campo, la monitorización y la validación de las entrevistas deberían llevarse a cabo conforme a las normas de calidad aplicables a la investigación. Durante las fases del proceso de datos y la comunicación de los resultados, se deberían realizar controles de calidad adicionales para asegurar que los datos son correctos y que los análisis, conclusiones y recomendaciones son consistentes con los datos.

El investigador que gestiona paneles debería garantizar que los panelistas puedan revisar y actualizar sus datos de perfil en cualquier momento y se les debería recordar periódicamente que lo hagan. Las muestras extraídas de un panel deberían incluir información sociodemográfica

actualizada. Para esto, una buena fuente para consultar prácticas normalizadas es ISO 26362:2009 – Access panels in market, opinión and social research.

9. *¿Se asegura usted de que los datos personales no se mantienen por más tiempo que el necesario para la finalidad para la que se recogió o procesó la información? ¿Tiene usted procedimientos para almacenar por separado o eliminar los datos de identificación de los ficheros de datos una vez que ya no son necesarios?*

El investigador debería establecer períodos de conservación de los datos de forma que sean lo más cortos posible; pero en todo caso, dichos periodos deben estar basados en la legislación aplicable, la fuente de los datos personales recogidos y dependiendo de si actúa como responsable del tratamiento o como encargado del tratamiento de los datos. En este último caso, los clientes pueden imponer por contrato periodos de retención.

En cuanto a la fuente de los datos personales, normalmente se utilizará y conservará información de estudios longitudinales o de información de perfil de los panelistas durante todo el tiempo que permanezcan como miembros activos. Por el contrario, se debería aplicar un período de retención más corto a los datos personales de participantes no panelistas que participan en una investigación ad-hoc. Obviamente, es importante no eliminar sus datos de carácter personal demasiado pronto ya que se deben realizar controles de calidad durante la fase de tratamiento de datos para asegurar la exactitud y para satisfacer las exigencias del principio de integridad de la privacidad de los datos.

Cuando se utilizan datos personales, la mejor práctica para el investigador es utilizar identificadores disociados.

Se debe mantener de forma segura y con acceso limitado al menor número posible de personas (por ejemplo, el personal de gestión del panel o de elaboración de muestras) un archivo maestro que asocie los nombres, direcciones o números de teléfono de los participantes con sus correspondientes números de identificación generados internamente. Así, los investigadores, el personal de tratamiento de datos o de codificación que necesiten analizar los datos a nivel de cada participante, pueden hacerlo sin ver los nombres, direcciones o números de teléfono de los participantes.

Cuando las respuestas del estudio hayan sido procesadas y se hayan reportado como datos estadísticos agregados, los datos personales de los participantes, junto con sus correspondientes identificadores disociados, deberían eliminarse de modo que el instituto de investigación no mantenga datos de carácter personal.

10. *¿Cuenta usted con procedimientos establecidos para responder a las solicitudes de las personas relativas a los datos personales que se les hayan recogido? ¿Los procedimientos para tramitar las solicitudes de acceso de los individuos incluyen comprobar la identidad del solicitante y responder a sus solicitudes en un período de tiempo razonable, permitiéndoles corregir los datos inexactos o eliminar los datos por completo?*

Deberían desarrollarse, comunicarse y cumplirse procedimientos formales para responder a las personas que deseen acceder a los datos personales que mantiene el instituto. Es importante comprobar la identidad de las personas que solicitan el acceso para evitar comunicar datos personales a otras personas inapropiadamente.

Una vez que la identidad de una persona que hace una solicitud de acceso ha sido comprobada - la persona es quien dice ser y tiene el derecho legal para acceder a los datos personales en cuestión- el investigador debería esforzarse por cumplir con la solicitud de acceso lo más rápido posible; por ejemplo, dentro de 10 a 30 días, dependiendo de la legislación aplicable. Si el instituto

de investigación requiere tiempo adicional para cumplir con la solicitud, es posible extender el plazo establecido en la ley, siempre que el solicitante sea informado y se cuente con razones de peso para ampliar el plazo. Puede ser necesario este tiempo adicional, por ejemplo, para realizar consultas o para reunir la información solicitada de varias bases de datos.

