UNHCR ACNUR
La Agencia de la ONU para los Refugiados

GUÍA SOBRE LA PROTECCIÓN DE DATOS PERSONALES DE LAS PERSONAS DE INTERÉS DEL ACNUR

2018

POLÍTICA DE PROTECCIÓN DE DATOS

1. Índice

1. Disposiciones generales

1.1. Objetivo

El objetivo de esta *Guía sobre la protección de datos personales de las personas de interés* es ayudar al personal del ACNUR en la aplicación e interpretación de la Política sobre la Protección de Datos Personales de las Personas de Interés (PPD), adoptada en mayo de 2015.[1] Promueve la implementación de principios y prácticas en todas las operaciones del ACNUR.

1.2. Fundamento

La Política de Protección de Datos prevé en el párr. 1.1 que se complementará con directrices operativas. Si bien la Política estableció el marco general, incluidos los principios básicos del tratamiento de datos personales (párr. 2.1 de la PPD), una serie de conceptos claves (por ejemplo, datos personales, privacidad desde el diseño), herramientas (por ejemplo, evaluaciones de impacto) y procedimientos (por ejemplo, notificación de filtración y aprobación de acuerdos de transferencia de datos), la Guía es una herramienta que desarrolla y elabora sobre estos principios, conceptos y procedimientos con el fin de facilitar su implementación. La Guía también responde a las solicitudes en el terreno y de auditores.

1.3. Ámbito

El ámbito de esta Guía corresponde al ámbito de la Política de Protección de Datos, es decir, se aplica a todo el tratamiento de datos personales de personas de interés del ACNUR (párr. 1.3.1 y 1.3.2 de la PPD). Esta Guía se aplica a todo el personal del ACNUR. Es particularmente relevante para los controladores de datos, puntos focales de protección de datos y procesadores de datos.

1.4. Términos y definiciones

Además de los definidos en la Política de Protección de Datos, esta Guía introduce una serie de términos y definiciones adicionales. Las definiciones marcadas con (*) corresponden a las definiciones establecidas en el párr. 1.4 de la Política de Protección de Datos.

"Datos agregados" significa que los datos se combinan de manera que muestran valores o tendencias sin incluir los registros de los titulares de los datos o datos que harían que un titular de los datos sea identificable.

"Anonimización" es el proceso de eliminar o modificar todos los identificadores y códigos personales de tal manera que los titulares de los datos no pueden ser identificados y no existe una probabilidad razonable de que la identificación pueda tener lugar sobre la base de los datos, solos o en combinación con otros datos.

[1] ACNUR, *Política sobre la Protección de Datos Personales de las Personas de Interés del ACNUR ("Política de Protección de Datos")*, 27 de mayo de 2015, disponible en: http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=58aadc2b4.

"Asentimiento" es la voluntad y las opiniones expresadas por una niña o un niño para participar en actividades y servicios de asistencia o protección en situaciones en las cuales no puede legalmente dar su consentimiento formal para el tratamiento de datos personales debido a la edad, nivel de madurez y/u otros factores.

"Consentimiento" significa cualquier indicación informada y libremente expresada de un acuerdo por parte de la persona interesada para el tratamiento 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" significa el miembro del personal del ACNUR, por lo general el Representante en una oficina u operación del ACNUR en el país, que tiene la autoridad y la responsabilidad de supervisar la gestión del tratamiento de datos personales y determinar su finalidad. (*)

"Minimización de datos" significa un procedimiento estándar para minimizar los riesgos de protección de datos y garantizar que los datos recopilados, compartidos o procesados de otro modo sean necesarios y pertinentes para lograr un propósito específico.

"Procesador de datos" significa cualquier miembro del personal del ACNUR u otra persona física u organización, incluyendo una agencia Implementadora o un tercero que lleva a cabo el tratamiento de datos personales en nombre del controlador de datos. (*)

"Punto focal de protección de datos" significa, en principio, el funcionario de protección de más alto rango del ACNUR en una oficina de país u operación del ACNUR, que ha sido designado por el controlador de datos para ayudar en el desempeño de sus responsabilidades con respecto a esta Política. (*)

"Evaluación del impacto en la protección de datos" es una herramienta y un proceso para evaluar los impactos sobre la protección de los interesados en el tratamiento de sus datos, y para identificar acciones correctivas para evitar o minimizar tales impactos. (*)

"Oficial de Protección de Datos" significa el funcionario del ACNUR en la División de Protección Internacional, que supervisa, monitorea e informa sobre el cumplimiento global de la Política. (*)

"Intercambio de datos" significa cualquier acto de transferir o hacer que los datos personales de las personas de interés sean accesibles en las oficinas del ACNUR o entre oficinas del ACNUR, o a un socio del ACNUR o un tercero.

"Titular de los datos" significa una persona que está contemplada dentro del ámbito de la Política de Protección de Datos y cuyos datos personales son objeto de tratamiento por parte del ACNUR. (*)

"Acuerdo de transferencia de datos" es un acuerdo entre el ACNUR y un tercero que establece los términos y las condiciones del uso de los datos personales, incluidos los conjuntos de datos específicos que se compartirán, el modo de transferencia de datos, para qué fines se pueden usar los datos, las medidas de seguridad de los datos y otros temas relacionados. (*)

"Expediente del caso individual" es el depósito central de los datos relacionados con una persona de interés específica, ya sea en formato impreso o electrónico, incluida toda la correspondencia pertinente creada y recibida por el ACNUR. Esto incluye, por ejemplo, formularios de solicitud de asilo; evaluaciones de necesidades de protección; formularios de registro; Formularios de solicitud de Determinación de la Condición de Refugiado (RSD, por sus siglas en inglés); formularios firmados de consentimiento y/o divulgación; transcripciones de entrevistas y notas de asesoramiento; documentos producidos por Personas de Interés (POC, por sus siglas en inglés) y familiares dependientes; solicitudes e informes de visitas a domicilio; documentos médicos (tales como formularios de evaluación médica); documentos de dietas; copias de las Evaluaciones del Interés Superior y las Determinaciones del Interés Superior y los pasos procedimentales relacionados; Formularios de Registro de Reasentamiento (RRF, por sus siglas en inglés); correspondencia con los socios, incluidas las autoridades gubernamentales y los países de reasentamiento; cualquier correo electrónico impreso u otra correspondencia relacionada con el caso.

"Agencia Implementadora" significa 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 (PPA, por sus siglas en inglés) con el fin de llevar a cabos la implementación de actividades programáticas dentro de su mandato. (*)

"Socio operacional" significa una organización que no recibe fondos del ACNUR, pero con la cual el ACNUR coopera y colabora para brindar protección y asistencia a las personas de interés, lo que podría incluir el intercambio de datos agregados/estadísticos y/o personales para facilitar una asistencia y prestación de servicios eficiente y evitar la duplicación de esfuerzos humanitarios.

