POLÍTICA

sobre la Protección de Datos Personales de las Personas de Interés del ACNUR

UNHCR
ACNUR
La Agencia de la ONU para los Refugiados

POLÍTICA DE
PROTECCIÓN DE DATOS

ÍNDICE

1

DISPOSICIONES GENERALES

1.1 OBJETIVO

Esta política establece las reglas y los principios relacionados con el procesamiento de los datos personales de las personas de interés del ACNUR. Su propósito es asegurar que el ACNUR procese los datos personales de una manera coherente con los *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales*[1] de la Asamblea General de las Naciones Unidas de 1990 y otros instrumentos internacionales relativos a la protección de datos personales y la privacidad de las personas. La política se complementará con directrices operativas que brindarán orientación sobre su implementación, supervisión y rendición de cuentas.

1.2 FUNDAMENTO

1.2.1 El ACNUR en el ejercicio de su mandato de proporcionar protección internacional y soluciones a los refugiados, y también a la hora de ofrecer sus buenos oficios a los Estados, a menudo es necesario que éste organismo procese los datos personales de las personas de interés de la Organización. Esto también puede incluir la necesidad de compartir datos personales con las agencias implementadoras y/o con terceros. Al procesar datos personales existen riesgos inherentes tales como la pérdida o divulgación accidental o no autorizada. Dada la situación de particular vulnerabilidad de las personas de interés del ACNUR, generalmente la naturaleza de sus datos personales es sensible y, por lo tanto, requiere un manejo cuidadoso de acuerdo con esta Política. Por consiguiente, para el ACNUR, la protección adecuada de

1 Asamblea General de la ONU, Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales, adoptada mediante Resolución A/Res/45/95, de 14 de diciembre de 1990, disponible en inglés en http://www.refworld.org/docid/3ddcafaac.html

los datos personales de las personas de interés es de especial importancia y la Organización tiene la responsabilidad de procesarlos de manera que se respeten los principios de la protección de datos.[2]

1.2.2 La política también complementa las disposiciones del Reglamento del Personal de las Naciones Unidas 1.2 (i) y compromisos del Código de Conducta del ACNUR, en particular, el Principio 6, que insta al personal a que salvaguarde y haga uso responsable de la información a la que tiene acceso.

1.3 ÁMBITO

1.3.1 Esta política se aplica a todos los datos personales que el ACNUR tenga con respecto a las personas de interés del ACNUR[3]. El procesamiento de otros datos, por ejemplo, agregados o anónimos, no está contemplado dentro del ámbito de esta política, pero está cubierto, entre otros, por la Política del ACNUR sobre la Clasificación, Manejo y Divulgación de Información.

1.3.2 Esta política se aplica si el procesamiento se lleva a cabo o bien dentro de una oficina del ACNUR o entre diferentes oficinas del ACNUR en el mismo país o más de un país, o bien si los datos personales se transfieren a las agencias implementadoras o a terceros. La política sigue siendo aplicable incluso después de que las personas ya no son personas de interés del ACNUR.

1.3.3 El cumplimiento de esta política es obligatorio para todo el personal del ACNUR.

---

2 El Comité Ejecutivo del Programa del Alto Comisionado se ha referido a los principios de protección de datos en las siguientes Conclusiones: N° 91 (LII) - 2001 (f), disponible en: http://www.acnur.org/t3/fileadmin/Documentos/BDL/2002/0714.pdf , No. 93 (LIII)– 2002 (b) (viii), disponible en: http://www.acnur.org/t3/fileadmin/Documentos/BDL/2003/2074.pdf , y No. 102 (LVI) – 2005 (v), disponible en: http://www.acnur.org/t3/fileadmin/Documentos/BDL/2005/3861.pdf .

3 ACNUR, Nota sobre el mandato del Alto Comisionado para los Refugiados y su Oficina, octubre 2013, disponible en: http://www.acnur.org/fileadmin/scripts/doc.php?file=fileadmin/Documentos/BDL/2014/9445 .

1.4 TÉRMINOS Y DEFINICIONES

Para los fines de esta política, se aplican las siguientes definiciones:

Consentimiento

Cualquier indicación informada y libremente expresada de acuerdo por parte de la persona interesada al procesamiento de sus datos personales, que se puede dar ya sea por medio de una declaración por escrito u oral o a través de una clara acción afirmativa.

Controlador de datos

El miembro del personal del ACNUR, por lo general el Representante de una oficina de ACNUR en el país, que tiene la autoridad para supervisar la gestión del procesamiento de datos personales y determinar su finalidad.