Aunque la legislación de protección de datos puede incluir exenciones que obligan a las organizaciones a rechazar el acceso a una persona a su información personal en ciertas situaciones, no es probable que esas exenciones sean de aplicación a los datos de carácter personal que se tratan en el marco de una investigación de mercado. Por ejemplo, la legislación aplicable puede permitir a las organizaciones negar solicitudes de acceso si la información está sujeta a la confidencialidad entre abogado y cliente. Otro ejemplo podría ser si la organización ha comunicado información a un órgano gubernamental por motivos de cumplimiento de la ley o de seguridad nacional, dicho órgano puede dar instrucciones a la organización en el sentido de denegar el acceso o no revelar que se les ha comunicado la información.

11. ¿Cuenta usted con protocolos de seguridad establecidos para cada fichero de datos de forma que se proteja contra riesgos tales como la pérdida o el acceso, destrucción, uso, modificación o divulgación no autorizados?

El cumplimiento de estas responsabilidades comienza con el desarrollo e implementación de una política de seguridad para proteger los datos de carácter personal y otro tipo de información confidencial. ISO 27001 es una norma reconocida de seguridad de la información en la que puede basarse una política de seguridad exhaustiva.

El uso de medidas de seguridad apropiadas para proporcionar la protección necesaria incluye:

- medidas físicas (archivadores cerrados con llave, restringiendo el acceso a las oficinas, sistemas de alarma, cámaras de seguridad);
- herramientas tecnológicas (contraseñas, encriptación, firewalls);
- controles en la organización (verificación de antecedentes, normas relativas a sacar ordenadores fuera de las instalaciones, limitando el acceso sobre la base de la "necesidad de conocer", formación del personal, acuerdos con clientes y subcontratistas).

La política de seguridad debería incluir también un procedimiento para hacer frente a una posible violación de datos de carácter personal a consecuencia de la cual se revelen datos personales. Si los datos fueron recogidos y proporcionados por un tercero, por ejemplo una base de datos de un cliente, dicho tercero deberá ser informado inmediatamente. También debe informarse a los participantes cuyos datos fueron revelados si dicha revelación les expone a algún riesgo (por ejemplo, el robo de identidad) y deben adoptarse medidas para proteger contra ese riesgo.

12. ¿Cuenta usted con una declaración clara del plazo de retención los datos personales?

El plazo de retención de los datos personales puede variar de un proyecto de investigación a otro dependiendo de una variedad de circunstancias indicadas anteriormente en la respuesta a la pregunta 9.

Aunque las normas generales sobre plazos de retención deberían estar incluidas en la política de privacidad, puede no siempre ser práctico informar de los plazos de retención exactos en los diferentes tipos de investigación. Por lo tanto, el investigador también debería considerar comunicar la información sobre retención de datos en la herramienta de captación del estudio, en la introducción del cuestionario o en formularios para obtener el consentimiento específico del estudio. Siempre se debería estar preparado para informar, bajo petición, de los plazos de retención de datos en un proyecto determinado.

5.4 Transferencia de datos

13. *¿Cuenta usted con normas y procedimientos definidos que determinen el uso y la divulgación de los datos personales?*

Estas reglas y procedimientos están claramente descritos en la legislación local sobre privacidad y protección de datos que existe en su país. Una explicación de lo que eso significa debería estar claramente documentada junto con procesos y documentos escritos para asegurar que el personal pueda aplicar los protocolos relativos a cómo gestionar los datos personales y para que el personal este familiarizado con estas normas y procedimientos. Por ejemplo, esto incluirá el principio de que se requiere el consentimiento del participante en la investigación antes de que sus datos puedan ser revelados, incluso a los clientes o a los investigadores de la organización del cliente.