"Datos personales" significa cualquier dato relacionado con un individuo que podría ser identificado con base en esos datos; y otra información; o por medios razonablemente factibles de ser utilizados en relación con esos 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 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" significa una violación de la seguridad de los datos que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o accidental o ilegal/ilícita de datos personales transferidos, almacenados o de otro modo procesados. (*)

"Persona de interés" significa una persona cuyas necesidades de protección y asistencia son de interés para el ACNUR. Esto incluye a las personas refugiadas, solicitantes de asilo, apátridas, desplazadas internas y retornadas. (*)

"Tratamiento de datos personales" significa cualquier operación o conjunto de operaciones que se realiza con relación a los datos personales o conjuntos de datos personales, ya sea por medios automatizados o no, tales como la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, uso, divulgación por transmisión, difusión o puesta a disposición de cualquier parte, alineación o combinación, restricción, borrado o destrucción. (*)

"Seudonimización" significa modificar los datos para que permanezcan asociados a un titular de los datos en particular sin que ese individuo sea identificado. Esto se hace asignando códigos de referencia o seudónimos a titulares de datos en lugar de sus datos de identificación personal. Estos códigos se guardan por separado y están sujetos a medidas técnicas y organizativas para garantizar que los datos no sean atribuibles a un titular de datos identificado o identificable.

"Solicitud de acceso del titular" significa una solicitud de una persona de interés, o su representante legal, para obtener información del ACNUR sobre los datos personales que tienen sobre ella y cualquier solicitud asociada para modificar o eliminar dicha información. También se pueden recibir solicitudes de acceso de los miembros de la familia con respecto a los datos contenidos en los archivos del ACNUR.

"Terceros" significa cualquier persona física o jurídica distinta al titular de los datos, el ACNUR o una agencia implementadora. Los ejemplos de terceros incluyen gobiernos nacionales, organizaciones internacionales gubernamentales y no gubernamentales, entidades del sector privado o individuos. (*)

"Personal del ACNUR" significa todas las personas que trabajan para el ACNUR, incluidos los miembros del personal, la fuerza laboral afiliada (consultores, el personal desplegado, los Voluntarios de las Naciones Unidas, etc.) y los pasantes.

1.5. Siglas

Esta guía también utiliza las siguientes abreviaturas:

BIMS (por sus siglas en inglés) Sistema de Gestión de Identidad Biométrica

CEPD Consejo Europeo de Protección de Datos

DIP (por sus siglas en inglés) División de Protección Internacional

DIST (por sus siglas en inglés) División de Sistemas de Información y Telecomunicaciones

DPIA (por sus siglas en inglés) Evaluación de impacto de protección de datos

DPO (por sus siglas en inglés) Oficial de Protección de Datos

FICSS (por sus siglas en inglés) Sección de Apoyo a la Información y la Coordinación en el Terreno

FSS (por sus siglas en inglés) Sección de Seguridad en el Terreno

ICDPPC (por sus siglas en inglés) Conferencia Internacional de Autoridades de Protección de Datos y Privacidad

IMRS (por sus siglas en inglés) Sección de Gestión y de la Identificación y Registro

IPMS (por sus siglas en inglés) Servicio de Gestión de Agencias Implementadoras

ISO (por sus siglas en inglés) Organización Internacional de Normalización

LAS (por sus siglas en inglés) Servicio de Asuntos Jurídicos

OIG Oficina del Inspector General

POC (por sus siglas en inglés) Personas de interés

PNSS (por sus siglas en inglés) Sección de Protección y Seguridad Nacional

PPA (por sus siglas en inglés) Acuerdo de Colaboración para Proyectos

PPD Política de Protección de Datos

RAS (por sus siglas en inglés) Sección de Archivos y Expedientes

RGPD Reglamento general de protección de datos de la Unión Europea

RSD (por sus siglas en inglés) Determinación de la Condición de Refugiado

TIC Tecnologías de la información y la comunicación

VSG Violencia Sexual y de Género

1.6. Estructura de la Guía

Esta Guía sigue esencialmente la estructura de la Política de Protección de Datos en el orden en que se tratan los principios básicos de protección de datos. Algunos principios básicos requieren más explicación y ocupan más dedicación que otros, es decir, el tratamiento legítimo y justo, los derechos de los titulares de los datos, la seguridad de los datos y la rendición de cuentas. Por consiguiente, la Guía aborda estos en secciones separadas. Otros principios se tratan conjuntamente en una sección. Además, debido a su importancia, varios conceptos y tipos de tratamiento de datos también son abordados en secciones separadas, es decir, datos personales, filtraciones de datos, evaluaciones de impacto y transferencias de datos. A lo largo de la Guía, se hace referencia a la Política de Protección de Datos para mostrar el estrecho vínculo entre ambos documentos y resaltar qué aspectos abarca la Política obligatoria. Otras fuentes se mencionan en las notas a pie de página.

2. Datos personales y datos anonimizados y seudonimizados

2.1. Datos personales

2.1.1 Al limitar su alcance a los **datos personales**, la PPD sigue deliberadamente un concepto y una noción establecidos en la legislación internacional y regional de protección de datos. La definición de datos personales en la PPD (párr. 1.4) debería ser equivalente a la definición común de "toda información sobre una persona física identificada o identificable ('titular de los datos')" (traducción libre).[2] La orientación y la interpretación fidedignas proporcionadas en esta definición, por ejemplo por el Tribunal Europeo de Derechos Humanos, el Consejo Europeo de Protección de Datos (CEPD), y el antiguo Grupo de Trabajo del Artículo 29, son, por lo tanto, también relevantes para la interpretación de la PPD del ACNUR.

2.1.2 Para determinar si una persona física es identificable, debe tenerse en cuenta todos los medios con probabilidades razonables de ser utilizados, como identificar a una persona directa o indirectamente. La **identificación** requiere elementos que describen a una persona de tal manera que sea distinguible de todas las otras personas y reconocible como un individuo. El nombre de una persona es un buen ejemplo. Sin embargo, en ciertos entornos, la referencia a una posición (por ejemplo, el jefe de una organización) puede ser suficiente y calificar como datos personales. En otros contextos, los nombres pueden no ser suficientes para establecer la identidad de una persona y se necesitan identificadores adicionales, como la fecha y el lugar de nacimiento, números personalizados o, cada vez más, datos biométricos.

2.2. Anonimización

2.2.1 En el párr. 1.3.1, la PPD menciona datos agregados o anonimizados como ejemplos que **no están contemplados dentro del ámbito de la Política,** pero no desarrolla la noción; la seudonimización no se menciona en la Política. Esta Guía ofrece una definición de ambos, anonimización y seudonimización, y una explicación adicional a continuación.

