Red de Vínculos Familiares del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja

Código de Conducta sobre protección de datos

Versión 1.0

Noviembre de 2015

Prólogo

El presente Código de Conducta (en adelante, el Código) fue redactado por un grupo de trabajo compuesto por representantes de la Cruz Roja Austríaca (Claire Schocher-Döring), la Cruz Roja de Bélgica (Flandes) (Axel Vande Veegaete, Nadia Terweduwe), la Cruz Roja Británica (Mark Baynham, Emily Knox), la Cruz Roja Alemana (Jutta Hermanns), la Oficina de la Cruz Roja para la Unión Europea (Olivier Jenard), el Comité Internacional de la Cruz Roja (Romain Bircher, Massimo Marelli, Katja Gysin) y la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (Christopher Rassi) (Grupo de Trabajo). Varios representantes adicionales de esas instituciones también participaron en la redacción, los debates y las reuniones, e hicieron aportes importantes. El Grupo de Trabajo comenzó a debatir este proyecto a finales de 2013 y ha mantenido varias reuniones de trabajo en Mechelen (abril de 2014), Bruselas (julio de 2014), Viena (septiembre de 2014), Sofía (noviembre de 2014) y Londres (enero de 2015), así como múltiples teleconferencias e intercambios de mensajes por correo electrónico. El Grupo de Trabajo adoptó el Código por consenso y ha incorporado los comentarios recibidos de numerosas Sociedades Nacionales.

Se consideró necesario el Código de Conducta debido a (1) los numerosos actores del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (el Movimiento) que operan en la Red de Vínculos Familiares y la necesidad de transferir datos en el seno del Movimiento y a otros actores, y (2) el entorno regulatorio cambiante en Europa y en todo el mundo en lo que respecta a la legislación y las normas de protección de datos. El Código establece los principios, compromisos y procedimientos mínimos que deben cumplir los miembros del Movimiento al procesar datos dentro de la Red de Vínculos Familiares. El Código se propone cumplir las normas más estrictas de protección de datos, especialmente la legislación de la Unión Europea sobre esta materia. Los usuarios de este Código deben asegurarse también de cumplir su propia legislación nacional. El Código es un documento de referencia integrado en el conjunto principal de materiales del Movimiento para dar orientación sobre Restablecimiento del contacto entre familiares (RCF). Cada miembro del Movimiento deberá adoptarlo e incorporarlo en sus propios procedimientos estándar.

Este Código brindará una única herramienta para uso de todos los miembros del Movimiento en relación con la protección de los derechos y las libertades fundamentales de las personas, en particular el derecho a la privacidad y a la protección de datos personales, que se ven afectados por las actividades de RCF. La intención es que el Código dé confianza tanto a las personas como a los entes reguladores en relación con el trabajo del Movimiento, y también a los miembros del Movimiento que necesiten transferirse datos unos a otros en los casos de RCF.

Índice

PÁGINA DE DEFINICIONES

Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (el Movimiento)

El Movimiento es un movimiento humanitario mundial cuya misión es "prevenir y aliviar, en todas las circunstancias, los sufrimientos humanos; proteger la vida y la salud y hacer respetar a la persona humana, en particular en tiempo de conflicto armado y en otras situaciones de urgencia; tratar de prevenir las enfermedades y promover la salud y el bienestar social; fomentar el trabajo voluntario y la disponibilidad de los miembros del Movimiento, así como un sentimiento universal de solidaridad para con todos los que tengan necesidad de su protección y de su asistencia".

El Movimiento se compone del Comité Internacional de la Cruz Roja (CICR), las Sociedades Nacionales de la Cruz Roja y de la Media Luna Roja (las Sociedades Nacionales) y la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja (FICR).

Agencia Central de Búsquedas (ACB)

La Agencia Central de Búsquedas es un servicio permanente del CICR, de acuerdo con las disposiciones de los cuatro Convenios de Ginebra y sus Protocolos adicionales y con los Estatutos del Movimiento. La ACB, en colaboración con otros componentes del Movimiento, lleva a cabo actividades de Restablecimiento del contacto entre familiares (RCF) en conflictos armados y otras situaciones de violencia, catástrofes y otras circunstancias que requieran una respuesta humanitaria. Según el Acuerdo de Sevilla de 1997, sus Medidas complementarias de 2005 y la Estrategia de RCF del Movimiento para el período 2008-2018, la ACB tiene la función directiva, dentro del Movimiento, en todo lo relativo a RCF; coordina las operaciones y actúa como asesor técnico de las Sociedades Nacionales.

Controlador de datos

El término controlador de datos hace referencia a cualquier componente del Movimiento que, solo o en conjunto con otros, establece los fines y los medios para el procesamiento de datos personales.

Procesador de datos

El término procesador de datos hace referencia a una persona, autoridad pública, agencia u otra entidad que procesa datos personales en nombre de un controlador de datos.

Referente de protección de los datos de RCF

El término referente de protección de los datos de RCF hace referencia a una persona o unidad a la que se asigna la responsabilidad de garantizar el cumplimiento del Código de Conducta.

Titular de los datos

El término titular de los datos hace referencia a una persona física (es decir, un individuo) que se puede identificar directa o indirectamente, en particular al hacer referencia a sus datos personales.

Para establecer si una persona es identificable, es necesario tener en cuenta todos los medios que pueda utilizar con una probabilidad razonable el controlador o cualquier individuo para identificar directa o indirectamente a esa persona. Para establecer si ciertos medios pueden utilizarse con una probabilidad razonable para identificar a una persona, es necesario tener en cuenta todos los factores objetivos, como el costo de la identificación y la cantidad de tiempo que requiere, con consideración tanto de la tecnología disponible en el momento del procesamiento como del desarrollo tecnológico. Por ello, los datos personales no incluyen información anónima no relacionada con una persona física que se identifique o resulte identificable ni datos que se hayan anonimizado de tal manera que no sea posible identificar al titular de los mismos. Este Código no tiene que ver con el procesamiento de ese tipo de información anónima, entre otras cosas con fines estadísticos y de investigación.

Al utilizar servicios en línea, puede asociarse a las personas con los identificadores en línea que facilitan sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de IP o los identificadores de cookies. Es posible que queden rastros que, al combinarse con identificadores únicos y con otros datos recibidos por los servidores, puedan utilizarse para crear perfiles de las personas en cuestión e identificarlas. Números, datos de ubicación, identificadores en línea (p. ej., direcciones IP o identificadores de cookies) u otros factores por sí mismos no deben considerarse datos personales si no identifican ni hacen identificable a una persona.

Familiares

Se considera familiares por lo menos a las siguientes personas:

- hijos nacidos dentro y fuera del matrimonio, hijos adoptivos e hijastros;
- parejas, tanto si están casadas como si no;
- padres, incluidos suegros, suegras y padres adoptivos;
- hermanos y hermanas nacidos de los mismos padres o de padres distintos o adoptivos;
- familiares cercanos[1].

La definición que puede hallarse en la legislación nacional también debería tenerse en cuenta.

1 En muchos contextos socioculturales, la familia puede incluir a todas aquellas personas que viven bajo el mismo techo o mantienen una relación estrecha entre ellas. Por ello, el concepto de familia debe entenderse según las prácticas y el reconocimiento de cada sociedad.

Menores

Todos los seres humanos menores de 18 años de edad, a menos que obtengan la mayoría de edad antes según la legislación aplicable al niño.

Otras personas

Además de la persona que solicita la búsqueda y de la persona buscada, las actividades de RCF pueden involucrar a otros individuos, como otros familiares, testigos, vecinos, líderes comunitarios, otras personas buscadas, etc.

Datos personales

El término datos personales hace referencia a cualquier información relativa a una persona física identificada o identificable. Una persona física identificable es una que puede identificarse, directa o indirectamente, en especial al hacer referencia a un identificador, como un nombre, un material audiovisual, un número, datos de ubicación, un identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona.

Los datos personales no incluyen información anónima, es decir, información: (a) no relacionada con una persona física identificada o identificable; o (b) que se haya anonimizado de tal manera que no sea posible identificar al titular de los datos.

Violación de los datos personales

Por violación de los datos personales se entiende una violación de la seguridad que implica la destrucción, pérdida, alteración o divulgación no autorizada de datos personales transmitidos, almacenados o procesados de alguna otra forma, ya sea potencial o de hecho y se produzca por accidente o de una manera ilegal.

Proceso/Procesamiento/Procesado

Proceso/Procesamiento/Procesado hace referencia a cualquier operación o conjunto de operaciones que se hagan con datos personales o conjuntos de datos personales, tanto si se hacen con medios automatizados o no, como su obtención, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión del tipo que sea o eliminación. Una transferencia de datos dentro o fuera del Movimiento constituye una operación de procesamiento.

