Códigos y Directrices de Investigación Mundial

LISTA DE CONTROL DE PROTECCIÓN DE DATOS DE ESOMAR

Revisada el 6 de Junio de 2017

ESOMAR es el portavoz mundial de la comunidad de datos, investigación y análisis, representando a más de 4900 profesionales individuales y 500 empresas que prestan o encargan análisis de datos o investigación en más de 130 países, aceptando todos ellos el Código Internacional CCI/ESOMAR.

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, el EU-US Privacy Shield Framework, el Suiza-US Privacy Shield Framework, 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 un tratamiento 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. 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

Actividad ajena a la (o que no es) investigación significa tomar una acción directa hacia un individuo cuyos datos personales han sido recogidos o analizados con la intención de cambiar sus actitudes, opiniones o acciones.

Análisis de datos significa el proceso de examinar conjuntos de datos para descubrir patrones ocultos, correlaciones desconocidas, tendencias, preferencias, y otra información útil para fines de investigación.

Aviso de privacidad (en ocasiones referido como política de privacidad) significa un resumen publicado de las prácticas de privacidad de una organización y que describen la manera en que una organización recoge, usa, comunica y gestiona los datos personales de un individuo.

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.

Consentimiento significa el acuerdo libre e informado dado por una persona para la recogida y tratamiento de sus datos personales.

Daño significa daño tangible y material (como puede ser una lesión física o una pérdida económica), daño intangible o moral (como pueden ser daños a la reputación o clientela, o una intrusión excesiva en la vida privada, incluyendo mensajes individualizados de marketing no solicitados).

Datos personales (en ocasiones denominado información de identificación personal o IIP) significa cualquier información relacionada con una persona física viva (aquí referida como “el interesado”) que puede usarse para identificar a un individuo, por ejemplo por referencia a identificadores directos (como pueden ser un nombre, una localización geográfica específica, un número de teléfono, una imagen o una grabación de audio o video) o indirectamente por

referencia a las características físicas, fisiológicas, mentales, económicas, culturales o sociales de un individuo.

Datos primarios significa datos recogidos por un investigador sobre un individuo con fines de investigación.

Datos secundarios significa datos recogidos para otra finalidad y subsecuentemente empleados en la investigación.

Datos sensibles significa tipos específicos de información personal para los que la legislación local requiere sean protegidos con los estándares más elevados que sea posible para prevenir el acceso no autorizado y salvaguardar la privacidad o seguridad de un individuo u organización y que pueden requerir un consentimiento explícito adicional del interesado para poder ser tratados. La determinación de qué datos son sensibles varía entre jurisdicciones y pueden incluir el origen racial o étnico, registros de salud, la orientación sexual o los hábitos sexuales, antecedentes penales, opiniones políticas, localización, información financiera, creencias religiosas o filosóficas, afiliación sindical, y comportamientos ilegales tales como el consumo de drogas o alcohol.

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.

Individuos vulnerables significa individuos que puedan tener limitada la capacidad de tomar decisiones voluntarias e informadas, incluyendo aquellos con limitaciones cognitivas o incapacidades de comunicación.

Interesado significa cualquier individuo cuyos datos personales son usados en una investigación. También se le denomina “titular de los datos”.

Investigación, que incluye toda investigación de mercado, social y de la opinión, y el análisis de datos, significa la recopilación e interpretación sistemática de información sobre personas u organizaciones. Emplea métodos y técnicas estadísticas y analíticas de las ciencias sociales y conductuales aplicadas para generar perspectivas y apoyar la toma de decisiones a los proveedores de bienes y servicios, gobiernos, ONG’s y al público en general.

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.

Investigador significa cualquier individuo u organización que lleva a cabo un proyecto de investigación de mercado (o actúa como consultor), incluyendo a los que trabajan en la organización del cliente así como los subcontratistas utilizados.

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.

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.

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

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.

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.

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.