14. *¿Las condiciones bajo las cuales los datos personales pueden ser revelados están claras y sin ambigüedades?*

Los participantes en la investigación deben saber lo que se hace con sus datos personales y esto debe ser explicado verbalmente o proporcionado en algún documento escrito con el que estén de acuerdo los participantes en la investigación -es decir, a través de su consentimiento que debe ser registrado como evidencia de que están de acuerdo-.

15. *¿Está su personal al tanto de esas reglas y está formado en la manera de aplicar los procedimientos?*

Su política de privacidad describe las prácticas de recopilación y gestión de datos de su empresa. Es igualmente importante desarrollar internamente procedimientos operativos estandarizados (SOP) para asegurar que se cumplen los compromisos de privacidad con los participantes.

La formación del personal sobre la privacidad debería incluir una visión general de la legislación aplicable, los códigos de conducta sectoriales, las políticas de privacidad de su empresa de cara al consumidor y sus protocolos normalizados de trabajo. Debería proporcionarse formación sobre privacidad al menos anualmente y deberían mantenerse registros de asistencia.

Todo el personal de primera línea que interactúa con los participantes debería ser capaz de explicar con suficiente detalle las políticas y procedimientos de su empresa. Deberían saber a quién dirigirse internamente para obtener ayuda en caso de dudas que no sean capaces de responder.

Deberían definirse claramente las responsabilidades y se debería realizar una supervisión, incluyendo alguna forma de comprobar que se están cumpliendo los procedimientos.

5.5 Transferencia internacional de datos personales

16. *Si los datos personales se transfieren de una jurisdicción a otra, ¿se hace de tal manera que se cumpla con los requisitos de protección de datos, tanto en la jurisdicción de origen y como la de destino?*

Esto se refiere a menudo como una "transferencia internacional de datos personales". Ocurre cuando los datos son recogidos fuera de las fronteras nacionales y/o cuando el tratamiento de datos está deslocalizado o subcontratado en otro país; por ejemplo, cuando un cliente encarga a un investigador de otro país llevar a cabo un estudio con datos proporcionados por el cliente de sus consumidores o clientes. Cada país tiene sus propias normas sobre cómo deben ser tratados y protegidos los datos de carácter personal, normas que el investigador debe cumplir. Si bien esto puede parecer complejo, puede ser de ayuda si los aspectos de cumplimiento a los que se enfrenta el investigador se dividen en tres principales:

- Asegurar que la transferencia internacional de datos personales se realiza de acuerdo con la legislación nacional. La base más común para asegurar la adecuada protección en una transferencia internacional es mediante el consentimiento o el uso de cláusulas contractuales apropiadas y, cuando sea necesario por la legislación nacional aplicable, la obtención de la autorización previa de la Autoridad Nacional de Protección de Datos u otra autoridad reguladora de la privacidad aplicable en el uso de esos contratos. Como medida de seguridad adicional y para reducir aún más el riesgo cuando se deslocalice el tratamiento de datos, se deberían eliminar los datos personales identificados cuando sea posible, de modo que sólo se utilice un número de identificación disociado para vincular los datos a nivel individual con la identidad de los participantes.

- El grado en que un investigador puede llevar a cabo una transferencia internacional al actuar como encargado del tratamiento, como por ejemplo cuando se lleva a cabo un estudio utilizando una muestra suministrada por el cliente. Incluso cuando el investigador ha tenido la precaución de asegurar que todas las transferencias internacionales cumplen las normas que regulan dichas transferencias, también debería tener en cuenta cuando actúa como encargado del tratamiento (es decir, cuando actúa en nombre de un responsable del tratamiento, por ejemplo el cliente de la investigación), ya que el responsable del tratamiento puede no permitir la transferencia internacional de los datos personales de los que es responsable, lo que puede afectar la forma en que se pueda llevar a cabo el proyecto. Debería haber un acuerdo por escrito en vigor entre ambas partes sobre lo anterior.