Procesador de datos

Cualquier miembro del personal del ACNUR u otra persona física u organización, incluyendo una agencia implementadora o un tercero que lleva a cabo el procesamiento de datos personales en nombre del controlador de datos.

Punto focal de protección de datos

En principio, el funcionario de protección de más alto rango del ACNUR en una oficina de país u operación del ACNUR, que asiste al controlador de datos en el desempeño de sus responsabilidades con respecto a esta Política.

Evaluación del impacto en la protección de datos

Una herramienta y un proceso para evaluar los impactos sobre la protección de los interesados en el procesamiento de sus datos personales y para identificar acciones correctivas, según sea necesario, con el fin de evitar o minimizar tales impactos.

Oficial de protección de datos

El funcionario del ACNUR en la División de Protección Internacional de la Sede que supervisa, monitorea e informa sobre el cumplimiento de esta Política. Las responsabilidades del oficial de protección de datos se exponen en la sección 7.3.

Titular de los datos

Una persona cuyos datos personales sean objeto de procesamiento.

Acuerdo de transferencia de datos

Un acuerdo entre el ACNUR y una agencia implementadora o un tercero que establece los términos y las condiciones del uso de los datos personales, incluyendo los componentes de datos que han de ser compartidos, el modo de transferencia, cómo se pueden usar los datos, las medidas de seguridad de los datos y otros temas relacionados.

Agencia implementadora

Una organización establecida como una entidad autónoma e independiente del ACNUR con la que el ACNUR se asocia mediante un acuerdo de colaboración para proyectos con el fin de llevar a cabo la implementación de las actividades programáticas dentro de su mandato.

Datos personales

Cualquier dato relacionado con un individuo, quien podría ser identificado por tales datos; por tales datos y otra información; o por medios que razonablemente podrían ser usados con relación a tales datos. Los datos personales incluyen datos biográficos (biodatos), tales como el nombre, sexo, estado civil, la fecha y el lugar de nacimiento, el país de origen, el país de asilo, el número de registro individual, la ocupación, la religión y el origen étnico, datos biométricos[4] tales como una fotografía, una huella dactilar, una imagen del rostro o del iris, así como cualquier manifestación de opinión acerca de la persona, tales como evaluaciones de su condición y/o necesidades específicas.

Filtración de datos personales

Una violación de la seguridad de los datos que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal/ilícita de datos personales transferidos, almacenados o de otro modo procesados.

Persona de interés

Una persona cuyas necesidades de protección y asistencia son de interés para el ACNUR. Esto incluye a los refugiados, solicitantes de asilo, apátridas, desplazados internos y retornados.

4 Los datos biométricos son características biológicas (anatómicas o fisiológicas) o de comportamiento personal que pueden ser utilizados para establecer la identidad de una persona mediante la comparación con datos de referencia almacenados.

© ACNUR / Dalia Khamissy

Procesamiento de datos personales

Cualquier operación o conjunto de operaciones, automatizadas o no, que se realiza en relación a los datos personales, incluyendo pero no limitado a la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, uso, transferencia (ya sea en forma computarizada, oral o escrita), difusión o cualquier otra puesta a disposición, corrección o destrucción.

Terceros

Cualquier persona física o jurídica distinta al titular de los datos, el ACNUR o una agencia implementadora. Ejemplos de terceros son los gobiernos nacionales, organizaciones internacionales gubernamentales o no gubernamentales, entidades del sector privado o individuos.

2

PRINCIPIOS BÁSICOS

2.1 PRINCIPIOS BÁSICOS DEL PROCESAMIENTO DE DATOS PERSONALES

El personal del ACNUR debe respetar y aplicar los siguientes principios básicos al procesar datos personales:

(i) Procesamiento legítimo y justo

(ii) Especificación del propósito

(iii) Necesidad y proporcionalidad

(iv) Precisión

(v) Respeto de los derechos de las personas interesadas

(vi) Confidencialidad

(vii) Seguridad

(viii) Rendición de cuentas y supervisión

2.2 PROCESAMIENTO LEGÍTIMO Y JUSTO

El procesamiento de datos personales sólo podrá llevarse a cabo de forma legítima y de una manera justa y transparente. El ACNUR sólo podrá procesar datos personales con base en uno o más de los siguientes fundamentos legítimos:

(i) Con el consentimiento de la persona interesada

(ii) En los intereses vitales o superiores de la persona interesada

(iii) Para que el ACNUR pueda cumplir su mandato

(iv) Más allá del mandato del ACNUR, para garantizar la protección y seguridad de las personas de interés o de otros individuos

2.3 ESPECIFICACIÓN DEL PROPÓSITO

Los datos personales deben ser recopilados para uno o más propósitos específicos y legítimos y no deben ser procesados de manera incompatible con ese/esos propósito(s).