Hitos de procesamiento

Los hitos de procesamiento son los pasos clave del procedimiento. Los controladores de datos deben

documentar esos hitos, que incluyen:

- fecha y fuente de la obtención de datos;
- si la base legal del procesamiento es el consentimiento, cualquier limitación del consentimiento que haya expresado el titular de los datos;
- fecha, tipo y resultado de la solicitud del titular de los datos para ejercer sus derechos como tal;
- fecha y destinatario de cualquier transferencia de datos;
- fecha y formato de publicación;
- Evaluación del Impacto de la Protección de Datos (DPIA, por sus siglas en inglés), si se lleva a cabo;
- cierre del expediente;
- archivo, si corresponde.

Destinatario

El término destinatario hace referencia a una persona, autoridad pública, agencia u otra entidad más allá del titular de los datos, el controlador de datos o el procesador de datos a la que se divulguen los datos personales.

Actividades de Restablecimiento del contacto entre familiares y actividades relacionadas con Restablecimiento del contacto entre familiares

Restablecimiento del contacto entre familiares (RCF) es un término genérico que describe un conjunto de actividades destinadas a evitar la separación entre familiares, a los que ayuda a restablecer y mantener el contacto, así como actividades destinadas a aclarar el destino y el paradero de las personas desaparecidas.

Estas actividades pueden vincularse con otros servicios de apoyo, como la provisión de asistencia psicológica y psicosocial, legal, administrativa y material a familias y personas afectadas, así como con programas de reubicación y reintegración y servicios de bienestar social (para más detalles, v. el Anexo 1).

Servicios de RCF

Las Sociedades Nacionales y las delegaciones del CICR en todo el mundo tienen en sus estructuras personal especializado que desarrolla e implementa actividades de RCF y actividades relacionadas con RCF.

La Red de Vínculos Familiares

Cuando las familias se separan y hay personas que desaparecen por conflictos armados, otras situaciones de violencia, catástrofes, migraciones u otras crisis humanitarias, debe hacerse todo lo

posible para averiguar qué les ha ocurrido y su paradero, restablecer el contacto entre ellas y, si corresponde, reunirlas.

Los servicios de RCF de las Sociedades Nacionales y el CICR forman una única red mundial denominada **"Red de Vínculos Familiares"**. La ACB actúa como asesora técnica y coordinadora de esta Red de Vínculos Familiares. La fuerza de esta red humanitaria es su capacidad mundial de movilizar personal y voluntarios y de trabajar, conforme a una metodología y principios comunes y de una manera transfronteriza, en zonas afectadas por conflictos armados, otras situaciones de violencia, catástrofes, migraciones y otras crisis humanitarias.

En el sitio web sobre Vínculos Familiares: http://familylinks.icrc.org, se ofrece más información sobre la Red de Vínculos Familiares.

Persona vulnerable

En el contexto de este Código, una persona vulnerable hace referencia a cualquier individuo con una capacidad reducida de expresar de forma libre, específica y fundamentada sus propios deseos, por (i) el impacto emocional y psicológico de la separación familiar y las condiciones humanitarias que afectan a esa persona o por (ii) la complejidad del procesamiento necesario, que le dificulta la tarea de apreciar los riesgos y oportunidades, o una combinación de ambos factores.

1. Introducción

1.1 Propósito de este Código de Conducta

Este Código establece los principios, compromisos y procedimientos mínimos que el personal de RCF del CICR, las Sociedades Nacionales y la Federación Internacional debe cumplir al procesar datos en el marco de las actividades de RCF, para: (1) cumplir las normas y la legislación de protección de datos correspondientes; (2) permitir el flujo de datos personales sin obstáculos que requieren las actividades de RCF, y (3) proteger los derechos y las libertades fundamentales de los solicitantes, las personas buscadas y otros individuos, como testigos u otros familiares, relacionados con las actividades de RCF según el derecho internacional humanitario (DIH), el derecho internacional de los derechos humanos y otras normas internacionales, en particular el derecho a la privacidad y a la protección de los datos personales.

1.2 Alcance de este Código de Conducta

1.2.1 Restablecimiento del contacto entre familiares

Este Código es aplicable a las actividades de RCF y a las actividades relacionadas con RCF de los controladores de datos (v. Anexo 1).

1.2.2 Datos personales

Este Código es aplicable al procesamiento de datos personales (incluidos datos relativos a personas fallecidas) por parte de los controladores de datos, respetando a los solicitantes, las personas buscadas y otros individuos relacionados con las actividades de RCF.

1.3 La Red de Vínculos Familiares

Los Convenios de Ginebra de 1949, sus Protocolos adicionales de 1977, los Estatutos del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (los Estatutos del Movimiento), resoluciones adoptadas por el Consejo de Delegados y resoluciones de la Conferencia Internacional de la Cruz Roja y de la Media Luna Roja encomiendan a los controladores de datos el cometido de llevar a cabo actividades de RCF.

Las Sociedades Nacionales ejecutan ese cometido como auxiliares de sus autoridades públicas respectivas en el ámbito humanitario y desempeñan una función única en materia de RCF en todo el mundo. Organizan, en coordinación con las autoridades públicas, distintos servicios para ayudar a las víctimas de conflictos armados, desastres naturales y otras emergencias en las cuales se necesita ayuda.

1.4 Principios y directrices del Movimiento

1.4.1 Principios Fundamentales

Los controladores de datos llevan a cabo sus actividades según los Principios Fundamentales que guían al Movimiento: humanidad, imparcialidad, neutralidad, independencia, servicio voluntario, unidad y universalidad. Cualquier procesamiento de datos personales que lleven a cabo los servicios de RCF de los controladores de datos debe ser compatible con estos principios.

1.4.2 No causar daños

Los servicios de RCF de los controladores de datos hacen todo lo posible por evitar causar daños a personas en el procesamiento de los datos personales.

1.4.3 Confidencialidad o normas para la divulgación de información

Cuando los titulares de los datos transmitan información con los controladores de datos de manera confidencial, los controladores de datos deberán respetar y garantizar la protección de esa información.

Los controladores de datos deben cumplir todas las obligaciones legales nacionales, regionales e internacionales que correspondan, con las restricciones que se resumen en esta Sección 1.4. Al establecer la aplicabilidad de esas obligaciones, deberá hacerse referencia a: (1) cualquier privilegio o inmunidad o exención de obligaciones con los que cuenten los controladores de datos en el país o la región en cuestión; y (2) cualquier protección legal derivada del derecho internacional, incluido el DIH, y del cometido asignado por los Estatutos del Movimiento.

1.4.4 Directrices operacionales vigentes

El procesamiento de datos personales se lleva a cabo según las directrices de la Red de Vínculos Familiares, como "El restablecimiento del contacto entre familiares. Guía para uso de las Sociedades Nacionales de la Cruz Roja y de la Media Luna Roja"[2], "Evaluación de las necesidades en materia de restablecimiento del contacto entre familiares manual para las Sociedades Nacionales y el CICR", "El restablecimiento del contacto entre familiares en casos de catástrofe. Manual para el terreno" y "Directrices sobre los servicios de restablecimiento del contacto entre familiares en favor de las personas separadas como consecuencia de la migración"[3], y la "Normativa profesional relativa a la labor de protección llevada a cabo por los agentes humanitarios y los defensores de los derechos humanos en los conflictos armados y otras situaciones de violencia[4].

[2] En revisión.

[3] Pueden encontrarse documentos de orientación pertinentes en la Extranet de RCF (en construcción).

[4] https://www.icrc.org/spa/resources/documents/publication/p0999.htm

2. Principios básicos de procesamiento y compromisos del controlador de datos

2.1 El fin que se especifica

En el momento de la obtención de datos, el controlador de datos establecerá y dejará claros los fines específicos, explícitos y legítimos con los que se procesan los datos.

El procesamiento de datos se realiza principalmente con el fin humanitario de restablecer el contacto entre familiares cuando se refiere a personas separadas como consecuencia de conflictos armados, otras situaciones de violencia, catástrofes, migraciones u otras situaciones que requieran una respuesta humanitaria.

Se pueden procesar los datos con fines distintos de los que se especificaron inicialmente en el momento de su obtención, siempre que ese procesamiento adicional sea necesario con un fin humanitario compatible con ese, como las actividades relacionadas con RCF, y que en todo momento cumpla todas las leyes pertinentes de protección de datos (para más información, v. Anexo 1).

2.2 Procesamiento legal y justo

El procesamiento de datos personales por parte del controlador de datos debe basarse en uno o varios de los siguientes aspectos:

- consentimiento del titular de los datos;
- interés vital del titular de los datos o de otras personas;
- interés público;
- interés legítimo de los controladores de datos;
- cumplimiento de una obligación legal.