2.2.2 El punto y la característica de la anonimización es que un conjunto de datos personales ha sido **modificado irreversiblemente de tal manera que el titular de los datos ya no es identificable**. No se puede dejar ningún elemento en la información que podría, mediante el ejercicio de un esfuerzo razonable, servir para volver a identificar a la persona interesada. Donde los datos han sido **anonimizados con éxito, ya no son datos personales**. Con respecto a las técnicas de anonimización, los controladores de datos y

[2] Véase el Consejo de Europa, *Convención para la Protección de las Personas en relación al Tratamiento Automático de Datos Personales*, 28 de enero de 1981, CETS No. 108, en su forma enmendada por su Protocolo, 25 de junio de 2018, CETS No. 223 (Convenio Modernizado 108), disponible en inglés y francés en: https://rm.coe.int/16808ade9d, Artículo 2 (a); Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo sobre la protección de las personas físicas en relación con el tratamiento de datos personales y la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*, 27 de abril de 2016, disponible en inglés en: https: // eur-lex.europa.eu/legal-content/EN/TXT/PDF/ uri=CELEX:32016R0679&from=EN, Artículo 4 (1); y Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (ICDPPC), *Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid)*, 5 de noviembre de 2009, disponible en: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf, Parte I 2.a.

procesadores de datos del ACNUR deben verificar que producen el resultado deseado.[3] Cuando se carece de los conocimientos especializados necesarios, se alienta a los funcionarios responsables a ponerse en contacto con la División de Sistemas de Información y Telecomunicaciones (DIST) y/o solicitar asesoramiento adicional al Oficial de Protección de Datos (DPO).

2.3. Seudonimización

2.3.1 La anonimización debe distinguirse de la seudonimización, que desactiva la identificación al **reemplazar los identificadores con un seudónimo**. La seudonimización se logra, por ejemplo, mediante la encriptación de los identificadores en los datos personales; un ejemplo común en el ACNUR es el uso de números de registro o identidad en lugar de los nombres de las personas de interés. **Los datos seudonimizados siguen siendo datos personales para aquellos autorizados a utilizar la clave de descifrado**, que permite la reidentificación. Para todos aquellos que no poseen la clave de desencriptación, los seudonimizados aún pueden identificarse, pero con dificultad, es decir, no con los medios con los que es razonablemente probable que se utilicen. Sin embargo, la seudonimización a menudo es una buena práctica ya que ofrece un cierto nivel de protección de datos dependiendo de las circunstancias operacionales concretas.

2.4. Datos agregados

2.4.1 Con respecto a los datos agregados que se derivan de los datos personales, la gestión inadecuada podría, en determinadas circunstancias, presentar riesgos para las personas de interés para el ACNUR. Este es el caso, por ejemplo, cuando los datos agregados son **combinados con otros conjuntos de datos o son sometidos a la verificación de datos** u otras técnicas que transforman los datos anonimizados en datos personales, para que las personas sean identificables. Esto debe equipararse con nombrar a un individuo. Para la identificación, puede ser suficiente poder establecer una conexión confiable entre elementos de datos particulares y un individuo conocido.

2.4.2 Sin embargo, incluso cuando la anonimización se lleva a cabo de manera efectiva, y la política de protección de datos ya no es aplicable, se le recuerda al personal del ACNUR los **riesgos de protección inherentes a utilizar, y en particular compartir y publicar, datos agregados**. Por ejemplo, existe el riesgo de que los conjuntos de datos divulguen la ubicación real de grupos pequeños o "en situación de riesgo", por ejemplo, mediante el mapeo de datos como el país de origen, la religión o vulnerabilidades específicas a las coordenadas geográficas. Estrechamente relacionado está el aspecto de que los datos agregados, por ejemplo, sobre la VSG u otros incidentes de protección, solo deben compartirse si existe un número suficiente de incidentes totales (generalmente más de 50) y no deben desglosarse por edad, sexo, área geográfica o cualquier otros puntos de datos donde no existe un volumen suficiente de incidentes para garantizar que no

[3] Véase, por ejemplo, Grupo de trabajo sobre protección de datos del artículo 29, *Dictamen 05/2014 sobre Técnicas de Anonimización*, Documento de trabajo 216, adoptado el 10 de abril de 2014, disponible en inglés en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommenda-tion/files/2014/wp216_en.pdf; y Oficina del Comisionado de Información del Reino Unido, *Anonimización: Gestión del riesgo de protección de datos - código de práctica*, noviembre de 2012, disponible en inglés en: https://ico.org.uk/media/1061/anonymisation-code.pdf.

puedan ser rastreados a individuos o ubicaciones geográficas.[4] Estas consideraciones son impulsadas por imperativos de protección general, relacionados con la prevención del daño físico, la estigmatización, la discriminación, la intimidación o prácticas xenófobas a grupos o individuos, la criminalización, el racismo o poner en peligro las relaciones con las comunidades de acogida.

2.4.3 Si el intercambio o la publicación de datos anónimizados podrían presentar riesgos de protección, el ACNUR puede concertar un **acuerdo formal con los socios o las organizaciones de investigación** con quien se comparten los datos, estableciendo los términos y las condiciones para el uso de los datos, incluida la obligación de mantener la confidencialidad del conjunto de datos e impedir el acceso no autorizado. También se pueden incluir disposiciones para que el ACNUR revise el material antes de su publicación. Las operaciones deben buscar el apoyo de los Oficiales regionales de Gestión de la Información, de estar disponibles, o de la Sección de apoyo a la Información y la Coordinación (FICSS) y el Oficial de Protección de Datos (DPO) en la Sede, cuando sea necesario.

3. Tratamiento legítimo y justo

En esta sección, la Guía proporciona explicaciones breves del principio de tratamiento legítimo y justo, orientación para la comprensión de cada base legítima, ejemplos de contextos típicos del ACNUR y orientación para la elección de la base legítima apropiada. La búsqueda del consentimiento/asentimiento de las niñas y los niños y de las personas con condiciones de salud mental y discapacidades intelectuales se abordan por separado al final de esta sección.

3.1. Introducción

3.1.1 Según el párr. 2.2 de la PPD, el tratamiento de datos personales solo puede llevarse a cabo sobre una base legítima y de manera justa y transparente. La necesidad de una **base legítima**, también conocido como tratamiento legítimo, tiene su origen en las normas de Derechos Humanos que requieren de una base legítima para cualquier interferencia con el derecho al respeto de la vida privada del titular de los datos.[5] Considerando la naturaleza del ACNUR como entidad de las Naciones Unidas que se beneficia de privilegios e inmunidades, se eligió el término "base legítima" en lugar de fundamento jurídico o legalidad. A efectos del tratamiento de datos personales por parte del ACNUR, la PPD como una Política del Alto Comisionado es el documento fuente apropiado para identificar las bases legítimas.