2.4 NECESIDAD Y PROPORCIONALIDAD

El procesamiento de datos personales debe ser necesario y proporcionado a los objetivos para los que se están procesando. Por lo tanto, los datos que se procesan deben ser adecuados y pertinentes a la finalidad identificada, y no deben exceder ese propósito.

2.5 PRECISIÓN

Los datos personales deben ser registrados con la mayor precisión posible y, cuando sea necesario, actualizados para garantizar que cumplen con el propósito(s) para los que se procesan.

2.6 RESPETO DE LOS DERECHOS DEL TITULAR DE LOS DATOS

Los derechos del titular de los datos relacionados con la información, el acceso, la rectificación, la cancelación y la oposición, se describen en la sección 3 de esta Política.

2.7 CONFIDENCIALIDAD

El personal del ACNUR debe mantener la confidencialidad de los datos personales de las personas de interés en todo momento, incluso después de que un titular de los datos ya no es persona de interés para el ACNUR.

2.8 SEGURIDAD

Con el fin de garantizar la confidencialidad e integridad de los datos personales, es necesario poner en práctica adecuadas medidas de seguridad de datos técnicos y de organización. La seguridad de datos y otros temas relacionados se describen en la sección 4. La transferencia de datos personales a terceros se limita a las condiciones establecidas en la sección 6.

2.9 RENDICIÓN DE CUENTAS Y SUPERVISIÓN

Con el fin de garantizar la rendición de cuentas para el procesamiento de datos personales de acuerdo con esta Política, el ACNUR establecerá una estructura de rendición de cuentas y supervisión tal y como se define en la sección 7.

3

DERECHOS DEL TITULAR DE LOS DATOS

3.1 INFORMACIÓN

Al recopilar los datos personales del titular de los datos, el ACNUR debe, por escrito o verbalmente, y de manera y con un lenguaje que sea comprensible, informar al titular de los datos de lo siguiente:

(i) El o los objetivos específicos para los que se procesarán los datos personales o categorías de datos personales;

(ii) Si dichos datos serán transferidos a una o más agencias implementadoras o a terceros o, cuando los datos están siendo recopilados por una agencia implementadora en nombre del ACNUR, que los interesados estén informados de este hecho;

(iii) La importancia de que el titular de los datos proporcione información precisa y completa;

(iv) La obligación del titular de los datos de mantener al ACNUR, y/o, en su caso, a las agencias implementadoras, informadas de los cambios en su situación personal[5];

(v) Cualquier consecuencia de la negativa o el rehusarse a proporcionar los datos personales solicitados;

(vi) El derecho del titular de los datos de solicitar el acceso a sus datos personales, o la rectificación o eliminación de los mismos;

(vii) El derecho del titular de los datos a oponerse a la recopilación de datos personales;

(viii) Cómo presentar una reclamación ante el controlador de datos y ante la Oficina del Inspector General.

5 En particular, los cambios en el estado civil, por ejemplo, nacimientos, defunciones y matrimonios.

3.2 ACCESO

A solicitud del titular de los datos, éste puede recibir lo siguiente del ACNUR:

(i) Confirmación de si los datos relacionados con él o ella han sido, está siendo o serán procesados; y

(ii) Información sobre los datos personales que se procesan, el propósito(s) para el procesamiento de estos datos y las agencias implementadoras y/o terceros a los que dichos datos han sido, están siendo o serán transferidos.

3.3 CORRECCIÓN Y ELIMINACIÓN

3.3.1 El titular de los datos podrá solicitar la corrección o eliminación de los datos personales que son inexactos, incompletos, innecesarios o excesivos.

3.3.2 Cuando un titular de datos solicita la corrección o eliminación de sus datos personales, el ACNUR debe solicitar la prueba relativa a la inexactitud o al carácter incompleto de estos datos.

3.4 OBJECIÓN

Sujeta a la sección 3.7 abajo, un titular de datos podrá oponerse al procesamiento de sus datos personales cuando existen motivos legítimos relacionados con su situación personal específica. Si se justifica la objeción, el ACNUR ya no debe procesar los datos personales en cuestión.

3.5 MODALIDADES DE SOLICITUDES

3.5.1 Las solicitudes de información sobre el acceso, corrección o eliminación de datos personales o sobre una objeción, pueden ser realizadas por el titular de datos o su representante legal autorizado, o, en el caso de un niño, por un padre o tutor legal. Las solicitudes deben ser presentadas verbalmente o por escrito a la oficina del ACNUR en el país donde se están procesando los datos.