2.2.1 Consentimiento del titular de los datos

El consentimiento como opción preferencial: el consentimiento del titular de los datos es la base de preferencia para el procesamiento de datos personales. El consentimiento se debe otorgar sin ambigüedad por cualquier método adecuado que permita indicar libremente, con fundamento y de manera específica, los deseos del titular de los datos, mediante una declaración escrita, oral o de otro tipo o mediante una acción afirmativa clara por parte del titular de los datos que establezca que acepta que se procesen sus datos personales. Ese consentimiento cubre todas las actividades de procesamiento que se lleven a cabo con el mismo fin. El titular de los datos debería recibir explicaciones formuladas en un lenguaje sencillo sobre los siguientes aspectos:

- la identidad y los datos de contacto del controlador de datos;
- el fin específico del procesamiento de sus datos personales, con una explicación de los riesgos y beneficios potenciales que implica;

- el hecho de que el controlador de datos puede procesar sus datos personales con fines distintos de los que se especifican inicialmente en el momento de su obtención, si hacerlo es compatible con el fin específico que se mencionó anteriormente;
- las circunstancias en las que tal vez no sea posible tratar de manera confidencial los datos personales de esa persona;
- el derecho del titular de los datos a acceder a sus datos personales, corregirlos y eliminarlos y a objetar más tarde al procesamiento de esos datos, y sus limitaciones;
- una indicación de las medidas de seguridad que aplica el controlador de datos con respecto al procesamiento de los datos;
- que el controlador de datos puede necesitar transferir datos a otro país;
- una indicación de la política del controlador de datos sobre la retención de registros (durante cuánto tiempo se conservan los registros y las medidas que se adoptan para garantizar que sean correctos y estén actualizados);
- si sus datos personales podrían compartirse con otras instituciones (incluidos otros componentes del Movimiento) o con las autoridades del Estado en el país donde se obtuvieron los datos, o si podrían hacerse públicos, y si el titular aprueba el uso de sus datos personales tal como se explica.

Se puede dar un consentimiento con limitaciones. Se registran los detalles del consentimiento que se otorga, el nivel de confidencialidad necesario y cualquier limitación aplicable, que acompañan a esos datos personales durante todo su procesamiento.

Alternativas al consentimiento: particularmente cuando no se puede obtener el consentimiento de una manera razonable, se procesan los datos personales sobre alguna de las bases siguientes:

- interés vital;
- interés público;
- interés legítimo del controlador de datos; o
- cumplimiento de una obligación legal.

En esos casos, el controlador de datos se asegurará, si es posible, de que el titular de los datos sea consciente de ese procesamiento y esté en condiciones de objetar ese procesamiento si lo desea.

2.2.2 Interés vital

Se presume que el procesamiento de datos personales por parte de los servicios de RCF del controlador de datos, para restablecer el contacto entre familiares, averiguar lo sucedido y el

paradero de las personas desaparecidas y brindar asistencia de emergencia y protección, defiende el interés vital del titular de los datos o de otras personas en ciertas circunstancias, especialmente:

- cuando al titular de los datos lo busquen sus familiares, cuando se haya denunciado su desaparición, cuando se lo haya privado de su libertad o sometido a abusos, o cuando posiblemente esté muerto;
- cuando el titular de los datos sea particularmente vulnerable o no esté en condiciones de otorgar un consentimiento libre y fundamentado ni de calcular o entender los riesgos y los beneficios del procesamiento de sus datos personales.

2.2.3 Interés público

Las actividades de RCF y las actividades relacionadas con RCF del controlador de datos son de interés público, ya que son exclusivamente humanitarias, según se resume en la Sección 1.3 anterior. (Para consultar ejemplos, v. Anexo 2)

2.2.4 Interés legítimo

También se procesan los datos personales en circunstancias en las que el controlador de datos tiene un interés legítimo por hacerlo, siempre y cuando ni los intereses ni los derechos y las libertades fundamentales del titular de los datos invaliden ese interés legítimo (para consultar ejemplos, v. Anexo 3).

2.2.5 Cumplimiento de una obligación legal

El controlador de datos también procesará los datos personales en cumplimiento de cualquier obligación legal correspondiente, como el respeto de la legislación nacional y regional y las órdenes de los tribunales, sujeto a los Principios Fundamentales del Movimiento. Las obligaciones legales pueden según la situación y el país de que se trate.

2.3 Compromisos de procesamiento

2.3.1 Responsabilidad y rendición de cuentas

El controlador de datos deberá asegurarse de que cualquier persona o entidad que tenga acceso a los datos personales y siga sus instrucciones (por lo tanto, sea procesadora) solo procese esos datos en cumplimiento de este Código. El controlador de datos deberá asegurarse también de que las responsabilidades de cada una de las entidades que participen en el procesamiento de datos personales se asignen claramente y se reflejen en cláusulas contractuales adecuadas. Consulte la Sección 4 a continuación para más información sobre la transferencia de datos a terceros cuando se contemple la posibilidad de que el tercero destinatario no vaya a procesar los datos exclusivamente según las instrucciones del controlador de datos.

2.3.2 Procesamiento de datos adecuados, pertinentes y actualizados

Datos adecuados: los datos personales procesados por los servicios de RCF del controlador de datos se revisarán para garantizar que sean adecuados y pertinentes y que no sean excesivos en relación con el fin para el cual se obtienen y procesan, excepto cuando se archiven.

Precisión de los datos: los datos personales deberán ser lo suficientemente precisos y completos y estar lo suficientemente actualizados para el fin con el cual se obtienen y procesan.

2.3.3 Protección intencional y por defecto

Se adoptarán medidas técnicas y organizativas adecuadas para cumplir los requisitos de este Código al diseñar sistemas de gestión de datos y establecer procedimientos para la obtención de datos personales.

2.3.4 Evaluación del Impacto de la Protección de Datos (DPIA, por sus siglas en inglés)

Cuando sea probable que el procesamiento presente riesgos específicos para los derechos y las libertades de los titulares de los datos, como las transferencias, la publicación y la divulgación de los datos, el controlador de datos llevará a cabo una DPIA antes de procesarlos, si es posible previa consulta con el titular de los datos y con otras partes interesadas, para establecer y evaluar en particular:

- los beneficios de procesar los datos;
- el origen, la naturaleza, la probabilidad y la gravedad de esos riesgos;
- las medidas adecuadas que se deben adoptar para demostrar que se minimizan los riesgos y que el procesamiento de esos datos personales cumple este Código y cualquier legislación correspondiente.

El resultado de una DPIA debería ser la minimización del riesgo de daños o de posibles violaciones de los derechos y libertades del titular de los datos. El controlador de datos documentará el resultado y las razones por las cuales se llegó a él. El controlador de datos también deberá garantizar que las medidas que se tomen como consecuencia de la DPIA se implementen adecuadamente y tengan los efectos deseados.

2.3.5 Documentación para el procesamiento de datos

El controlador de datos deberá garantizar que se mantengan registros electrónicos o en papel, en los que se establezcan: (i) bases de datos para el procesamiento de datos personales e (ii) hitos clave del procesamiento de datos. Esos hitos deberán registrarse en la base de datos o en el expediente individual del titular de los datos.

2.3.6 Retención de los datos

Los datos personales se archivarán o eliminarán según la política de retención de datos de los servicios de RCF del controlador de datos, cuando ya no se necesiten con el fin para el que se obtuvieron, para un procesamiento adicional o para su procesamiento sobre otra base legítima o legal (v. también Sección 3.3).

2.3.7 Seguridad de los datos

Siempre se adoptarán, en todo momento del procesamiento de los datos, medidas de seguridad técnicas, físicas y organizativas razonables para proteger los datos personales contra pérdidas, robos y accesos y divulgaciones no autorizados o ilegales. Solo se permitirá acceder a los datos personales al personal del controlador de datos que necesite ese acceso para realizar una tarea o proveer un servicio específico, con medidas de seguridad y restricciones de acceso (para más detalles, v. Anexo 4).

2.3.8 Violaciones de los datos personales

El controlador de datos deberá notificar al titular de los mismos cuando se produzca una violación de los datos en los casos en los que sea probable que afecte los derechos y las libertades de esa persona.

El objetivo de notificar al titular de los datos sobre violaciones de sus datos personales es minimizar los riesgos de que se produzcan efectos negativos para esa persona.

El controlador de datos puede decidir que no es necesario comunicar una violación de los datos personales al titular de los mismos si puede aplicarse alguno de los aspectos siguientes o varios:

- el controlador de datos ha implementado medidas de protección organizativas, tecnológicas o físicas adecuadas, y esas medidas se han aplicado a los datos afectados por la violación de los datos personales;
- el controlador de datos ha adoptado medidas posteriores que garantizan que ya no es probable que los derechos y libertades del titular de los datos se vean gravemente afectados;
- hacerlo supondría un esfuerzo desproporcionado, en particular por las condiciones logísticas o de seguridad imperantes o por el número de casos. En esas circunstancias, el controlador de datos se planteará, en cambio, si sería adecuado emitir una comunicación pública o tomar alguna medida similar para informar con la misma eficacia a los titulares de los datos;
- afectaría un interés público sustancial, incluida la viabilidad de las operaciones del controlador de datos;
- acercarse al titular de los datos podría poner en peligro a esa persona, dadas las circunstancias de seguridad imperantes.