[4] Véase acerca de este y otros aspectos en esta sección: ACNUR, *Anuario estadístico del 2015, Capítulo 6: De la protección de datos a la estadística*, disponible en inglés en: http://www.unhcr.org/56655f4c21.html; véase también Grupo de las Naciones Unidas para el Desarrollo (GNUD), *Privacidad de datos, ética y protección, Nota de orientación sobre grandes datos para alcanzar la Agenda 2030*, 2017, disponible en inglés en: https://undg.org/wp-con-tent/uploads/2017/03/UNDG-Big-Data-Guidance-Note.pdf y Oficina del Alto Comisionado para los Derechos Humanos, *Un enfoque de datos basado en los derechos humanos: No dejar a nadie atrás en la Agenda 2030 para el Desarrollo, Nota de orientación para la recopilación y desagregación de datos*, 2018, disponible en inglés en: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproach-toData.pdf.

[5] Véase el Comité de Derechos Humanos de las Naciones Unidas (CDH), *Observación general No. 16 del CCPR: Artículo 17 (Derecho a la privacidad), El derecho al Respeto de la Privacidad, la Familia, el Hogar y la Correspondencia, y la Protección del Honor y la Reputación*, 8 de abril de 1988, disponible en inglés en: http://www.refworld.org/docid/453883f922.html, párr. 3 y 8.

3.1.2 El PPD también aclara que el ACNUR (solo) puede procesar datos personales basados en una o más de las bases legítimas mencionadas anteriormente. Por ejemplo, el tratamiento de datos personales en el interés vital o superior de las personas de interés también estaría cubierto por el mandato del ACNUR. Sin embargo, la Política **no establece una jerarquía explícita de bases legítimas,** aunque la relevancia de cada una puede deducirse del orden en que se enumeran en el párr. 2.2 de la PPD: (i) consentimiento - (ii) interés vital o superior - (iii) mandato del ACNUR - (iv) más allá del mandato del ACNUR, para garantizar la protección y seguridad de las personas. La Política tampoco proporciona orientación sobre qué base legítima se aplica en qué situación. Solo el párr. 2.2 (iv) de la PPD ("Más allá del mandato del ACNUR, para garantizar la protección y seguridad de las personas...") indica que las otras bases legítimas (consentimiento y el interés vital o superior) están destinadas a cubrir actividades de tratamiento de datos personales *dentro del* mandato del ACNUR.

3.1.3 El elemento **equidad** en general requiere que el ACNUR sea transparente, lo que significa que sea claro y abierto con las personas de interés como titulares de los datos sobre cómo se usará su información. Este aspecto, también denominado principio de transparencia, está cubierto esencialmente por la PPD del ACNUR en lo que respecta al derecho a la información del titular de los datos (párr. 3.1 de la PPD). En este párrafo, la PPD enumera en los puntos (i) a (viii) toda la información relevante que debe proporcionarse al recopilar datos personales. Respetar el derecho a la información es, por lo tanto, acorde con el principio de transparencia. Otros aspectos de la equidad se refieren al tratamiento de datos personales solo de forma que las personas de interés razonablemente podrían esperar del ACNUR, no utilizando datos de manera que podrían tener un impacto injustificadamente adverso o discriminatorio en ellas y prestando especial atención al procesar datos particularmente sensibles (como los datos médicos, datos relativos a la condena o sospecha de delitos, la identidad de los testigos, las personas que viven en la clandestinidad debido a amenazas a su seguridad, o información relacionada con la orientación sexual o la pertenencia a una comunidad minoritaria religiosa o étnica).

3.2. Consentimiento

3.2.1 El **consentimiento** es la base legal más utilizada y a menudo la preferida para el tratamiento de datos personales. Sin embargo, dada la vulnerabilidad de la mayoría de los beneficiarios y la naturaleza de las emergencias humanitarias, muchas organizaciones humanitarias no estarán en una posición para poder contar con el consentimiento para la mayoría de su tratamiento de datos personales[6]. Si el consentimiento es o no es la base legítima apropiada depende de un análisis detallado y una profunda comprensión de cada situación. La imparcialidad y el respeto por los derechos de las personas requiere que el ACNUR aplique el consentimiento siempre que la situación le permita a la persona ejercer su elección de forma libre e informada. Ejemplos típicos del trabajo del ACNUR para los procedimientos que requieren el consentimiento del individuo son: el registro (véase abajo, sin embargo, bajo el mandato del ACNUR), RSD, la repatriación voluntaria, el reasentamiento, la asistencia, evaluaciones de necesidades, el rastreo y la gestión de casos de VSG.

[6] Comité Internacional de la Cruz Roja (CICR), *Manual sobre protección de datos en la acción humanitaria*, junio de 2017, disponible en inglés en: https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action, Capítulo 3, página 45, párr. 3.2.

3.2.2 Basado en la definición en el párr. 1.4 de la PPD, para que el consentimiento constituya una base legítima viable, debe ser manifestado libremente y de manera informada. **Manifestado libremente** significa que el individuo tiene una elección genuina y puede rechazar o retirar el consentimiento sin consecuencias adversas. En situaciones de emergencia, pero también con respecto al acceso a la asistencia (alimentos, efectivo) y en ausencia de otras fuentes viables de ingresos, esta condición podría no cumplirse debido a que las personas refugiadas u otras personas de interés podrían no ver otra alternativa a aceptar que sus datos se recopilen y se comparten con los socios. Cualquier coacción o influencia indebida es incompatible con la condición de consentimiento otorgado libremente.

3.2.3 El consentimiento **informado** requiere que el titular de los datos reciba explicaciones, lo que permite una apreciación y comprensión completas de las circunstancias, los riesgos y los beneficios del tratamiento. Los factores tales como la edad, el género, el nivel de educación, la salud o la discapacidad pueden afectar la capacidad de una persona para comprender las consecuencias del tratamiento de datos y deben tenerse en cuenta en la forma en que se proporciona la información (véase también a continuación: Buscar el consentimiento /asentimiento de las niñas y niños, y de personas con condiciones de salud mental y discapacidades intelectuales). La información debe proporcionarse en un lenguaje sencillo sin jerga técnica, pero completo, con un nivel de detalle lo suficiente para permitir que el titular de los datos pueda apreciar claramente los flujos de datos futuros, incluidos los riesgos y las consecuencias que el ACNUR conoce. Para ser completa, la información debe abarcar todas las actividades de tratamiento de datos previstas que se llevarán a cabo, especialmente qué conjuntos de datos o elementos se compartirán o se transferirán con el gobierno de acogida, las agencias implementadoras u otros terceros.