3.5.2 Antes de cumplir con cualquier solicitud u objeción, el ACNUR debe asegurarse de la identidad de la persona que realiza la solicitud u objeción. Se requiere que el individuo se identifique de una manera apropiada. En el caso de un representante legal o tutor legal, debe ser suministrada la prueba de dicha autoridad legal. Las solicitudes y objeciones por parte de los padres o tutores de los niños deben ser evaluadas con respeto al interés superior del niño.

3.6 REGISTRO Y RESPUESTA POR PARTE DEL ACNUR

3.6.1 El ACNUR debe registrar el hecho de haber brindado la información al titular de datos de conformidad con la sección 3.1, así como registrar las solicitudes recibidas para el acceso, corrección, eliminación u objeción y la respuesta proporcionada en relación con esas solicitudes relativas a las secciones 3.2, 3.3 y 3.4.

3.6.2 El ACNUR debe dar respuesta a una solicitud u objeción bajo la sección 3 dentro de un plazo razonable, por escrito u oralmente, y en una forma y utilizando un lenguaje que sea comprensible para el titular de los datos y/o su representante o tutor legal, según sea el caso.

© ACNUR / M. Abu Asaker

3.7 RESTRICCIONES

Con base en las consultas realizadas al Oficial de Protección de Datos, y a otras contrapartes pertinentes en la Sede, el ACNUR puede negarse a dar una respuesta o limitar o restringir su respuesta a una solicitud u objeción bajo la sección 3 cuando:

(i) Se trate de una medida necesaria y proporcionada para proteger o garantizar uno o más de los siguientes:

(a) La seguridad y la protección del ACNUR, de su personal o del personal de las agencias implementadoras; o

(b) Las necesidades operativas imperiosas y las prioridades del ACNUR en el cumplimiento de su mandato.

(ii) Existen razones para creer que la solicitud es manifiestamente abusiva, fraudulenta u obstructiva a la finalidad del procesamiento.

4

PROCESAMIENTO DE DATOS POR EL ACNUR

4.1 CONFIDENCIALIDAD DE LOS DATOS PERSONALES

4.1.1 Los datos personales son, por definición, clasificados como confidenciales. La confidencialidad de los datos personales debe, en todo momento, ser respetada por el ACNUR al procesar los datos personales.

4.1.2 Con el fin de garantizar y respetar la confidencialidad, los datos personales deben ser archivados y almacenados de manera que sean accesibles sólo al personal autorizado y transferidos sólo a través del uso de medios de comunicación protegidos.

4.2 SEGURIDAD DE DATOS PERSONALES

4.2.1 El ACNUR debe garantizar e implementar un alto nivel de seguridad de los datos que se adecue a los riesgos que entraña la naturaleza y el procesamiento de los datos personales, la disponibilidad y la calidad de los equipos necesarios, el costo y la viabilidad operativa.

4.2.2 Las medidas de seguridad de los datos del ACNUR deben proteger los datos personales contra el riesgo de destrucción, pérdida, alteración, divulgación no autorizada o acceso a los datos personales en forma accidental o ilícita/ilegítima.

4.2.3 Teniendo en cuenta la tecnología disponible y el costo de implementación, el ACNUR debe poner en práctica medidas organizativas y técnicas adecuadas para garantizar que el procesamiento cumpla con los requisitos de la presente Política. Esto incluye la implementación de tecnologías para mejorar la protección de datos y herramientas que permitan a los procesadores de datos mejorar la protección de datos personales ("privacidad por diseño y por defecto").

4.2.4 Las medidas organizativas incluyen:

(i) Establecer procedimientos operativos estándares;

(ii) La organización de la formación del personal en materia de protección y seguridad de los datos; y

(iii) La realización de evaluaciones de impacto de protección de datos (sección 4.5).

4.2.5 Las medidas técnicas incluyen:

(i) El mantenimiento de la seguridad física de las instalaciones, los equipos portátiles, los archivos de casos individuales y los registros;

(ii) El mantenimiento de la seguridad del equipo y la tecnología de la información (IT, por sus siglas en inglés), por ejemplo, el control de acceso (por ejemplo, contraseñas, acceso por niveles), control de usuario, control de almacenamiento, control de entrada, control de comunicación y transporte (por ejemplo, encriptación).

4.2.6 En condiciones de seguridad en deterioro que suponen un grave riesgo de filtraciones de datos personales, el ACNUR debe tomar todas las medidas necesarias y posibles para evitar este tipo de filtraciones de datos personales, mediante la reubicación, o, como último recurso, la destrucción de los expedientes individuales, ya sean en papel o soporte informático, que contienen datos personales, con el fin de evitar cualquier perjuicio a los titulares de los datos.