3. Derechos de los titulares de los datos

3.1 Información y acceso

Al obtener datos personales, o lo antes posible después de hacerlo, el controlador de datos deberá brindar al titular, si las restricciones logísticas y de seguridad lo permiten, información sobre el procesamiento de esos datos, oralmente o por escrito, con los medios más adecuados para hacerlo

(para consultar una lista de la información que se debe brindar, v. el Anexo 5).

Los titulares de los datos tienen derecho a obtener, en cualquier momento que lo soliciten, una confirmación sobre si en ese momento se procesan datos personales sobre ellos. Cuando efectivamente se procesen en ese momento, tendrán derecho a obtener acceso a sus datos y a información sobre los fines de ese procesamiento, los destinatarios de esos datos personales y las medidas de seguridad adoptadas.

Si lo solicitan, se les deberá facilitar una copia de los documentos que contengan sus datos personales.

Esta sección no será aplicable cuando deba restringirse el acceso a los datos como consecuencia de:

- un interés público superior;
- los intereses de protección de los datos y los derechos y libertades de otras personas;
- que no se puedan modificar significativamente los documentos de que se trate.

El controlador de datos mantendrá un registro de las solicitudes de acceso y del resultado de cada una de ellas, incluidas las categorías de datos personales que se hayan revelado o las negativas de acceso a la información.

3.2 Divulgación a familiares o tutores

Se presume que una solicitud de divulgación de datos personales por parte de un familiar o tutor legal de un niño o de otro titular de datos que no pueda dar su consentimiento por incapacidad defiende los intereses de esa persona y debe, por lo tanto, otorgarse, salvo que haya razones suficientes para pensar lo contrario. Deberá consultarse siempre que sea posible a la persona afectada, para establecer si tiene alguna objeción a esa divulgación.

3.3 Rectificación y eliminación

Rectificación: el controlador de datos responderá a las solicitudes de rectificación de datos personales, en particular cuando los datos sean incorrectos o estén incompletos. El controlador de datos comunicará las rectificaciones realizadas a los destinatarios de esos datos personales, a menos que la rectificación no sea significativa o que esa comunicación requiera un esfuerzo desproporcionado.

Eliminación: el titular de los datos tiene derecho a que se eliminen sus datos personales de las bases de datos activas del controlador de datos en cualquiera de los casos siguientes:

- cuando ya no se necesiten para el fin con el cual se obtuvieron sus datos personales y no se necesiten para un procesamiento adicional;
- cuando el titular de los datos haya retirado su consentimiento del procesamiento y no haya ninguna otra base para el procesamiento de esos datos personales;

- cuando el titular de los datos objete de manera satisfactoria el procesamiento de sus datos personales;
- cuando el procesamiento de los datos personales del titular incumpla de alguna otra manera este código.

Sin embargo, se permite una retención continuada de los datos personales de ese titular cuando sea necesaria o esté justificada:

- con fines históricos, estadísticos y científicos, por ejemplo, para documentar las medidas adoptadas por un controlador de datos en cumplimiento del cometido encomendado por los Convenios de Ginebra de 1949, sus Protocolos adicionales de 1977 o los Estatutos del Movimiento;
- por razones de interés público en el ámbito de la salud pública;
- con vistas a la publicación por parte de cualquier persona de material periodístico, literario o artístico, en el ejercicio del derecho a la libertad de expresión y de información.

Además, se permitirá una retención continuada de los datos personales de un titular cuando la ley la requiera. Se notificará al titular de los datos la decisión adoptada en relación con su solicitud, que deberán documentar los controladores de datos.

El controlador de datos se reserva el derecho a rechazar una solicitud de rectificación o eliminación por parte del titular de los datos si considera que esa persona puede haber hecho esa solicitud bajo presión ilegítima o en el caso de que una eliminación pueda ser perjudicial para los intereses vitales del titular de los datos.

El controlador de datos comunicará la eliminación de datos personales a los destinatarios de esos datos y les pedirá que supriman cualquier enlace o copia de esos datos, a menos que los datos eliminados no sean significativos o que esa comunicación requiera un esfuerzo desproporcionado.

3.4 Objeción al procesamiento

El titular de los datos tiene derecho a objetar, con fundamentos razonables relativos a su situación particular, el procesamiento de sus datos personales basado en los intereses legítimos del controlador de datos o en el interés público. Cuando se acepte esa objeción, los datos personales respectivos dejarán de procesarse, a menos que el controlador de datos demuestre razones legítimas superiores para que continúe el procesamiento.

Cuando se acepte la objeción, el controlador de datos la comunicará a los destinatarios de los datos, a menos que hacerlo represente un esfuerzo desproporcionado.

3.5 Reparaciones

El titular de los datos deberá enviar su solicitud al controlador de datos, que deberá responderla en un

plazo razonable y, en todo caso, en el plazo que establezca la ley.

El personal que reciba una solicitud de un titular de datos deberá:

- acceder a la solicitud y notificar al solicitante cómo se ha cumplido o va a cumplirse;
- informar al titular de los datos que presenta la solicitud de por qué no puede cumplirse o no va a cumplirse;
- informar al titular de los datos de la posibilidad de presentar una queja al controlador de datos.

4. Disposiciones especiales sobre las transferencias de datos

4.1 Principios generales

4.1.1 Antecedentes

Las actividades de RCF y las actividades relacionadas con RCF suelen requerir la transferencia transfronteriza de datos personales entre controladores de datos.

Es posible que los servicios de RCF de un controlador de datos necesiten también transferir datos personales a entidades como organizaciones no gubernamentales (ONG), organizaciones internacionales, autoridades y otras terceras partes necesarias para la realización de actividades de RCF y actividades relacionadas con RCF.

Esas transferencias se realizan de acuerdo con las actividades de la Red de Vínculos Familiares, según se explica en la Sección 1.3; en ese sentido, se llevan a cabo por razones importantes basadas en el interés público y respetan los principios y las directrices del Movimiento que se abordan en la Sección 1.4.

Además, en la mayoría de los casos, esas transferencias se basan en el consentimiento o en la protección de los intereses vitales del titular de los datos o de otras personas.

4.1.2 Principios generales aplicables a las transferencias de datos

Una transferencia de datos dentro o fuera del Movimiento constituye una operación de procesamiento. Como tal, está sujeta a los Principios básicos que se establecen en el Capítulo 2 y en los Derechos de los titulares de los datos que se establecen en el Capítulo 3.

Sin embargo, las transferencias son una operación de procesamiento especialmente delicada. Por ello, algunos de los requisitos de procesamiento son particularmente importantes, como la DPIA, la información que se brinda al titular de los datos y la seguridad de los datos.

Tal como se establece en la Sección 3.1, la transferencia a todas las terceras partes razonablemente previsibles se debe prever antes de la obtención de los datos o en el momento de obtenerlos, y se debe tener siempre que sea posible el consentimiento del titular de los datos para la transferencia de estos.

No se deben transferir datos personales a personas ni instituciones a menos que hacerlo sea adecuado y que se adopten medidas de seguridad proporcionales, según la sensibilidad de los datos, la urgencia de la acción humanitaria y las restricciones logísticas y de seguridad, como detalla este Código.

4.1.3 Evaluación del Impacto de la Protección de Datos para las transferencias de datos

El requisito de llevar a cabo una DPIA es especialmente importante en el contexto de las transferencias de datos. Por ello, cuando sea probable que la transferencia de datos presente riesgos específicos para los derechos y las libertades de los titulares de los datos, el controlador de datos llevará a cabo una DPIA (v. Anexo 6 para más orientación) antes de realizar la transferencia, según se establece en la Sección 2.3.4 anterior.

4.1.4 Condiciones

Las transferencias de datos están sujetas a las siguientes condiciones, que son acumulativas:

- el procesamiento por parte del destinatario debe limitarse estrictamente a los fines específicos de las actividades de RCF y las actividades relacionadas con RCF y a fines compatibles son esos;
- la cantidad de datos personales y el tipo de estos debe limitarse estrictamente a las necesidades del destinatario para los fines específicos o para el procesamiento adicional previsto;
- la transferencia debe ser compatible con las expectativas razonables del titular de los datos.

4.1.5 Documentación de las transferencias de datos

El controlador de datos deberá asegurarse de que se mantengan registros electrónicos o en papel de las transferencias (v. también 2.3.5).

Los registros de las transferencias deberán incluir todos los aspectos siguientes:

- nombre del destinatario;
- fin que se especifica para la transferencia;
- fecha de la transferencia;
- descripción de las categorías de los datos personales transferidos;
- cualquier limitación del uso de datos que acepta el destinatario.