3.2.4 La definición de consentimiento en la PPD también aclara que el consentimiento puede ser otorgado por medio de una **declaración escrita u oral o por una clara acción afirmativa**. Ejemplos de consentimiento por escrito son el Formulario de Repatriación Voluntaria y el Formulario de Registro de Reasentamiento (Sección 8 del DRR: Declaración). Además de los procesos establecidos, como el registro, la determinación de la condición de refugiado, el reasentamiento, la repatriación voluntaria y la gestión de casos de violencia sexual y de género, la responsabilidad de establecer procedimientos de consentimiento apropiados sigue recayendo en el controlador de datos. Cualquiera que sea el método para otorgar el consentimiento, esta Guía fomenta el registro apropiado del consentimiento, por ejemplo, en una transcripción de entrevista, como nota para el archivo o en una grabación de audio.

3.3. Interés vital o superior

3.3.1 Cuando el consentimiento no se puede obtener de manera válida, los datos personales aún pueden procesarse si es de interés vital para el titular de los datos, es decir, cuando el tratamiento de datos es **necesario para proteger un interés que es esencial para la vida, la integridad, la salud, la dignidad o la seguridad del interesado**[7]. El interés superior se refiere al principio establecido en el artículo 3 (1) de la Convención sobre los Derechos del Niño y puede utilizarse como base legítima cuando el

[7] Véase CICR, *Manual sobre protección de datos en acción humanitaria*, Capítulo 3, página 48, párr. 3.3.

tratamiento de los datos personales de las niñas y niños responde a su interés superior. Para el ACNUR, esto requeriría la realización adecuada de un procedimiento de interés superior (ver también a continuación: Buscar el consentimiento/asentimiento de las niñas y los niños).

3.3.2 Algunos **ejemplos** incluyen: asistencia urgente y vital en las etapas preliminares de una respuesta a gran escala/de emergencia, el tratamiento de datos de las personas de interés que no pueden dar su consentimiento debido a su estado de salud (incluida la inconsciencia) o que no tienen la capacidad para ello (incluso debido a condiciones de salud mental y discapacidades intelectuales), para garantizar la liberación de una persona de interés de la detención o de una instalación similar, cuando el ACNUR no tiene acceso para obtener el consentimiento directamente de la persona y el tratamiento de datos personales relacionados a las niñas o niños no acompañados o separados en beneficio de su interés superior.

3.4. Lograr que el ACNUR pueda cumplir su mandato

3.4.1 Con el objetivo de procesar los datos personales de las personas de interés, el mandato del ACNUR tal y como se establece en su Estatuto y se enmienda en las resoluciones posteriores de la Asamblea General de las Naciones Unidas[8] puede considerarse una base legítima. La noción general de esta categoría de base legítima es la de 'motivos importantes de interés público'[9]. Se activan importantes motivos de interés público **cuando la actividad en cuestión es parte de un mandato humanitario establecido en virtud del derecho internacional**[10]. Los casos donde esta base legítima puede ser relevante incluyen la distribución de asistencia, cuando podría no ser factible obtener el consentimiento de todos los posibles beneficiarios, y cuando podría no estar claro si la vida, la seguridad, la dignidad y la integridad de las personas de interés estén en juego, es decir, cuando la base de interés vital o superior no se aplicaría.

3.4.2 Algunos **ejemplos** para contar con esta base legítima son: el registro y la RSD bajo mandato, cuando este es un requisito previo para el trabajo del ACNUR en la prestación de protección y asistencia a las personas de interés; la transferencia rutinaria de datos biográficos básicos a los gobiernos de acogida, cuando así lo requiera un acuerdo del país del país de acogida o un memorando de entendimiento (MOU); el tratamiento de datos para anonimizar o seudonimizar; el tratamiento de datos para combatir el fraude cometido por las personas de interés, o cuando las personas de interés estén implicados en un caso de posible mala conducta por parte de cualquier persona o entidad con un vínculo contractual con el ACNUR; el mantenimiento de la seguridad de la información de las bases de datos del ACNUR y la infraestructura de TIC; cuando los datos se proporcionan al ACNUR por parte de socios o terceros con fines de protección o asistencia; o el tratamiento de datos para archivarlos.

[8] Véase ACNUR, *Nota sobre el mandato del Alto Comisionado para los Refugiados y su Oficina*, octubre de 2013, disponible en: http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=52f0fe9b4.

[9] Véase, por ejemplo, el artículo 6 (1) (e) del RGPD (Reglamento General de Protección de Datos) que reconoce como tratamiento legítimo cuando el tratamiento es "necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".

[10] Véase CICR, *Manual sobre la protección de datos en la acción humanitaria*, Capítulo 3, página 49, párr. 3.4.

3.5. Más allá del mandato del ACNUR, para garantizar la protección y la seguridad de las personas de interés u otras personas

3.5.1 Esta base legal se encuentra **en correlación directa con los párrs. 6.3 y 6.4 de la PPD** relativa a la transferencia de datos personales a organismos nacionales e internacionales encargados de hacer cumplir la ley y a tribunales y cortes. Otros ejemplos podrían incluir: medidas adoptadas para que el ACNUR responda de manera efectiva a las filtraciones de datos personales (si las medidas irían más allá del mandato); implementación de procedimientos de gestión de seguridad que son necesarios para garantizar la seguridad de las personas de interés, el personal del ACNUR y otros, en particular en el contexto de una amenaza grave y continua para la seguridad; y medidas tomadas en el contexto de investigaciones formales sobre posibles conductas indebidas por cualquier persona vinculada contractualmente a la ONU, incluyendo posibles abusos y explotación sexual, en particular si buscar el consentimiento podría comprometer la integridad de la investigación y/o exponer a las víctimas u otras personas a daños.

3.6. Determinar la base legítima apropiada

3.6.1 De acuerdo con el párrafo 7.2.2 (i) de la PPD, la responsabilidad de determinar la base legítima aplicable para los fines específicos y legítimos del tratamiento de datos corresponde al controlador de datos, asistido por el punto focal de protección de datos. En caso de que surgen preguntas, el Oficial de Protección de Datos (DPO) puede ser consultado (párr. 7.2.3). Aparte de la **necesidad fundamentada** de procesar datos personales basada en la base legítima apropiada, la **relevancia práctica** de su determinación a menudo radica en decidir si se requiere o no el consentimiento. Cuando el consentimiento es la base legitima relevante, la consecuencia de denegar o retirar el consentimiento es que los datos personales no deben procesarse. Además, cuando se determina que el consentimiento no es la base legítima apropiada, el ACNUR deberá asumir una mayor responsabilidad en la evaluación de los riesgos y beneficios o el tratamiento, sobre todo cuando se trata de nuevas tecnologías y en situaciones caracterizadas por flujos de datos complejos y múltiples partes interesadas[11]. Además, el ACNUR aun así está obligado a ejercer la debida diligencia y evaluar el impacto del tratamiento de datos una vez que se obtiene el consentimiento como requisito general del mandato de protección del ACNUR.