4.3 GARANTIZAR LA PRECISIÓN DE LOS DATOS PERSONALES

4.3.1 El ACNUR puede corregir o eliminar los datos personales registrados en sus sistemas que son inexactos, incompletos, innecesarios o excesivos.

4.3.2 El ACNUR debe actualizar los registros de datos personales cuando sea necesario y verificarlos periódicamente.

4.3.3 Cuando los datos personales son corregidos o eliminados en los sistemas del ACNUR, el ACNUR debe notificar, tan pronto como sea razonablemente posible, a todas las agencias implementadoras y/o terceros a los que se les transfirieron los datos personales pertinentes.

4.4 NOTIFICACIÓN DE FILTRACIÓN DE DATOS PERSONALES

4.4.1 Se requiere que el personal del ACNUR notifique al controlador de datos lo más pronto posible en cuanto se conozca de una filtración de datos personales y que registre la infracción adecuadamente.

4.4.2 Si es probable que una filtración de datos personales resulte en perjuicios o daños personales a un titular de datos, el controlador de datos deberá esforzarse por comunicar la filtración de datos personales a la persona titular de los datos y tomar las medidas de mitigación apropiadas sin retrasos injustificados. En tales casos, el controlador de datos también debe notificar al Oficial de Protección de Datos sobre la filtración de datos personales.

4.4.3 La notificación debe describir lo siguiente:

(i) La naturaleza de la filtración de los datos personales, incluyendo las categorías y el número de titulares de los datos y los registros de los datos en cuestión;

(ii) Las conocidas y previsibles consecuencias adversas de la filtración de datos personales; y

(iii) Las medidas adoptadas o propuestas para ser tomadas con el fin de mitigar y hacer frente a los posibles efectos adversos de la filtración de datos personales.

4.5 EVALUACIONES DE IMPACTO DE PROTECCIÓN DE DATOS

4.5.1 Al elaborar nuevos sistemas, proyectos o políticas o antes de firmar acuerdos de transferencia de datos con agencias implementadoras o con terceros que puedan tener un impacto negativo sobre la protección de los datos personales de las personas de interés, el ACNUR debe llevar a cabo una Evaluación de Impacto de Protección de Datos (DPIA, por sus siglas en inglés). Una DPIA se requiere cuando es probable que la recopilación y el procesamiento o la transferencia de datos personales sean extensiva, repetida o estructural (es decir, cuando los datos se comparten con una agencia implementadora o con un tercero durante cierto periodo de tiempo).

4.5.2 Una DPIA debe contener una descripción general del sistema, el proyecto, la política o el acuerdo de intercambio de datos previsto que implica el procesamiento de datos personales, un análisis de los riesgos para los derechos de los titulares de los datos en razón de las circunstancias y la naturaleza de los datos personales procesados, las salvaguardias, la seguridad y otras medidas establecidas o propuestas para garantizar el cumplimiento de esta política.

4.5.3 Los controladores de datos son los responsables de organizar y elaborar las DPIA, cuando sea necesario. Las DPIA normalmente se llevan a cabo a nivel de país, a menos que se decida que una DPIA se llevará a cabo a nivel mundial o regional debido al alcance del sistema o arreglo.

4.5.4 Los controladores de datos deben mantener al Oficial de Protección de Datos plenamente informado sobre cualquier DPIA que se lleva a cabo bajo su responsabilidad y compartir una copia de la DPIA.

4.6 RETENCIÓN

4.6.1 Los datos personales que no se registran en los expedientes de casos individuales no deberán conservarse más tiempo de lo necesario de acuerdo a la finalidad para el cual fueron recolectados.

4.6.2 Todos los archivos de casos individuales, ya sean abiertos o cerrados, se consideran registros permanentes, y por lo tanto deben conservarse permanentemente de acuerdo con la política de acceso de los archivos del ACNUR[6].

6 Política de acceso del ACNUR, disponible en inglés en: . http://www.unhcr.org/3b03896a4.html

5

PROCESAMIENTO DE DATOS POR AGENCIAS IMPLEMENTADORAS

5.1 CONDICIÓN GENERAL

Cuando la recopilación y procesamiento de datos personales es una de las responsabilidades de las agencias implementadoras, los datos personales están siendo recopilados y procesados en nombre del ACNUR. Por estas razones, se espera que las agencias implementadoras respeten y apliquen normas y principios básicos de protección de datos personales iguales o comparables a los que figuran en la presente Política (en particular, las secciones 2, 3 y 4). Esto se aplica cuando el ACNUR tiene la intención de transferir datos personales a las agencias implementadoras o bien si las agencias implementadoras recopilan datos personales con el fin de llevar a cabo las actividades acordadas.