4.1.6 Acuerdos

Como se establece en la Sección 4.1.2, una transferencia de datos personales puede producirse si el controlador de datos está convencido de la existencia de medidas de seguridad adecuadas en relación con la protección de los datos personales por parte del destinatario. Pueden establecerse las medidas de seguridad adecuadas mediante acuerdos sobre el tratamiento de los datos personales a los que se llegue, siempre que sea posible, con terceras partes ajenas al Movimiento, en los casos en que se contemple la realización de transferencias periódicas.

Es posible que no sea adecuado transferir ciertas categorías de datos incluso cuando se llegue a acuerdos.

4.2 Métodos de transmisión

En caso de que se produzca una transferencia, se adoptarán medidas adecuadas para garantizar la seguridad de la transmisión de datos personales a terceras partes. El nivel de seguridad adoptado y el método de transmisión deberán ser proporcionales a la naturaleza y la sensibilidad de los datos personales y a los riesgos que resalte la DPIA.

5. Disposiciones especiales sobre la publicación de datos

5.1 Principios generales

La publicación de datos personales por parte del controlador de datos constituye una operación de procesamiento. Como tal, está sujeta a los Principios generales que se establecen en el Capítulo 2 y a los Derechos de los titulares de los datos que se establecen en el Capítulo 3. Sin embargo, la publicación es una operación de procesamiento especialmente delicada. Una vez que se publican los datos personales, el controlador de datos y el titular de los mismos pierden en gran medida la capacidad de controlar la manera en que se procesan. Por ello, deben seguirse también los principios adicionales que se establecen en este capítulo.

Los servicios de RCF del controlador de datos, sujetos a la DPIA y a las obligaciones legales correspondientes, pueden publicar datos personales para restablecer el contacto entre familiares separados por conflictos armados, otras situaciones de violencia, desastres naturales y migraciones. Esos datos pueden incluir nombres, fotos y estados (como sano y salvo, herido, fallecido, desaparecido, desplazado) y pueden publicarse en Internet, a través de los medios de comunicación, en afiches o con otras herramientas adecuadas.

Según la Sección 2.2.1, el consentimiento del titular de los datos es la base de preferencia para la publicación de datos personales.

5.2 Evaluación del Impacto de la Protección de Datos para la publicación de datos

El requisito de llevar a cabo una DPIA, que se establece en la Sección 2.3.4 anterior y en el Anexo 6, es especialmente importante en el contexto de la publicación de datos.

Además de los elementos que se establecen en la Sección 2.3.4 anterior sobre la “Evaluación del Impacto de la Protección de Datos”, la DPIA en el contexto de la publicación deberá tener en cuenta los siguientes elementos:

- la legislación y la normativa nacionales sobre protección de datos aplicables a la publicación de esos datos;
- la situación de seguridad, respeto de los derechos humanos y el DIH y la protección de los titulares de los datos en cada país en particular;
- si es suficiente con datos anónimos o agregados o es necesario publicar datos personales, si hay otra forma de proteger la identidad de los titulares de los datos que cumpla el fin específico de la publicación (esas formas adicionales pueden incluir, por ejemplo, no asociar una foto con nombres/rasgos distintivos/ubicaciones precisas);
- el método y las condiciones de publicación;
- la posibilidad de hacer cumplir el requisito de limitar el uso adicional por parte de terceras partes que quieran utilizar los datos publicados;
- la posibilidad de especificar el período durante el cual pueden estar publicados ciertos datos en un soporte de medios concreto y el método para su destrucción, una vez que se haya cumplido el fin que se especifica para su publicación;
- la utilidad y la pertinencia de las publicaciones, según se establece mediante evaluaciones periódicas del controlador de datos;
- en el contexto de la comunicación pública, la importancia de proteger de la curiosidad pública a las personas vulnerables.

Si el titular de los datos es una persona vulnerable, deberán tenerse en cuenta, cuando corresponda, consideraciones adicionales como medidas de protección suplementarias para proteger su confidencialidad y su anonimato. El principio rector de la protección de la víctima es “no causar daños” y actuar en defensa de los intereses de los titulares de datos que sean vulnerables.

5.3 Documentación de la publicación de datos

El controlador de datos deberá asegurarse de que se haga y mantenga un registro de publicaciones. Los registros de publicaciones de datos deberán incluir todos los aspectos siguientes:

- fecha de publicación;
- si es pertinente, fecha en que debe revisarse la base de esa publicación, según la DPIA;
- si es pertinente, fecha en la que los datos deben eliminarse de la publicación;
- descripción de las categorías de los datos personales publicados;
- cuando sea posible, detalles de los soportes de medios utilizados.

5.4 Datos que deben publicarse para RCF

Los datos que se pueden publicar deben definirse para cada contexto concreto, y es posible que haya orientación particular en relación con ciertas categorías específicas de titulares de datos. Según la DPIA, las medidas de mitigación específicas pueden incluir:

- que la publicación se limite a datos absolutamente necesarios para permitir al lector u

oyente identificar a las personas cuyos nombres o fotos se publican y restablecer el contacto;

- que las fotos de personas vulnerables no se publiquen en combinación con otros datos personales (p. ej., su nombre), y que nunca se publique la dirección de un menor.

5.5 Datos que deben publicarse para los archivos públicos

Los datos personales archivados pueden hacerse públicos en cumplimiento de la legislación correspondiente.

5.6 Datos que deben publicarse para la comunicación pública

Pueden publicarse datos personales con el fin de promocionar las actividades de RCF o de sensibilizar a la población sobre situaciones preocupantes, en cumplimiento de la legislación correspondiente. La comunicación pública también está vinculada con la libertad de información y de expresión y con la rendición de cuentas pública. Sin embargo, como en el caso de cualquier publicación, deberán respetarse los principios que se establecen en este Código y deberá realizarse una DPIA.

5.7 Derecho a retirar el consentimiento o a la eliminación de datos publicados

Cuando se realice una publicación basada en el consentimiento, el titular de los datos podrá retirar en cualquier momento su consentimiento para la publicación de materiales en los que se lo identifique. En esos casos, el controlador de datos tomará todas las medidas necesarias, con conciencia de las dificultades inherentes a la eliminación de documentos públicos (especialmente en Internet), para retirar los materiales publicados e impedir su publicación.

Cuando la publicación se base en un elemento que no sea el consentimiento, deberán seguirse los procedimientos que se establecen en la Sección 3.4, “Objeción al procesamiento”.

6. Aplicación del Código de Conducta

Un grupo de aplicación del Código de Conducta dará apoyo a la implementación de esté código a nivel global, al promover el aprendizaje y el desarrollo continuos.

Todos los controladores de datos deberán aplicar con eficacia el presente Código, sujeto a la legislación nacional, de la siguiente manera:

- el Código deberá reflejarse en las políticas, directrices y programas de RCF;
- el Código deberá formar parte de la la gestión de personal de RCF y de la capacitación de cada uno de los controladores de datos;
- deberá designarse un referente de protección de los datos de RCF, y deberán difundirse sus datos de contacto;
- participación en encuestas periódicas sobre la puesta en práctica de este Código;
- cooperación con el grupo de aplicación del Código;
- el seguimiento, que incluye autoseguimiento, diálogo, revisión por pares y otros tipos de revisión, se hará de forma voluntaria para garantizar una mejora y un aprendizaje organizativo continuos.

El grupo de aplicación del Código lo revisará y actualizará cuando sea necesario.

7. Referencias

7.1 Orientación e instrumentos jurídicos

- "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales" de la ONU, adoptados por la resolución 49/95 de la Asamblea General el 14 de diciembre de 1990
- Art. 17 del Pacto Internacional de Derechos Civiles y Políticos
- "Estándares internacionales sobre protección de datos personales y privacidad", adoptados por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, 5 de noviembre de 2009, http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf
- Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", 108, 28 de enero de 1981, BRON
- "Directiva 95/46/EC del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", 24 de octubre de 1995, *OJ* L 281 23 de noviembre de 1995, págs. 31-50
- Art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, 4 de noviembre de 1950
- Art. 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), 13 de diciembre de 2007, *OJ* C 236, 26 de noviembre de 2012, págs. 0001-0390
- Artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, *OJ* C 303/1, 14 de diciembre de 2007
- Organización para la Cooperación y el Desarrollo Económico (OCDE), "Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980" (actualizadas en 2013), oe.cd/privacy
- OCDE, "Directrices para la protección de los consumidores en el contexto del

comercio electrónico", 9 de diciembre de 1999, www.oecd.org/sti/consumer/34023811.pdf