3.6.2 También debe tenerse en cuenta que obtener el **consentimiento no es lo mismo que proporcionar información** sobre el tratamiento de datos. El primero es una base legítima, el último un derecho individual del titular de los datos y la consecuencia del principio de transparencia que debe respetarse independientemente de la base legítima para el tratamiento. Finalmente, el derecho a objetar según el párr. 3.4 de la PPD también debe respetarse cuando el tratamiento de datos personales se basa en bases legítimas distintas del consentimiento, no obstante, dentro de los límites establecidos en el párr. 3.4 y 3.7 de la PPD.

[11] CICR, *Manual sobre la protección de datos en la acción humanitaria*, Capítulo 3, página 45, Sección 3.2.

3.7. Buscar el consentimiento/asentimiento de las niñas y los niños

3.7.1 Las **niñas y niños** requieren protección específica y son una categoría particularmente vulnerable de titulares de datos. Puede que estén menos conscientes de los riesgos y las consecuencias, así como de las garantías y los derechos relacionados con el tratamiento de sus datos. Con respecto a la base legítima para procesar los datos personales de las niñas y lo niños, en la mayoría de las situaciones el consentimiento puede y debe obtenerse de los padres de la niña o el niño, de un miembro de la familia con la patria potestad, o del cuidador legal o habitual.

3.7.2 Sin embargo, en el caso de las niñas o niños no acompañados o separados, o cuando los padres y/o el cuidador de la niña o niño pueden ser el origen de riesgos o daños para estas personas menores de edad, el ACNUR y sus socios se encuentran en una situación en que ciertas acciones, especialmente los procedimientos del interés superior requieren el tratamiento de los datos personales de la niña o niño. En tales situaciones, el consentimiento de la niña o niño puede seguir siendo la base legítima apropiada siempre que ella/él tenga la capacidad de comprender el proceso y sus derechos y obligaciones consiguientes. Por lo tanto, el utilizar el **consentimiento de la niña o niño** requiere una evaluación de la capacidad evolutiva, incluida la edad, el nivel de madurez y el desarrollo, y/u otros factores. También puede ser necesario tener en cuenta las normas jurídicas nacionales aplicables, por ejemplo, cuando se trabaja con las autoridades nacionales o se requiere su aprobación.

3.7.3 En el caso de las personas menores de edad que no pueden dar su consentimiento, el ACNUR puede procesar sus datos personales basándose en "los intereses vitales o superiores de la persona interesada" (párr. 2.2 (ii) de la PPD). Sin embargo, e independientemente de esta base legítima, cuando la persona menor de edad puede comprender y aceptar participar en servicios o actividades, se debe solicitar un asentimiento informado. **Asentir** es la voluntad y las opiniones expresadas por una niña o niño para participar en servicios o actividades, por ejemplo, para participar en una actividad de protección infantil, recibir atención médica o beneficiarse de la asistencia.

3.7.4 Al recopilar datos personales de niñas y niños, el personal del ACNUR debe esforzarse por garantizar que se lleve a cabo en un **ambiente amigable para las niñas y niños y que los procedimientos** se lleven a cabo por personal con conocimientos y experiencia en el trabajo con niñez. Las entrevistas se deben realizar de una manera sensible a la edad y al género, teniendo en cuenta el nivel de desarrollo y madurez, así como las circunstancias y necesidades individuales y contextuales de la persona menor de edad. Cualquier comunicación sobre el tratamiento de datos debe hacerse en un lenguaje claro y sencillo y preferiblemente en múltiples formatos (por ejemplo, visual, de audio y fácil de leer).

3.8. Buscar el consentimiento de personas con condiciones de salud mental y discapacidades intelectuales

3.8.1 Las personas de interés con discapacidades, incluidas las que tienen condiciones de salud mental y discapacidades intelectuales, tienen los mismos derechos para tomar decisiones con respecto al uso de sus datos personales que otras personas. El personal del ACNUR debe asumir, salvo que se indique lo contrario, que estas personas tienen la **capacidad para dar consentimiento** y seguir sus procedimientos regulares para obtener y registrar el consentimiento, adaptados a las necesidades y preferencias de comunicación del individuo, y otras necesidades de apoyo.

3.8.2 Puede que los **métodos de comunicación** necesitarán ser adaptados para personas con discapacidades, dependiendo de sus preferencias de comunicación. Algunos podrían requerir apoyo y asistencia adicional en situaciones en las que se recopilan datos personales. Cuando el personal del ACNUR no está seguro sobre la capacidad de una persona para comprender el proceso y sus correspondiente derechos y obligaciones, debe involucrar a un supervisor (u otro colega con experiencia relevante) para considerar apoyo adicional y poder determinar la voluntad y preferencias de la persona. El ACNUR puede solicitar el permiso de la persona para incluir a un cuidador u otra persona de apoyo, si esto se considera seguro. Esta persona puede facilitar el entendimiento o la comunicación y debe usarse para apoyar la capacidad de la persona de comprender y dar su consentimiento (en lugar de una forma de sustitución de la toma de decisiones). Si se determina que una persona no puede comprender adecuadamente el proceso, y sus correspondientes derechos y obligaciones, el personal del ACNUR puede decidir procesar los datos sobre una **base legítima alternativa, tal como el interés vital y superior**.

4. Otros principios de protección de datos

4.1. Especificación del propósito

4.1.1 El principio de especificación del propósito, también conocido como el principio de limitación del propósito, es **uno de los principios claves** en el campo de la protección de datos. Está vinculado a otros principios, en particular con los principios de la base legítima, la necesidad y la proporcionalidad, el derecho a la información, la seguridad de los datos y la rendición de cuentas. **Sin claridad sobre el (los) propósito(s) específico(s) para el tratamiento de datos** es difícil o imposible determinar la base legítima apropiada, los elementos de datos necesarios mínimos para ser procesados, informar plenamente al titular de los datos, establecer las medidas de seguridad de datos necesarias y que los controladores de datos tomen decisiones responsables.