- La transferencia internacional de datos personales en la recogida de datos personales de participantes en la investigación de otros países; por ejemplo, en encuestas online dirigidas a participantes de la investigación residentes en un país distinto del que el investigador que está realizando el estudio. La legislación aplicable sobre privacidad será normalmente la nacional del país donde el investigador esté basado. Sin embargo, el investigador también debe garantizar que el estudio o el panel es compatible con cualquier otra legislación nacional aplicable en el país donde se están recogiendo los datos. Las prácticas recomendadas incluyen asegurarse de que: (1) en toda herramienta de captación se informa claramente de los datos legales del investigador (nombre de la empresa, dirección postal, etc.), incluyendo el país; (2) la política de privacidad online utilizada incluye una declaración simple pero clara e inequívoca de la transferencia internacional que se realizará derivada de la participación en el estudio o en el panel; y (3) hay una referencia a la transferencia internacional en la pregunta de consentimiento en la captación del panel.

5.6 Externalización y subcontratación

17. *¿Cuenta usted con requisitos claros, incluyendo controles adecuados, para los encargados del tratamiento externos u otros subcontratistas?*

Deben comunicarse requisitos claros a todos los encargados del tratamiento externos, u otros subcontratistas, relativos al cumplimiento de las normas de protección de datos aplicables a los

datos personales cuando se transfieran datos por cualquier medio. Debería haber una protección adicional en la transmisión de los datos, ya sea a nivel individual o agregado, mediante el uso de procesos informáticos específicos, tales como el encriptado de los datos transferidos o el uso de plataformas de transferencia FTP seguras. Si los subcontratistas o encargados del tratamiento externos van a realizar copias de seguridad de cualquier dato, entonces debe haber procesos claros para proteger esos datos durante el almacenamiento y para su eliminación cuando ya no se necesiten.

5.7 Política de privacidad

18. *¿La información sobre su política de privacidad y normas de protección de datos personales está fácilmente disponible y en una forma que sea fácilmente comprensible para los participantes?*

Muchas jurisdicciones requieren que la información esté disponible en una política de privacidad que esté fácilmente disponible para los participantes en una investigación. Aunque el contenido y detalle requerido varía de un país a otro, el investigador siempre debe identificarse claramente a los participantes en la investigación y asegurarse de que se explica: el propósito de la investigación, cómo se recogen los datos personales, la forma en que se gestionarán (recogida, almacenamiento, uso, acceso y comunicación) y cómo obtener más información o presentar una queja.

El investigador debe asegurarse de que las políticas son fáciles de entender, relevantes para el lector, fácil de localizar, lo más concisas posible y adaptadas a las operaciones de la organización. Esto incluye disponer de la política en tantos idiomas como sea práctico y revisar y actualizar la política cuando sea necesario.

19. *¿Queda clara la identidad y la responsabilidad del responsable del tratamiento?*

El investigador debe asegurarse de que sus propios roles y responsabilidades en la gestión de datos de carácter personal están claros para los participantes en la investigación. Esto incluye la identificación del responsable del tratamiento y si se emplea a algún encargado del tratamiento externo. Los participantes no deben tener dudas acerca de qué organización es responsable en última instancia de la gestión de sus datos.

Algunas jurisdicciones también requieren que un individuo específico sea identificado como responsable de los procesos de protección de datos de la compañía.

En el caso de las encuestas en las que no se identifica al cliente y en las que se utilizan muestras proporcionadas por este, los participantes deberían ser informados de que el nombre del cliente no será revelado hasta el final de la encuesta porque la divulgación de esta información por adelantado podría introducir un sesgo en la respuesta. Dado que en muchos casos la legislación nacional de protección de datos otorga a los participantes un derecho legal de saber de quién ha obtenido el investigador sus datos de carácter personal, el investigador debe estar preparado para identificar el nombre del cliente en cualquier momento a solicitud de los participantes.