- Marco de Privacidad de APEC, 2005, http://www.apec.org/Groups/Committee-on-Trade- and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- Estatutos del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, según fueron enmendados en 2006
- Resolución 4 del Consejo de Delegados sobre la estrategia de restablecimiento del contacto entre familiares del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja, 24 de noviembre de 2007
- Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Resolución sobre privacidad y acción internacional humanitaria, Ámsterdam, Países Bajos, 2015, https://icdppc.org/document-archive/adopted-resolutions/

7.2 Doctrina

- COMITÉ INTERNACIONAL DE LA CRUZ ROJA (CICR), *El restablecimiento del contacto entre familiares en casos de catástrofe. Manual para el terreno*, CICR, 2009.
- COMITÉ INTERNACIONAL DE LA CRUZ ROJA (CICR), *Evaluación de las necesidades en materia de restablecimiento del contacto entre familiares manual para las Sociedades Nnacionales y el CICR*, CICR, 2010.
- COMITÉ INTERNACIONAL DE LA CRUZ ROJA (CICR), *Directrices sobre los servicios de restablecimiento del contacto entre familiares en favor de las personas separadas como consecuencia de la migración*, CICR, 2010.
- COMITÉ INTERNACIONAL DE LA CRUZ ROJA (CICR), *Estrategia de restablecimiento del contacto entre familiares, con referencias legales*, Suiza, CICR, 2009.
- MORGAN, O., TIDBALL-BINZ, M., VAN ALPHEN, D. (eds.), *La gestión de cadáveres en situaciones de desastre: guía práctica para equipos de respuesta*, Washington, D.C., 2009.

ANEXOS

Anexo 1: Actividades de RCF y actividades relacionadas con RCF

Las actividades de RCF, según la situación y el contexto, pueden ser de distintos tipos:

- organización del intercambio de noticias familiares;
- búsqueda de personas;
- registro de datos de personas (niños o adultos) y seguimiento de sus casos para evitar su desaparición y permitir que se informe a sus familiares;
- reunión y repatriación de familiares,
- obtención, gestión y envío de información sobre los fallecidos;
- transmisión de documentos oficiales, como partidas de nacimiento, documentos de identidad o diversos certificados emitidos por las autoridades;
- emisión de certificados de detención de personas y documentos que den fe de otras situaciones que provocaron que se incluya a las personas en cuestión en un registro;
- emisión de documentos de viaje del CICR;
- seguimiento de la integración de las personas que se han reunido con sus familiares;
- promoción y apoyo del establecimiento de mecanismos para averiguar lo sucedido a personas dadas por desaparecidas y determinar su paradero.

V. también http://familylinks.icrc.org

Actividades relacionadas con RCF: otros servicios humanitarios relacionados con las actividades de RCF, que lleva a cabo el personal de RCF:

- apoyo material, psicológico y psicosocial a los familiares de los desaparecidos y a otras personas afectadas por conflictos armados, otras situaciones de violencia, catástrofes, migraciones y otras crisis humanitarias;
- apoyo a las autoridades pertinentes para la gestión y la identificación forense de restos humanos;
- (derivación a) servicios de bienestar social;
- servicios de restablecimiento o (derivación a) servicios de apoyo para la reinserción de grupos vulnerables;
- archivo (memoria individual o familiar; memoria de la humanidad; necesidades administrativas individuales, rendición de cuentas de las partes, investigación histórica, estadística y médica);
- comunicación pública para la promoción de las actividades de RCF y las actividades

relacionadas con RCF

Anexo 2: Interés público

A continuación, se ofrecen algunos ejemplos de interés público.

- Cuando se trata de crisis a gran escala que requiere acción inmediata, lo cual impide operar sobre la base del consentimiento, y en las que no es posible establecer claramente si se puede aplicar la base del interés vital legítimo. Un ejemplo pueden ser los numerosos migrantes rescatados en el mar.
- Cuando las operaciones de procesamiento son muy complejas y requieren de tecnologías complejas y la participación de procesadores externos, lo cual hace difícil que los titulares de los datos puedan apreciar plenamente los riesgos y los beneficios de las medidas de procesamiento necesarias y tomar una decisión bien fundamentada sobre esa base. Cuando no se puedan establecer los intereses vitales del titular de los datos o de otra persona (ya sea por la falta de urgencia o porque se busca al titular de los datos), el procesamiento puede producirse sobre la base del cometido encomendado al controlador de datos, siempre y cuando se lleve a cabo una DPIA satisfactoria.
- En distribuciones de asistencia, en las que a veces no se puede obtener el consentimiento de todos los beneficiarios posibles y en las que no hay una probabilidad razonable de que estén en juego la vida y la integridad del titular de los datos ni de otras personas (en cuyo caso es posible que el “interés vital” sea la base de procesamiento más adecuada).
- Cuando se procesen datos personales cuyo titular esté detenido. Eso puede suceder, por ejemplo, al procesar datos personales relativos a personas privadas de libertad en el contexto de un conflicto armado u otra situación de violencia, cuando el CICR (o la Sociedad Nacional) no haya podido aún visitar al titular de los datos que está privado de libertad y obtener su consentimiento y cuando las condiciones de detención imperantes podrían refutar la presunción para la aplicación de la base del “interés vital”.

Anexo 3: Interés legítimo

A continuación, algunos ejemplos de interés legítimo.

- El procesamiento es necesario para el cumplimiento eficaz del cometido del controlador de datos, de conformidad con los Principios Fundamentales (en particular, los de neutralidad, independencia e imparcialidad) y sus modalidades de trabajo habituales.
- Se procesan datos en la medida estrictamente necesaria a los efectos de garantizar la seguridad de los sistemas de información y de la propia información, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, las autoridades públicas, los equipos de respuesta ante emergencias informáticas (CERT, por sus siglas en inglés), los equipos de respuesta ante incidencias de seguridad (CSIRT, por sus siglas en inglés), los proveedores de redes y servicios de comunicación electrónica y los proveedores de tecnologías y servicios de seguridad. Eso podría incluir, por ejemplo, impedir el acceso no autorizado a redes de comunicación electrónica, así como la distribución de códigos maliciosos y la perpetración de ataques de denegación de servicio, para evitar daños a los sistemas informáticos y de comunicación electrónica.
- El procesamiento de datos personales en la medida estrictamente necesaria a los efectos de prevenir, evidenciar e impedir un fraude o un robo.
- El procesamiento de datos personales a los efectos de anonimizar o pseudonimizar los datos personales.
- Cuando sea necesario para establecer, ejercer o defender demandas legales, más allá de si se trata de un procedimiento judicial, administrativo o uno que se soluciona sin acudir a los tribunales; el *marketing* directo y la comunicación pública.

Anexo 4: Seguridad de los datos

Los datos personales se deben procesar de tal manera que se garantice la seguridad adecuada de esos datos, incluida la prevención de accesos o usos no autorizados de los datos y de los equipos que se emplean para su procesamiento.

Cualquier persona que actúe bajo la autoridad del controlador de datos y que tenga acceso a datos personales deberá procesarlos solamente en cumplimiento del Código de Conducta y de la Política de Seguridad de los Datos aplicable, como se explica más adelante en este Anexo.

Para preservar la seguridad e impedir procesamientos que violen este Código, el controlador de datos deberá evaluar los riesgos específicos inherentes al procesamiento e implementar medidas para mitigar esos riesgos. Esas medidas deberán garantizar un nivel de seguridad adecuado (que tenga en cuenta la tecnología disponible, la seguridad imperante y las condiciones logísticas, y los costos de implementarlas) en relación con los riesgos y la naturaleza de los datos personales que se deben proteger. Esto incluye medidas que impliquen:

- capacitación;
- gestión de derechos de acceso a bases de datos con datos personales;
- seguridad física de bases de datos;
- seguridad de IT;
- cláusulas de discreción;
- métodos de destrucción de datos personales;
- cualquier otra medida adecuada.

El objetivo de estas medidas es garantizar la seguridad de los datos personales en los planos tanto técnico como organizativo, y su protección con medidas razonables y adecuadas frente a modificaciones, copias y manipulaciones no autorizadas, destrucción ilegal, pérdida accidental y divulgación o transferencia indebida.

Las medidas de seguridad de los datos variarán según los siguientes factores, entre otros:

- el tipo de operación;
- la naturaleza y la sensibilidad de los datos personales de que se trate;
- la forma o el formato de almacenamiento;
- el entorno o el lugar donde se encuentran los datos personales específicos;
- las condiciones logísticas y de seguridad imperantes.

Las medidas de seguridad de los datos deberán revisarse periódicamente y mejorarse para garantizar un nivel de protección de los datos que sea adecuado para el grado de sensibilidad que se aplica a los datos personales.