4.1.2 La Política de Protección de Datos solo aborda el principio en un párrafo. En el párr. 2.3 de la PPD, se hace referencia a la necesidad de que el (los) propósito(s) para la recopilación sean (i) específicos, y (ii) legítimos. Además, no debe haber **ningún tratamiento que sea incompatible con tal(es) propósito(s)**. La Política también establece que corresponde al controlador de datos, asistido por el punto focal de protección de datos, determinar el (los) propósito(s) específico(s) y legítimo(s) del tratamiento de datos (párr. 7.2.2 de la PPD). A continuación, se proporciona orientación adicional para la comprensión adecuada de este principio, incluidos algunos ejemplos prácticos.

4.1.3 Los controladores de datos deben determinar y manifestar el o los propósitos específicos **antes** de la recopilación de los datos personales[12]. En particular en el caso de grandes grupos poblacionales donde el contacto directo con las personas de interés es escaso y difícil, se recomienda a las operaciones del país que reflexionen cuidadosamente sobre todos los propósitos específicos, especialmente las transferencias a socios y terceros con suficiente antelación con el fin de proporcionar esta información a los titulares de datos, por ejemplo, en el momento del registro.

4.1.4 Con respecto al nivel de especificidad, la asesoría es ser **tan específico como sea razonablemente posible**. Por ejemplo, en lugar de referirse a la protección de las personas refugiadas, es necesario establecer claramente las actividades precisas, tales como la emisión de certificados de personas solicitantes de asilo, la realización de evaluaciones de necesidades o el monitoreo de la situación de las personas solicitantes de asilo detenidos. Del mismo modo, en lugar de referirse a los tipos generales de asistencia (por ejemplo, dinero en efectivo o alimentos), se recomienda a los controladores de datos que especifiquen los propósitos, tales como la autenticación en el punto de recolección de alimentos o efectivo o el seguimiento posterior a la distribución. Esto no solo es importante para cumplir con el requisito de consentimiento informado y el derecho a ser informado (párr. 3.1 (i) de la PPD) pero también para reflejar los propósitos específicos en los acuerdos de transferencia de datos (como se requiere en el párr. 6.2.2 (i) y 6.1.2 (ii) de la PPD).

4.1.5 La legitimidad de los propósitos no debe equipararse con el principio de base legítima. Propósitos legítimos para el ACNUR son aquellos que son **compatibles con su mandato** en el sentido amplio, que incluye, por ejemplo, la prestación de buenos oficios. Por otra parte, lo que es legítimo para un tercero puede no serlo para el ACNUR.

4.1.6 El tratamiento posterior debe ser compatible con los propósitos iniciales. Esto lógicamente se desprende de la Política. Los nuevos propósitos requieren una nueva base legítima. La "desviación de uso", o una situación en la que los mismos sistemas y/o conjuntos de datos se utilizan para otros fines que los originalmente designados, sería incompatible con el principio de especificación del propósito. Típicos **ejemplos para fines compatibles** son el uso de datos personales por el controlador de datos para las estadísticas, el archivado y la investigación científica o histórica[13]. En el contexto específico del ACNUR, el tratamiento de datos personales para una solución como el reasentamiento o la repatriación voluntaria no comunicada previamente al titular de los datos requiere una

[12] Véase el Grupo de trabajo sobre protección de datos del artículo 29, *Opinión 03/2013 sobre la limitación del propósito*, Documento de trabajo 203, adoptado el 2 de abril de 2013, disponible en inglés en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[13] Véase el Artículo 5 (b) del RGPD.

nueva base legítima, es decir, el consentimiento. El ofrecer un nuevo tipo de asistencia o servicio también sería un nuevo propósito que requiere una nueva base legítima, aunque no necesariamente el consentimiento. Sin embargo, reemplazar un socio de proyecto existente por un nuevo socio para un proyecto idéntico podría considerarse un propósito compatible. Podría estar **dentro de las "expectativas razonables" de las personas de interés** que el ACNUR proceda de esa manera siempre que no haya dudas válidas sobre la aceptación del socio. En tales escenarios, se alienta al ACNUR a actualizar la información que proporciona a las personas de interés y comunicar los cambios programáticos a través de comités y otros foros de comunicación para garantizar que las personas de interés estén informadas del cambio y puedan optar por no intercambiar datos si así lo desean.

4.2. Necesidad y proporcionalidad

4.2.1 El principio de necesidad y proporcionalidad está **estrechamente relacionado con el principio de especificación del propósito**. Lo que es necesario y proporcionado en términos del tratamiento de datos necesita ser evaluado en función de los propósitos específicos y legítimos. La Política aclara que "los datos que se procesan deben ser adecuados y pertinentes a la finalidad identificada, y no deben exceder ese propósito" (párr. 2.4 de la PPD). El principio también se conoce como el principio de '**minimización de datos**.[14]

4.2.2 Ya sea para fines de recopilación de datos internos o para decidir qué datos pueden transferirse a terceros, el personal del ACNUR siempre debe tratar de limitar o minimizar los elementos de datos personales a los que son necesarios para los propósitos específicos. El principio debe ser respetado **por los controladores de datos y los procesadores de datos**. A diferencia de otros principios, el párr. 7.2.2 de la PPD no asigna la responsabilidad explícitamente a uno de ellos. Existen numerosos ejemplos de esta responsabilidad conjunta en las operaciones del ACNUR, en particular en actividades que requieren entrevistar o asesorar a las personas de interés. Si bien la orientación sobre cómo llevar a cabo el asesoramiento durante el registro, las entrevistas RSD, los procedimientos BID, las necesidades o los diagnósticos participativos pueden haber sido desarrolladas o proporcionadas por los controladores de datos (como parte de su responsabilidad para garantizar el cumplimiento general de la Política, párr. 7.2.1 de la PPD), los procesadores de datos necesitan implementar una orientación general y aplicarla cuando se comuniquen con las personas de interés.

4.2.3 En otros ejemplos, cuando los elementos de datos específicos que se necesitan recopilar están predeterminados en el material de orientación interno respaldado por sistemas o formularios electrónicos, por ejemplo, niveles de registro en la base de datos proGres del ACNUR, o en acuerdos de transferencia de datos (véase a este respecto párr. 6.1.2 (iii) y 6.2.2 de la PPD), la responsabilidad de respetar el principio de necesidad y proporcionalidad se habría trasladado completamente al controlador de datos. En situaciones donde los procesadores de datos tienen un cierto margen de discreción, por ejemplo, en las entrevistas de RSD o durante las evaluaciones, no deben sentirse

[14] Véase el artículo 5 (4) (c) del Convenio modernizado 108 y el artículo 5 (c) del RGPD. Véase también la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) y el Consejo de Europa, *Manual sobre la ley europea de protección de datos*, Edición 2018, disponible en inglés en: http: //fra.eu-ropa.eu/en/publication/2018/handbook-european-data-protection-law, Sección 3.3 página 125.