5.2 VERIFICACIÓN

Independientemente de un acuerdo de asociación, antes de transferir datos personales a una agencia implementadora o contratar a una agencia implementadora para la recolección y procesamiento de datos personales, el ACNUR debe verificar que el procesamiento de datos personales por parte de la agencia implementadora satisface los estándares y principios básicos de esta política. Dicha verificación podrá formar parte de una Evaluación de Impacto de Protección de Datos.

© ACNUR / Frederic Noy

5.3 ACUERDOS DE COLABORACIÓN

El ACNUR debe exigir a las agencias implementadoras que cumplan con esta política como un compromiso que forma parte de la firma de acuerdos de colaboración. Tales acuerdos también deben especificar el o los propósitos específicos para el procesamiento de datos personales y la base legítima para su procesamiento.

5.4 CAPACIDAD DE LA AGENCIA

El ACNUR puede que tenga que asistir a las agencias implementadoras a crear o mejorar su capacidad para cumplir con las normas y los principios de protección de datos contenidos en esta Política. Dicha asistencia puede estar relacionada con el establecimiento o ajuste de políticas, la realización de capacitación o la puesta en marcha de medidas técnicas y organizativas.

5.5 TERMINACIÓN DE LA ASOCIACIÓN

Tras la terminación de una asociación, todos los datos personales recopilados en el marco de la asociación serían devueltos al ACNUR. Los acuerdos de colaboración podrán establecer excepciones, en particular cuando existen razones legítimas para ello, a saber, el consentimiento de los titulares de los datos.

6

TRANSFERENCIA DE DATOS PERSONALES A TERCEROS

6.1 CONDICIONES GENERALES

6.1.1 El ACNUR puede transferir datos personales a terceros con la condición de que el tercero proporcione un nivel de protección de datos igual o comparable a esta Política.

6.1.2 Teniendo en cuenta los posibles riesgos de protección de datos que implican las transferencias a terceros, el ACNUR debe prestar especial atención a los siguientes principios básicos de esta Política:

(i) La transferencia se basa en una o más bases legítimas;

(ii) La transferencia es para uno o más propósitos específicos y legítimos;

(iii) Los datos personales que se van a transferir son adecuados, pertinentes, necesarios y no excesivos en relación con el o los propósitos para los que se están transfiriendo;

(iv) El titular de los datos ha sido informado, ya sea en el momento de la recolección de conformidad con la sección 3.1, o con posterioridad, sobre la transferencia de sus datos personales, a menos que se aplica una o más de las restricciones en la sección 3.7;

(v) El tercero respete la confidencialidad de los datos personales que le son transferidos por parte del ACNUR. Independientemente de que se haya firmado o no un acuerdo de transferencia de datos entre el ACNUR y el tercero, el ACNUR debe buscar el acuerdo por escrito del tercero sobre el hecho de que los datos personales serán confidenciales en todo momento. Con el fin de garantizar y respetar la confidencialidad, los datos personales deben ser archivados y almacenados de manera que sean accesibles sólo al personal autorizado y transferidos sólo a través del uso de medios de comunicación protegidos.

(vi) El tercero mantiene un alto nivel de seguridad de datos que protege los datos personales contra el riesgo de destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilícita/ilegítima.

6.1.3 Además, el ACNUR debe garantizar que la transferencia de datos personales no tenga efectos negativos sobre:

(i) la seguridad y protección del personal del ACNUR y/o el personal de las agencias implementadoras; y/o

(ii) el funcionamiento efectivo de una operación del ACNUR ni comprometa el mandato del ACNUR, por ejemplo, debido a la pérdida de un ambiente de confianza entre el ACNUR y las personas de interés o la pérdida de la percepción del ACNUR como organización independiente, humanitaria y no política.

6.1.4 Antes de comprometerse a transferir datos personales a un tercero, el ACNUR ha de evaluar el nivel de protección de datos ofrecido por el tercero. Como parte de esta evaluación, el controlador de datos debe evaluar, entre otros, las leyes y reglamentos aplicables, las políticas y los estatutos internos del tercero, las obligaciones contractuales específicas o medidas para respetar los marcos específicos de protección de datos, su implementación efectiva, así como los medios técnicos y organizativos de seguridad de datos puestos en marcha. De conformidad con la sección 4.5, el controlador de datos podría tener que llevar a cabo una DPIA.

6.2 ACUERDOS DE TRANSFERENCIA DE DATOS

6.2.1 A menos que existan motivos suficientes para no hacerlo, previo a la transferencia de datos personales a un tercero, el controlador de datos debe tratar de firmar un acuerdo de transferencia de datos, o, en su caso, incorporar cláusulas de protección de datos dentro de los acuerdos más amplios, sobre todo cuando es probable que la transferencia de datos personales sea extensiva, repetida, o estructural, es decir, cuando el mismo tipo o tipos de datos se comparten con el mismo tercero para el mismo propósito durante un determinado periodo de tiempo.