El controlador de datos será responsable de coordinar los siguientes elementos:

- el establecimiento de un sistema de gestión de la seguridad de la información. Para eso, deberá establecer y actualizar periódicamente una Política de Seguridad de los Datos basada en normas internacionalmente aceptadas y en una evaluación de riesgos, que deberá consistir por ejemplo en pautas de seguridad física, una política de seguridad de IT, pautas de seguridad del correo electrónico, pautas de uso de los equipos de IT, tipología de la gestión de la información, un plan de contingencia y pautas para la destrucción de documentos;
- el desarrollo de una infraestructura de comunicación y de bases de datos para preservar la integridad y la seguridad de los datos, en cumplimiento de la política de seguridad establecida;
- tomar, de acuerdo con el presente Código, todas las medidas adecuadas para proteger la seguridad de los datos procesados en el sistema de información del controlador de datos.

1. Derechos de acceso a bases de datos

El controlador es responsable de:

- el otorgamiento de acceso a las bases de datos que contengan datos personales;
- la seguridad de las instalaciones que permiten acceder a ese sistema al personal autorizado para hacerlo;
- el cumplimiento de las normas de seguridad a las que hace referencia este Anexo;
- la garantía de que el personal al que se otorgue acceso esté en condiciones de respetar el presente Código. Eso incluye una capacitación y la inclusión de un compromiso de discreción en el contrato de empleo que se firme, antes de que se otorgue acceso a las bases de datos;
- la garantía de que el acceso se otorgue sobre la base de la “necesidad de saber”;
- el mantenimiento de un registro de personal con acceso a cada una de las bases de datos y su actualización cuando corresponda (p. ej., cuando se asignen al personal responsabilidades distintas que ya no requieran ese acceso);
- si es factible, deberá mantenerse, para posibilitar la rendición de cuentas, un registro histórico del personal que haya tenido acceso a cada una de las bases de datos durante el período en el que los datos procesados por esos miembros del personal se mantengan en la base de datos.

Cada miembro del personal deberá procesar los datos dentro de los límites de los derechos de procesamiento que se le hayan otorgado.

Puede someterse a obligaciones de discreción contractuales adicionales a los miembros del personal con más derechos de acceso o que estén a cargo de la administración de los derechos de acceso.

2. Seguridad física

Cada uno de los controladores de datos es responsable de:

- establecer normas de seguridad que definan controles de seguridad técnicos, administrativos y de procedimientos para garantizar niveles de confidencialidad adecuados, así como la

integridad física y la disponibilidad de las bases de datos (ya sean físicas o basadas en IT), según los riesgos imperantes que se identifiquen;

- garantizar que se informe al personal de esas normas de seguridad y que los miembros del personal las cumplan;
- desarrollar mecanismos de control adecuados para garantizar que se mantenga la seguridad de los datos;
- garantizar que se apliquen, a los lugares de almacenamiento, estándares adecuados de protección frente a incendios y a riesgos eléctricos;
- garantizar que los volúmenes de almacenamiento se mantengan en el mínimo estrictamente necesario.

3. Seguridad de IT

El controlador de datos deberá:

- establecer normas de seguridad que definan controles de seguridad técnicos, administrativos y de procedimientos para garantizar niveles de confidencialidad, integridad y disponibilidad adecuados para los sistemas de información que se utilicen, según la evaluación de riesgos;
- desarrollar mecanismos de control adecuados para garantizar que se mantenga la seguridad de los datos;
- establecer normas de seguridad específicas para parte de la infraestructura de comunicación de IT, una base de datos o un departamento específico si se considera necesario.

Toda la correspondencia por correo electrónico, ya sea interna o externa, que contenga datos personales deberá procesarse sobre la base de la “necesidad de saber”. Los destinatarios de la correspondencia por correo electrónico deberán seleccionarse cuidadosamente, para evitar una divulgación innecesaria de datos personales.

Los accesos remotos a los servidores y el uso doméstico de computadoras de escritorio y portátiles deben cumplir los estándares de protección que se establecen en la política de seguridad de IT del controlador de datos. A menos que sea absolutamente necesario por razones operacionales, debe evitarse el uso de puntos de acceso a Internet y conexiones sin cable no seguras para recuperar, intercambiar, transmitir o transferir datos personales.

El personal que gestione datos personales debe adoptar las precauciones necesarias al establecer conexiones remotas con los servidores del controlador de datos. Las contraseñas deben protegerse siempre, y los miembros del personal deben comprobar que han salido adecuadamente de los sistemas informáticos y que han cerrado los navegadores abiertos.

Las computadoras portátiles, los teléfonos inteligentes y otros equipos portátiles requieren precauciones de seguridad especiales, particularmente cuando se trabaja en entornos difíciles. Los equipos portátiles deben guardarse en todo momento en lugares seguros y protegidos.

No deben utilizarse dispositivos portátiles o extraíbles para almacenar documentos que contengan datos personales clasificados como particularmente sensibles. Si fuera inevitable hacerlo, los datos

personales se deberán transferir a sistemas informáticos y aplicaciones de bases de datos adecuados en cuanto sea razonablemente práctico hacerlo. Si se utilizan dispositivos de memoria flash, como memorias USB y tarjetas de memoria, para almacenar temporalmente datos personales, esos dispositivos deben estar protegidos y sus registros electrónicos deben encriptarse. Debe eliminarse la información del dispositivo portátil o extraíble en cuanto se haya almacenado correctamente, si ya no es necesario tenerla en ese soporte.

Recuperación y copias de seguridad

Se deben cubrir todos los registros electrónicos con mecanismos de recuperación y procedimientos de copia de seguridad eficaces, y el responsable de ICT (Information and Communications Technology, Tecnología de la Información y la Comunicación) debe asegurarse de que se hagan periódicamente copias de seguridad. La frecuencia de los procedimientos de copia de seguridad variará según la sensibilidad de los datos personales en cuestión. Se deben automatizar los registros electrónicos para permitir una recuperación sencilla en situaciones en las que los procedimientos de copia de seguridad sean difíciles debido, entre otros factores, a cortes de luz periódicos, fallos del sistema y desastres naturales.

Cuando ya no se necesiten los registros electrónicos y las aplicaciones de bases de datos, el controlador de datos deberá coordinar con el responsable de ICT pertinente para asegurarse de su eliminación permanente.

4. Obligación de mantener discreción y conducta del personal

La obligación de mantener discreción es un elemento clave de la seguridad de los datos personales. La obligación de mantener discreción implica:

- que todo el personal y los consultores externos firmen acuerdos de discreción y confidencialidad, en el marco de sus contratos de empleo o consultoría. Este requisito va junto con el requisito de que el personal solo procese datos según las instrucciones del controlador de datos;
- que cualquier procesador externo tenga cláusulas de confidencialidad en su contrato. Este requisito va junto con el requisito de que el procesador solo procese datos según las instrucciones del controlador de datos;
- la aplicación estricta de la tipología de la gestión de la información, basada en su nivel de confidencialidad;
- la garantía de que cualquier solicitud por parte de los titulares de los datos de que sus datos personales se procesen de cierta manera concreta, y en particular que se consideren confidenciales y no se transmitan a terceras partes, se registre correctamente en el expediente del titular de los datos.

Para limitar el riesgo de filtraciones, solo el personal debidamente autorizado podrá encargarse de

obtener y gestionar datos de fuentes confidenciales y tener acceso a documentos según la tipología de la gestión de la información correspondiente.

Los miembros del personal son responsables de atribuir niveles de confidencialidad a los datos que procesen, basados en la tipología de la gestión de la información aplicable, y de respetar la confidencialidad de los datos que consulten, transmitan o utilicen a los efectos de su procesamiento externo.

El miembro del personal que atribuyó inicialmente un nivel de confidencialidad puede modificar en cualquier momento ese nivel que ha atribuido a los datos, especialmente al atribuirles un nivel de confidencialidad inferior al que se indicó previamente si considera que los datos requieren una menor protección.

5. Planificación de contingencias

El controlador de datos es responsable de revisar y poner en marcha un plan de evacuación de los registros para casos de emergencia.

6. Métodos de destrucción

Cuando se establezca que ya no es necesario conservar ciertos datos personales, todos los registros y copias de seguridad se deberán destruir o anonimizar.

El método de destrucción dependerá, entre otras cosas, de:

- la naturaleza y la sensibilidad de los datos personales;
- el formato y el dispositivo de almacenamiento;
- el volumen de registros electrónicos o en papel.

El controlador deberá evaluar la sensibilidad antes de la destrucción, para asegurarse de que se utilicen métodos de destrucción adecuados para eliminar esos datos personales.

Destrucción de registros en papel

Los registros en papel se deberán destruir con métodos como la trituración y la quema, que no permiten reconstruirlos o utilizarlos en el futuro.

Si se decide que los registros en papel deben digitalizarse, mediante una conversión correcta de los registros de papel al formato electrónico, deberá destruirse cualquier rastro de los registros en papel, a menos que la legislación nacional correspondiente requiera la retención de los registros en papel o establezca que debe guardarse una copia en papel a efectos de archivo.