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, adquirir, y/o conservar los datos personales necesarios desde una perspectiva 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 pasiva así como cuando se trabaja con fuentes de datos secundarios. Por lo tanto, es responsabilidad del investigador asegurar que los únicos datos personales usados en la investigación sean 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 la organización 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 de la empresa de investigación.

Lo anterior supone que los datos recogidos en la investigación 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 de cómo se compartirá y utilizará esa información.

5.2 Información y consentimiento

4. *¿Cuándo se recogen datos primarios, 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.

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 interesado 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, del responsable del tratamiento; y (d) si los datos serán comunicados a terceros.

El investigador debería considerar 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 personales de forma no intencionada o de personas que no sean participantes en la investigación. 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 interesados 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 interesado para ser usados con fines de investigación de mercados, la transparencia hacia el interesado es un elemento crítico en la comunicación hacia éste. Al interesado 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 interesado debe ser informado de esto en el momento de la recogida de los datos personales.

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 en la organización de investigación son consistentes con los compromisos asumidos con los interesados 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 Internacional CCI/ESOMAR y las Guías de ESOMAR/GRBN, y la coherencia con los compromisos de privacidad asumidas con los interesados.

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 interesados.

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 interesado 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 personales sin el conocimiento de las personas cuyos datos se recogen. Todos los interesados 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, o por un medio pasivo como puede ser 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 del método de recogida de datos podría no ser conocido por un interesado para proporcionarle la información suficiente en relación con tales métodos de recogida. Considere el uso de avisos "de formato abreviado" por capas 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 geolocalización, la "escucha pasiva" y/o la medición del sistema operativo del dispositivo móvil, requieren una descripción detallada y el consentimiento explícito del interesado a tales actividades.

8. *Cuando emplea datos personales recogidos para una finalidad distinta de la investigación (por ejemplo, datos de clientes, datos de redes sociales, etc.) ¿se asegura de que el uso es legítimo y de que se protegen los derechos de los interesados?*

Tanto investigadores como no investigadores buscan cada vez más obtener y usar datos secundarios para aumentar o sustituir la recogida de datos primaria. Antes de acceder y tratar tales datos, el investigador debe asegurarse que su uso previsto es compatible con la finalidad para la

que fueron originalmente recogidos. Debe verificar que la recogida original fue legal y que se contaba con el consentimiento de los interesados, expreso o implícito. Además, debe determinar el interés legítimo garantizando que la finalidad es únicamente para investigación.

El investigador también debe diseñar su investigación de manera que el tratamiento ulterior de los datos no implica un riesgo de causar daños a los interesados. El investigador debe establecer salvaguardias para mitigar el riesgo de tales daños, por ejemplo asegurando que la identidad de los interesados no se descubre o comunica sin su previo consentimiento con medidas para reducir la granularidad de los datos de forma que se reduzca la posibilidad de que se identifique a un individuo, y asegurando de que no se le dirigirá al interesado ninguna actividad ajena a la investigación como consecuencia directa de que sus datos sean usados en una investigación.

5.3 Integridad/Seguridad

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

Deberían realizarse controles de calidad 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.

10. *¿Se asegura usted de que los datos personales no se conservan por más tiempo que el necesario para la finalidad para la que se recogió, obtuvo o trató 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, la información de estudios longitudinales o la de información de perfil de los panelistas normalmente será usada y conservada durante todo el tiempo que permanezcan como miembros activos. Por el contrario, se debería aplicar un período de conservación más corto a los datos personales de interesados no panelistas que participan en una investigación ad-hoc. Obviamente, es importante no eliminar sus datos personales 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, es una buena práctica para el investigador utilizar identificadores seudonimizados.

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 interesados con sus correspondientes números de identificación generados internamente. Así, los investigadores, el personal de proceso de datos o de codificación que necesiten analizar los datos a nivel individual, pueden hacerlo sin ver los nombres, direcciones o números de teléfono de los interesados.