6.2.2 Los acuerdos de la transferencia de datos deberían, entre otros:

(i) abordar el o los objetivos para la transferencia de datos, los elementos de datos específicos a ser transferidos, así como las medidas de protección y seguridad de datos a ser puestos en marcha;

(ii) requerir que el tercero se comprometa a que sus medidas de protección y seguridad de datos están de acuerdo con esta Política; y

(iii) estipular los mecanismos de consulta, supervisión, rendición de cuentas y revisión para monitorear la transferencia por la vigencia del contrato.

6.2.3 El Oficial de Protección de Datos y el Servicio de Asuntos Jurídicos (LAS, por sus siglas en inglés) son los responsables de revisar y aprobar todos los acuerdos de transferencia de datos. Las copias de los acuerdos finales deben ser presentadas al Oficial de Protección de Datos.

6.3 TRANSFERENCIA A ORGANISMOS NACIONALES ENCARGADOS DE HACER CUMPLIR LA LEY Y A LOS TRIBUNALES

6.3.1 En circunstancias apropiadas, el ACNUR puede transferir datos personales a un organismo nacional encargado de hacer cumplir la ley o a un tribunal nacional. Estas transferencias pueden ser solicitadas por el organismo encargado de hacer cumplir la ley o la corte, o por iniciativa propia del ACNUR. Las transferencias pueden estar relacionadas con personas sujetas a una investigación por un delito presuntamente cometido, o en relación con la o las víctimas o testigo(s) de un delito.

6.3.2 Además de las condiciones generales para la transferencia de datos personales a terceros (sección 6.1, con la excepción de 6.1.2 (iv)), el ACNUR sólo podrá cooperar con dicha solicitud y la transferencia de datos personales a un organismo nacional encargado de hacer cumplir la ley o a un tribunal nacional si se cumplen las siguientes condiciones:

(i) La transferencia es necesaria para fines de la detección, prevención, investigación o enjuiciamiento de un delito grave, en particular, con el fin de evitar un riesgo inmediato y sustancial para la seguridad y protección de un individuo o del público;

(ii) El organismo encargado de hacer cumplir la ley o el tribunal que la solicita es competente en relación con la detección, prevención, investigación o enjuiciamiento del delito en cuestión;

(iii) La transferencia ayudará sustancialmente al organismo encargado de hacer cumplir la ley o al tribunal en la consecución de estos fines y que los datos personales no pueden de otra manera ser obtenidos de otras fuentes;

(iv) La transferencia no interfiere de manera desproporcionada con el derecho a la privacidad u otros derechos humanos de un titular de datos o de otra persona de interés; y

(v) En el caso de datos relacionados con víctimas y testigos, tque se haya obtenido su consentimiento a la transferencia.

6.3.3 Previo a la transferencia de datos personales a un organismo nacional encargado de hacer cumplir la ley o a un tribunal nacional, se debe buscar el asesoramiento del Oficial de Protección de Datos, en consulta con la Unidad de Protección y Seguridad Nacional dentro de la División de Protección Internacional, la LAS y la o las Oficinas correspondientes.

6.4 ORGANISMO INTERNACIONAL ENCARGADO DE HACER CUMPLIR LA LEY, CORTE INTERNACIONAL, TRIBUNAL U OTRO ORGANISMO INTERNACIONAL

Las solicitudes de transferencias de datos personales por parte de la Corte Penal Internacional, los tribunales penales internacionales ad hoc, las comisiones de investigación del mandato de la ONU y organismos internacionales similares deben ser remitidas a la División de Protección Internacional (Oficial de Protección de Datos, Unidad de Protección y Seguridad Nacional y la Unidad de Enlace con los Derechos Humanos según el caso) y LAS.

6.5 PRIVILEGIOS E INMUNIDADES

La transferencia de datos personales es sin perjuicio de los privilegios e inmunidades del ACNUR en el marco de la *Convención sobre Privilegios e Inmunidades de las Naciones Unidas de 1946* y no debe ser interpretado como si lo fuera. Existen privilegios e inmunidades del ACNUR y su personal, independientemente de cualquier acuerdo de cooperación con el gobierno de un país. Cualquier consulta sobre privilegios e inmunidades debe ser dirigida a LAS del ACNUR.