20. *¿Está claro que el responsable del tratamiento es el responsable de los datos personales bajo su control, independientemente de la ubicación de los datos?*

Si el investigador puede subcontratar el tratamiento o transferir datos personales fuera de su propio país, debería estar preparado para informar al responsable del tratamiento de los detalles de los subcontratistas y la ubicación donde se realiza el proceso de los datos; y obtener el consentimiento previo por escrito del responsable del tratamiento cuando sea necesario. Cuando el instituto de investigación es el responsable del tratamiento, debería incluir referencias a la

utilización de un encargado del tratamiento y, en su caso, una lista de los países o regiones en su política de privacidad. El investigador debería estar alerta ante el hecho de que algunas jurisdicciones prohíben a los investigadores la transferencia de datos personales a países o regiones cuya legislación no tiene un nivel equivalente de protección de datos. Sujeto al cumplimiento de las normas que rigen la transferencia internacional impuestas por la legislación nacional local relevante, la transferencia de información personal dentro de una multinacional está permitido por la mayoría de las jurisdicciones, aunque algunos países requieren que se informe al titular de los datos personales dónde pueden estar situados sus datos.

6 CUESTIONES ESPECIALES

6.1 Recogida de datos de niños

La legislación nacional que fija la edad en la que ya no se requiere permiso de los padres varía sustancialmente. El investigador debe consultar la legislación nacional y los códigos de autorregulación en las jurisdicciones en las que se recogerán los datos, para determinar si se requiere el permiso de los padres o donde las sensibilidades culturales requieren un tratamiento particular. En ausencia de directrices nacionales, consulte la Guía ESOMAR, para entrevistas a niños y jóvenes.

La recogida de datos de niños requiere un permiso verificable del tutor legal del niño. Se le debe proporcionar al padre o adulto responsable suficiente información sobre la naturaleza del proyecto de investigación para permitirle tomar una decisión informada acerca de la participación del niño.

El investigador debería registrar la identidad del adulto responsable y su relación con el niño.

6.2 Investigación business-to-business

Un número considerable de proyectos de investigación implican la recogida de datos de personas jurídicas tales como empresas, escuelas, organizaciones sin ánimo de lucro y organizaciones similares. Tal investigación supone a menudo la recogida de información sobre la entidad, por ejemplo: facturación, número de empleados, sector, ubicación, etc.

En todos estos casos, las organizaciones participantes tienen derecho al mismo nivel de protección ante la revelación de su identidad el entregar los resultados que la ofrecida a personas individuales en otros tipos de investigación.

Vale la pena señalar que en muchos casos la legislación nacional de protección de datos considera que el título y los datos de contacto del lugar de trabajo de un individuo son datos de carácter personal. Algunas leyes de protección de datos van más allá y consideran de aplicación sus requisitos tanto a las personas físicas como a las jurídicas (por ejemplo, personas individuales y empresas).

6.3 Fotografías y grabaciones de audio y video

Numerosas técnicas nuevas de investigación crean, almacenan y transmiten fotografías y grabaciones de audio y vídeo como parte del proceso de investigación. Dos ejemplos destacados son la investigación etnográfica y los estudios mystery shopping.

El investigador debe reconocer que las fotografías y las grabaciones de audio y vídeo son datos personales y deben ser tratados como tales. Si el investigador solicita a los participantes que

proporcionen información en estos formatos, también debería proporcionar orientación sobre cómo minimizar la recogida de datos no solicitados, especialmente de personas no participantes.

Por último, algunos tipos de investigación observacional pueden implicar fotografiar, filmar o grabar en lugares públicos que afectan a personas que no han sido captadas como participantes en la investigación. En tales instancias el investigador debe obtener permiso para compartir este tipo de imágenes de aquellos individuos cuyas caras son claramente visibles y puedan ser identificados. Si no se puede obtener el permiso, entonces la imagen de la persona debería ser pixelada o anonimizada de otra manera. Además, deberían colocarse carteles claros y legibles para indicar que la zona está bajo observación, junto con los datos de contacto de la persona u organización responsable. Las cámaras deberían estar situadas de forma que capten sólo las zonas destinadas a la observación.