Cuando las respuestas del estudio hayan sido procesadas y se hayan reportado como datos estadísticos agregados, los datos personales de los interesados, junto con sus correspondientes identificadores seudonimizados, deberían eliminarse de modo que la organización de investigación no mantenga datos personales.

11. *¿Tiene establecidos procedimientos para responder a las solicitudes de los interesados relativas a los datos personales que se les hayan recogido? ¿Los procedimientos para tramitar las solicitudes de acceso de los interesados 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 los interesados que deseen acceder a los datos personales que la organización mantiene sobre ellos. Es importante comprobar la identidad de los interesados que solicitan el acceso para evitar comunicar datos personales a otras personas inapropiadamente.

Una vez que la identidad del interesado que solicita el 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 la empresa de investigación requiere un 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 o fuentes.

Aunque la legislación de protección de datos puede incluir exenciones que obligan a las organizaciones a rechazar el acceso de un interesado a su información personal en ciertas situaciones, no es probable que esas exenciones sean de aplicación a los datos personales que se tratan con fines de investigación. 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 persecución de un delito 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.

12. *¿Cuenta usted con protocolos de seguridad establecidos para cada conjunto de ficheros 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 la información personal y otro tipo de información confidencial. ISO 27001 es una norma reconocida de seguridad de la información sobre 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 en la seguridad de los datos a consecuencia de la cual se revelen datos personales. Si se trata de datos secundarios recogidos por un tercero; por ejemplo, una base de datos de un cliente, dicho tercero debe ser informado inmediatamente. También debe informarse a los interesados cuyos datos fueron revelados si dicha revelación les expone a algún riesgo (por ejemplo, el robo de identidad) y de las medidas adoptadas para proteger contra ese riesgo.

13. *¿Cuenta usted con una declaración clara del plazo de conservación de los datos personales?*

El plazo de conservación 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 conservación deberían estar incluidas en los avisos de privacidad, puede no siempre ser práctico informar de los plazos de conservación exactos para los diferentes tipos de investigación. Por lo tanto, el investigador también debería considerar comunicar la información sobre conservación 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 conservación de los datos en un proyecto determinado.

5.4 Transferencia de datos

14. *¿Cuenta usted con normas y procedimientos definidos que determinen el uso y la comunicación 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 interesado antes de que sus datos puedan ser comunicados, incluso a los clientes o a los investigadores de la organización del cliente, e independientemente de que los datos fueran recogidos por el investigador o por un tercero.

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

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

16. *¿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 recogida y gestión de datos de su empresa. Es igualmente importante desarrollar procedimientos operativos internos estandarizados (SOP's) para asegurar que se cumplen los compromisos de privacidad con los interesados.

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 procedimientos operativos internos estandarizados. Debería proporcionarse formación sobre privacidad al menos anualmente y deberían mantenerse registros de asistencia.

Todo el personal de primera línea que interactúa con los interesados 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

17. *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 en la de destino?*

Esto se denomina 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 aspectos principales:

- Asegurar que la transferencia internacional de datos personales se realiza de acuerdo con la legislación nacional e internacional aplicable. La base legal 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 tales 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 seudonimizado para vincular los datos a nivel individual con la identidad de los interesados.

- 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 que incluyan datos de interesados de otros países (por ejemplo, en encuestas online dirigidas a interesados residentes en un país distinto del país en el que el investigador está gestionando el estudio). La legislación aplicable sobre privacidad será normalmente la del país donde el investigador esté basado. Sin embargo, el investigador también debe asegurarse de 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 para la captación del panel.

5.6 Externalización y subcontratación

18. *¿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.

19. *¿Se cuenta con un acuerdo (contrato) con todos los subcontratistas empleados?*

Debe existir un acuerdo con cualquier subcontratista involucrado. El contrato debe contemplar los términos contractuales del trabajo encargado (incluyendo una descripción de las tareas, plazos, seguros, etc.) así como:

• requisitos de protección de datos; y
• requisitos de seguridad de la información.