Destrucción de registros electrónicos

Se debe derivar la destrucción de registros electrónicos al personal de ICT pertinente, porque las opciones de borrado de los sistemas informáticos no garantizan necesariamente una eliminación

completa.

Tras recibir las instrucciones correspondientes, el personal de ICT pertinente deberá asegurarse de eliminar completamente de los sistemas informáticos y los programas de software cualquier rastro de datos personales.

Las unidades de disco y las aplicaciones de bases de datos deberán limpiarse y todos los medios reescribibles, como, entre otros, CD, DVD, microfichas, cintas de vídeo y cintas de audio que se utilicen para almacenar datos personales se deberán borrar antes de volver a utilizarlos. Se debe hacer un seguimiento estricto de las medidas físicas para destruir registros electrónicos, como el reciclaje, la pulverización y la quema.

Registros de eliminación

El controlador de datos deberá asegurarse de que todos los contratos de servicios, memorandos de entendimiento, acuerdos y contratos escritos de transferencia o procesamiento pertinentes incluyan un período de retención para la destrucción de datos personales tras el cumplimiento del fin que se especifica. Las terceras partes deberán devolver los datos personales al controlador de datos y certificar que se han destruido todas las copias de esos datos, incluidos los datos personales divulgados a sus agentes autorizados y subcontratados. Deben mantenerse registros de eliminación que indiquen el momento y el método de destrucción, así como la naturaleza de los registros destruidos, y adjuntarse a los informes de proyecto o de evaluación.

La destrucción de grandes volúmenes de registros en papel puede subcontratarse a empresas especializadas. En esas circunstancias, el controlador de datos deberá asegurarse por escrito de que se respete la confidencialidad de los datos personales y de que la entrega de registros de eliminación y certificados de destrucción forme parte de las obligaciones contractuales de las terceras partes.

7. Otras medidas

La seguridad de los datos requiere, asimismo, normas organizativas internas adecuadas, incluida una divulgación interna periódica entre todos los empleados de las normas de seguridad de los datos y sus obligaciones según la legislación de protección de datos, especialmente en relación con sus obligaciones de confidencialidad.

Nombramiento de un responsable de seguridad

Cada uno de los controladores de datos deberá asignar la función de responsable de seguridad de los datos a un miembro de su personal o a varios (posiblemente de las áreas de administración o IT), para que lleven a cabo las operaciones de seguridad.

El responsable de seguridad deberá, en particular:

- garantizar el cumplimiento de los procedimientos de seguridad que establecen este Código y sus normas de seguridad correspondientes;
- actualizar esos procedimientos cuando sea necesario;
- realizar capacitaciones adicionales para el personal sobre seguridad de los datos.

Anexo 5: Información que se debe brindar

Información que se debe brindar:	Consentimiento	Interés vital/Interés público	Interés legítimo	Obligación contractual/legal
Controlador de datos/Personal a cargo	Sí	Sí	Sí	Sí
Propósito del procesamiento	Sí	Sí	Sí	Sí
Procesadores externos previstos	Sí	DPIA y divulgación de información privada, si es posible	Sí	Sí
Transferencias previstas	Sí	DPIA y divulgación de información privada, si es posible	Sí	Sí
Derechos del titular de los datos (información, acceso, corrección, eliminación, objeción)	Sí	DPIA y divulgación de información privada, si es posible	Sí	Sí
Si corresponde, establecer si la provisión de datos es un requisito legal o contractual	No aplicable	No aplicable	Sí	Sí

Anexo 6: Breve orientación sobre la DPIA

El propósito de una evaluación del impacto de la protección de datos (DPIA, por sus siglas en inglés) es identificar, evaluar y abordar los riesgos específicos para los datos personales que surgen de ciertas actividades de Restablecimiento del contacto entre familiares (RCF). Una DPIA debe llevar a la adopción de medidas para evitar, minimizar o mitigar de alguna otra manera los riesgos. El objetivo de esta guía de la DPIA es permitir al personal de RCF llevar a cabo una evaluación de ese tipo. **Las Sociedades Nacionales tienen a disposición como documento aparte una plantilla de DPIA para las actividades de RCF,** con ejemplos de los tipos de riesgos y de posibles medidas mitigantes.

Estos son algunos ejemplos de cuándo se debería plantear la realización de una DPIA:

- Su institución almacenaba sus archivos en CD y papel. Ahora quiere introducir un almacenamiento electrónico central para esos archivos. ¿Cómo va a decidir dónde conviene almacenar cada tipo de información?
- Un tsunami arrasa decenas de pueblos costeros. Se denuncia la desaparición de miles de personas. ¿Cuánta información personal debe obtener de los familiares de las personas desaparecidas? ¿Debe ser mucha o una cantidad mínima? ¿Debe incluir información sensible (p. ej., ADN, religión, afiliación política)?
- El gobierno implementa un sistema para centralizar toda la información sobre personas desaparecidas como consecuencia del tsunami. Quiere que usted le facilite la información que tiene sobre personas desaparecidas por esos hechos. ¿Cuánta información personal debe transmitir a las autoridades para buscar a las personas desaparecidas? ¿En qué condiciones debe darle información personal?
- Otra organización humanitaria le pide que comparta datos sobre los habitantes de un campamento de refugiados. ¿Debe compartir esos datos? ¿En qué condiciones? ¿Cuáles son las consecuencias de hacerlo? ¿Será igual de cuidadosa que usted esa organización en relación con los datos personales?
- ¿Puede publicar en Internet fotos de niños no acompañados que busquen a sus familiares? ¿Puede hacer carteles de niños desaparecidos? ¿En qué circunstancias y condiciones?
- Una red social le ofrece ayuda para el restablecimiento del contacto entre familiares tras una catástrofe. ¿Cómo puede colaborar con esa red social sin poner en peligro la seguridad de los datos personales de las personas afectadas?
- Mañana, el CICR tiene previsto hacer una visita a un lugar de detención donde presuntamente se encuentra una persona buscada. Dada la urgencia, ¿puede transferir una solicitud de búsqueda o un mensaje de Cruz Roja al CICR por correo electrónico?

En algunos casos, es posible que no haya tiempo suficiente para hacer una DPIA completa o que la complejidad, sensibilidad o escala de la operación de procesamiento no requiera una DPIA formal. Sin embargo, el personal de RCF siempre debe tener en mente una evaluación de riesgos en relación con la protección de los datos (y registrarla cuando sea posible) al tomar decisiones sobre la transferencia de datos. Por ello, el personal y los voluntarios de RCF deben ser conscientes del proceso de la DPIA y plantearse las preguntas que figuran a continuación.

Un **proceso** de DPIA suele tener los siguientes pasos. Estos pasos deben reflejarse en el informe de la DPIA.

A. Evaluación general

1. Según la complejidad, sensibilidad y escala de la operación de procesamiento, establecer:

- si es necesario realizar una DPIA;
- quién va a llevar a cabo la DPIA;
- quién va a revisar y validar la DPIA.

2. En el contexto de la actividad de RCF, describir cómo se obtienen, utilizan, almacenan y transmiten los datos personales. Eso incluye un panorama de las partes interesadas y una descripción de los flujos de información (es decir, qué información se recaba, sobre quién, quién debe obtenerla; cómo se utiliza la información; cómo, dónde y durante cuánto tiempo se guarda; si se recurre o no a procesadores externos, quién tiene acceso a la información).

3. Identificar las partes interesadas a las que se debe consultar. Podrían ser partes interesadas internas (como un experto en IT, un asesor jurídico, un psicólogo, expertos en programas, etc.) o externas (como otras instituciones, agencias gubernamentales, trabajadores sociales, líderes comunitarios, tutores legales, etc.).

B. Evaluación

4. Identificar los riesgos para las personas que surgen de la operación de procesamiento y los riesgos de incumplimiento del Código de Conducta sobre protección de datos.

5. Evaluar los riesgos.

6. Identificar medidas para evitar, minimizar o mitigar de alguna otra manera los riesgos.

7. Hacer recomendaciones.

C. Validación e implementación

8. Solicitar una revisión y lograr una validación.

9. Implementar las recomendaciones acordadas.

10. Actualizar la DPIA si hay cambios en la actividad.

Si se lleva a cabo una DPIA, eso debe reflejarse en un informe (con información sobre las secciones A), B) y C) que se detallaron antes). Según la complejidad, sensibilidad y escala de la operación de procesamiento, el **informe** de una DPIA (el resultado del proceso de DPIA) puede ser muy breve o más exhaustivo y detallado. El informe de una DPIA puede incorporar la plantilla que tienen a disposición por separado las Sociedades Nacionales.

Anexo 7: Cumplimiento de una obligación legal

Según las circunstancias del controlador de datos, puede incluir:

- el cumplimiento de la legislación nacional o regional, por ejemplo, en el ámbito del derecho laboral, los informes financieros, el fraude, el lavado de dinero;
- órdenes de los tribunales.