6.4 Almacenamiento en la nube

La decisión de almacenar datos personales en la nube debería ser meditada cuidadosamente. El investigador debe evaluar los controles de seguridad del proveedor de servicios de almacenamiento en la nube y sus términos y condiciones estándar. Muchos proveedores de servicios de almacenamiento en la nube ofrecen indemnizaciones débiles en el caso de que originen brechas de seguridad y los datos personales estén en peligro. Esto significa que la organización del investigador estaría asumiendo un riesgo considerable de daños económicos y pérdidas debido a graves violaciones a la privacidad que resulten en daños a los individuos afectados.

Por lo tanto, el investigador debería implementar controles de compensación para protegerse contra tales riesgos. Por ejemplo, debería encriptar los datos personales en movimiento (transferidos a/desde la nube) y en depósito (almacenados en los servidores del proveedor de nube). El investigador también debería considerar la contratación de una póliza de seguro para responsabilidad informática.

El investigador también debe tener en cuenta la ubicación física donde los datos personales se almacenan para determinar si el uso de almacenamiento en la nube supone una transferencia internacional. Consulte la Sección 5.5 de este documento para más información. Algunos proveedores de servicios de almacenamiento en la nube ofrecen lugares de almacenamiento en países específicos que pueden ser apropiados en algunos casos.

Por último, el investigador debería ubicar los datos personales en una nube privada, en lugar de en una pública. La nube privada es la que asigna, en un centro de datos particular, equipamiento informático exclusivo para la empresa del investigador. El principal beneficio de una nube privada es que el investigador siempre sabe dónde se encuentran los datos personales. Por el contrario, una nube pública puede implicar que los datos estén situados en dos o más centros de datos y en dos o más continentes, con la posible aparición de problemas de cumplimiento, tanto de los requisitos aplicables de acuerdo con la legislación sobre protección de datos como de los contratos suscritos con los responsables del tratamiento, que especifican dónde se deben ubicar los datos personales.

6.5 Datos anonimizados y disociados

Una parte clave de la responsabilidad de protección de datos de un investigador es eliminar la identificación de los datos antes de su liberación a un cliente o incluso al público en general. El proceso de anonimizar es una salvaguardia que implica la supresión o modificación de datos de identificación personal resultando en datos que no identifiquen individuos. Los ejemplos incluyen

el desenfoque de imágenes para disfrazar las caras o la entrega de resultados agregados de forma estadística para asegurar que no se pueda identificar a un individuo en particular.

Disociar implica la modificación de los datos personales de tal manera que todavía es posible distinguir los individuos en un conjunto de datos mediante el uso de un identificador único (por ejemplo con un número de identificación o con algoritmos de modificación), mientras se mantienen sus datos personales por separado para fines de control (ver P9).

Cuando se utilicen estas técnicas, el investigador debería consultar la legislación nacional y los códigos locales de auto-regulación para determinar qué elementos deben ser eliminados para satisfacer los requisitos legales en los procesos de anonimización/disociación de dichos datos.

7 FUENTES Y REFERENCIAS

DLA Piper, Data Protection Laws of the World
EphMRA Adverse Event Reporting Guidelines 2014
Código Internacional ICC/ESOMAR Para la Práctica de la Investigación Social y de Mercados
Guía ESOMAR para entrevistas a niños y jóvenes
ISO 26362:2009 – Access panels in market, opinion, and social research
ISO 20252 – Investigación de mercados, social y de la opinión
OCDE Principios de Privacidad

8 EL EQUIPO DEL PROYECTO

Co-presidentes:

- Reg Baker, Consultor del Comité de Normas Profesionales de ESOMAR y Marketing Research Institute International
- David Stark, Vicepresidente, Integrity, Compliance and Privacy, GfK

Miembros del equipo del proyecto:

- Debrah Harding, Director General, Market Research Society
- Stephen Jenke, Consultor
- Kathy Joe, Director de International Standards and Public Affairs, ESOMAR
- Wander Meijer, COO Global, MRops
- Ashlin Quirk, Consejero General en SSI
- Barry Ryan, Director - Policy Unit, MRS
- Jayne Van Souwe, Director, Wallis Consulting Group