5.7 Política de privacidad

20. *¿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 un aviso de privacidad que esté fácilmente disponible para los interesados. Aunque el contenido y detalle requerido varía de un país a otro, el investigador siempre debe identificarse claramente a los interesados y asegurarse de que se explica: la finalidad 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, fáciles 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.

21. ¿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 personales quedan claros para los interesados. Esto incluye la identificación del responsable del tratamiento y si se emplea a algún encargado del tratamiento externo. Los interesados 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 ciego en las que se utilizan muestras proporcionadas por el cliente, los participantes deberían ser informados al principio de la entrevista 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 interesados el derecho de saber de quién ha obtenido el investigador sus datos personales, el investigador debe estar preparado para identificar el nombre del cliente en cualquier momento a solicitud de los participantes.

22. ¿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 interesado sobre dónde pueden estar situados sus datos.

6 CUESTIONES ESPECIALES

6.1 Recogida de datos de niños, personas jóvenes y otras personas vulnerables

El investigador debe obtener el consentimiento del padre/madre o tutor legal antes de recoger datos personales de cualquier interesado al que se le haya asignado un tutor legal. Cuando se solicite el consentimiento, el investigador debe suministrar suficiente información sobre la naturaleza del proyecto de investigación de forma que permita a padre/madre o tutor legal tomar una decisión informada sobre la participación del interesado. Esto incluye:

- El nombre y los datos de contacto del investigador u organización que está llevando a cabo la investigación;
- La naturaleza de los datos a recoger del interesado;
- Una explicación de cómo se usarán y protegerán los datos;

- Una explicación de los motivos por los que se ha solicitado la participación del interesado y las ventajas probables o los posibles impactos;
- Una descripción del procedimiento para otorgar y verificar el consentimiento; y
- La solicitud de los datos de contacto (dirección o teléfono) del padre/madre o tutor legal para verificar el consentimiento.

El investigador también debería registrar la identidad del tutor y su relación con el interesado.

Actualmente no existe una definición común internacional de niño o persona joven. Incluso dentro de un mismo país la definición puede variar. Establecer una definición alternativa basada en características distintas a la edad (por ejemplo, capacidades cognitivas) para aplicarlo en un entorno de investigación es difícil, si no imposible. Por lo tanto, el investigador deberá apoyarse en cualquier definición relevante definida por la legislación local, por los códigos de conducta y por las normas culturales. En ausencia de directrices claras, ESOMAR y GRBN recomiendan definir niño como la persona menor de 12 años, y persona joven como la persona entre 13 y 17 años. Para más detalle, consulte la Guía ESOMAR, para entrevistas a niños y jóvenes.

6.2 Investigación business-to-business

Un número considerable de proyectos de investigación incluyen 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 personales. 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 de cliente misterioso (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 interesados 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 por observación pueden implicar fotografiar, filmar o grabar en lugares públicos de forma que afecta a personas que no han sido captadas como interesados. En tales casos, 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 violaciones de seguridad y cuando 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 interesados afectados.

Por lo tanto, el investigador debería implementar controles de compensación para protegerse contra tales riesgos. Por ejemplo, debería encriptar los datos personales en tránsito (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 se almacenan los datos personales 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 específicos en el país 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 seudonimizados

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 el borrado o modificación de datos de identificación personal resultando en datos que no identifiquen individuos. Algunos ejemplos incluyen: difuminar las imágenes para disfrazar las caras o entregar los resultados como agregación estadística para asegurar que no se pueda identificar a un individuo en particular.

Seudonimizar 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/seudonimización 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
Esquema de Privacy Shield
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, Gerente, Global Privacy - Program, Policy & Governance, American Express
- Jayne Van Souwe, Director, Wallis Consulting Group