7

RENDICIÓN DE CUENTAS Y SUPERVISIÓN

7.1 ESTRUCTURA DE RENDICIÓN DE CUENTAS Y SUPERVISIÓN

La estructura de la rendición de cuentas y supervisión del ACNUR mencionada en la sección 2.9 consistirá de los siguientes actores claves:

(i) Un Oficial de Protección de Datos dentro de la División de Protección Internacional en la Sede del ACNUR,

(ii) Controladores de datos en cada oficina de país/operación, y

(iii) Puntos focales de protección de datos en las oficinas/operaciones de país.

7.2 CONTROLADOR DE DATOS Y PUNTO FOCAL DE PROTECCIÓN DE DATOS

7.2.1 El controlador de datos es responsable de establecer y supervisar el procesamiento de datos personales bajo su área de responsabilidad. Él o ella también, por tanto, es el principal responsable del cumplimiento de la política. Para tal efecto, el controlador de datos deberá designar un punto focal de protección de datos. El punto focal de protección de datos debe, en principio, ser el funcionario más alto de protección del ACNUR en una oficina/operación de país.

7.2.2 El controlador de datos, asistido por el punto focal de protección de datos, debe implementar esta política a través de lo siguiente, entre otros:

(i) Determinar la base legítima aplicable y los fines específicos y legítimos del procesamiento de datos;

(ii) Asegurar la implementación de medidas de organización y seguridad, así como evaluar la seguridad de los datos de terceros;

(iii) Establecer procedimientos internos, por ejemplo en la forma de Procedimientos Operativos Estándares de Protección de Datos, que cubran todos los aspectos relevantes de esta Política, en particular, en relación con el respeto de los derechos de los titulares de los datos y las medidas destinadas a garantizar la confidencialidad y seguridad de los datos;

(iv) Asegurar que los aspectos de protección y seguridad de datos se incluyen adecuadamente en los acuerdos correspondientes a las agencias implementadoras;

(v) Negociar y celebrar acuerdos de transferencia de datos con terceros, según sea necesario o apropiado.

7.2.3 Si es necesario, el controlador de datos y/o puntos focales de protección de datos deben buscar la asesoría del Oficial de Protección de Datos en relación con las consultas con respecto a la aplicación e interpretación de la presente Política.

7.3 OFICIAL DE PROTECCIÓN DE DATOS

7.3.1 El ACNUR nombrará a un Oficial de Protección de Datos ubicado en la División de Protección Internacional del ACNUR en la Sede, cuyas tareas serán las siguientes:

(i) Proporcionar asesoramiento, apoyo y capacitación en materia de protección de datos y la presente Política;

(ii) Mantener inventarios de información proporcionada por los controladores de datos y los puntos focales de protección de datos, incluidos los acuerdos de transferencia de datos, casos concretos de intercambio de datos por el ACNUR con terceros, evaluaciones de impacto de protección de datos, notificaciones de filtración de datos y quejas de los titulares de los datos;

(iii) Fomentar activamente que los controladores de datos y otros actores pertinentes adopten medidas encaminadas al cumplimiento de esta Política;

(iv) Monitorear y presentar informes sobre el cumplimiento de esta Política;

(v) Coordinar con LAS según sea necesario en virtud de la presente Política.

7.3.2 El Oficial de Protección de Datos presentará un informe anual sobre la protección de datos, a través del Director de la División de Protección Internacional, al Alto Comisionado Asistente en materia de Protección.

7.4 OFICINA DEL INSPECTOR GENERAL

Esta política no afecta la función del mandato de la Oficina del Inspector General (OIG), en especial para recibir denuncias de supuesta mala conducta, por ejemplo, por violación de la confidencialidad o fraude, y para llevar a cabo investigaciones sobre esta mala conducta.[7] De este modo, la OIG complementa la estructura de monitoreo y cumplimiento establecida por esta Política.

7.5 OFICINA DE ÉTICA

En apoyo a esta política, la Oficina de Ética proporcionará orientación sobre prácticas y normas éticas y ayudará a mitigar los riesgos relacionados con el procesamiento de datos personales a través de la aplicación del Código de Conducta del ACNUR, y la Política del ACNUR sobre la Protección de las Personas contra las Represalias *('Whistle-blower Policy').*

[7] La información sobre la función de la OIG y cómo presentar una denuncia está disponible en inglés en: http://www.unhcr.org/pages/52e11b746.html y en español en: http://www.acnur.org/el-acnur/estructura-y-organizacion/organizacion/oig-oficina-inspector-general-acnur/?sword_list[]=oficina&sword_list[]=del&sword_list[]=inspector&sword_list[]=general&no_cache=1.

© ACNUR / Jared Kohler

UNHCR
ACNUR
La Agencia de la ONU para los Refugiados