excesivamente restringidos en su ejercicio de recopilación de datos, sino guiarse por una comprensión clara de los propósitos (específicos y legítimos) de su actividad. Otro ejemplo se refiere al diseño de encuestas, donde se recomienda al personal del ACNUR que distinga cuidadosamente entre lo que es necesario y lo que simplemente puede ser "bueno saberlo".[15]

4.3. Precisión de los datos

4.3.1 El principio de precisión de los datos, que a veces también se conoce como **principio de calidad de los datos,**[16] se describe en el párr. 2.5 de la PPD como la necesidad de registrar los datos personales con la mayor precisión posible para garantizar que cumplan los propósitos para los que se procesan. Deben tomarse todas las medidas razonables para garantizar que los datos personales inexactos se eliminen o se corrijan sin demoras excesivas, teniendo en cuenta los propósitos para los que se procesan[17]. La exactitud de los datos está estrechamente relacionada con la continua **necesidad de verificación** de los datos de registro y la necesidad de **resolver inconsistencias** en el contexto antifraude[18].

4.3.2 El ACNUR enfrenta desafíos para garantizar la precisión de los datos, que son inherentes a la naturaleza de su trabajo en situaciones de crisis humanitaria. Por ejemplo, al registrar a las personas de interés, solo puede basarse en la información verbal proporcionada por el individuo sin la posibilidad de verificar dicha información con las autoridades nacionales del registro civil, especialmente en el país o la zona de origen. Dependiendo del propósito de la recopilación de datos, o **cuanto más importante sea la información, mayor sea el esfuerzo necesario para garantizar su precisión**. Un ejemplo que viene al caso se refiere al establecimiento y la prueba de la identidad y la creciente recopilación y uso de datos biométricos para fines de verificación, autenticación y autorización.

4.3.3 En términos prácticos, el principio de precisión de los datos puede implementarse mediante las siguientes medidas:

(i) Al informar a las personas de interés de sus derechos, resaltar la importancia de que los titulares de los **datos proporcionen información precisa y completa**, las consecuencias de no hacerlo, así como el requisito de notificar al ACNUR o sus socios sobre cualquier cambio en su situación personal (véase párr. 3.1 (iii) a (v) de la PPD);

(ii) Dentro de las restricciones logísticas y de seguridad, **revisar, verificar y actualizar periódicamente los conjuntos de datos personales**, por ejemplo, a través de un registro continuo y ejercicios de verificación (véase párr. 4.3.2 de la PPD);

[15] Véase sobre este aspecto CICR, *Manual sobre la protección de datos en la acción humanitaria*, Capítulo 2, página 26, párr. 2.5.3.

[16] Véase, por ejemplo, ICDPPC, *La resolución de Madrid*, Principio 9.

[17] Véase también el artículo 5 (1) (d) del RGPD de la UE.

[18] Véase ACNUR, *Manual para el registro*, Parte 1, Capítulo 4 (párr. 4.4 - Verificación) y Parte 2, Capítulo 20 (Técnicas de verificación), disponible en inglés en: http://www.refworld.org/pdfid/3f967dc14.pdf y ACNUR, *Política para abordar el fraude cometido por personas de interés*, octubre de 2017, párr. 4.6.

(iii) Que aquellos datos que han sido cuestionados, o que el ACNUR tiene motivos para creer que no son precisos, estén **marcados como tales**, y se tomen medidas para dar seguimiento a posibles imprecisiones, siempre que sea posible, por ejemplo, en procedimientos de RSD;

(iv) Que **la fuente de los datos,** así como las modificaciones o eliminaciones sean **registradas**.

4.4. Retención, eliminación y devolución de datos

4.4.1 La retención de datos tiene vínculos estrechos con los principios de necesidad y proporcionalidad; también se considera como un **principio de limitación de almacenamiento**[19]. En la Política de Protección de Datos del ACNUR, se aborda en la sección sobre tratamiento de datos donde se afirma que los datos personales no deberán conservarse más tiempo de lo necesario, de acuerdo con la finalidad para el cual fueron recolectados (párr. 4.6.1.)

4.4.2 Sin embargo, este principio y su relevancia en el ACNUR son limitados porque los expedientes de casos individuales de las personas de interés[20], ya sean abiertos o cerrados, se consideran **registros permanentes** (véase párr. 4.6.2 de la PPD)[21]. Los archivos del ACNUR existen para hacer que la experiencia del ACNUR esté disponible para guiar y ayudar al ACNUR en la planificación y realización de sus actividades, y para proporcionar información que satisfaga las necesidades de investigación de las personas de interés para el ACNUR, la comunidad académica y el público en general[22]. De manera similar, en la legislación sobre protección de datos se reconoce generalmente que el tratamiento adicional con fines de archivo de interés público, investigación científica o histórica o con fines estadísticas, se considera compatible con los fines iniciales de recopilación de datos[23]. En el ACNUR, se alienta a las operaciones en los países a transferir expedientes permanentes a la Sección de Archivos y Expedientes (RAS) en cualquier momento cuando ya no sean necesarios para el trabajo diario para garantizar una conservación segura y protegida[24].

4.4.3 Con respecto a los datos personales de las personas de interés contenidos en otros expedientes o documentos que no forman parte de un expediente individual y, por lo tanto, son **expedientes temporales**, el respeto de la limitación de retención generalmente implica su destrucción. Por ejemplo, cuando ya no es necesario conservar las listas de distribución para asistencia, los manifiestos de transporte o las encuestas de hogares, estos registros (y cualquier copia de respaldo) pueden ser destruidos[25]. La eliminación de los expedientes temporales debe ser formalmente autorizada por la alta dirección de la Oficina de País y esta última debe ponerse en contacto con la RAS antes de enviar los

[19] Véase, Artículo 5 (1) (e) del RGPD y Artículo 5 (4) (e) del Convenio modernizado 108; véase también FRA y el Consejo de Europa, *Manual sobre la ley europea de protección de datos*, Sección 3.5, página 129.

[20] Para la definición de 'expediente de caso individual', consulte arriba en la Sección 1.4 de esta Guía.

[21] ACNUR, *Política sobre la gestión de expedientes y archivos del ACNUR*, Anexo B: Resumen de planes de expedientes del ACNUR, diciembre de 2017, Sección 2 (Identificación de expedientes permanentes en el terreno), párr. 3.

[22] ACNUR, *Política sobre la gestión de expedientes y archivos del ACNUR*, Anexo C, página 1, disponible en inglés en: http://www.unhcr.org/re-search/archives/3b03896a4/unhcr-archives-access-policy.html.

[23] Véase Artículo 5 (1) (b) y 89 del RGPD.

[24] ACNUR, *Política sobre la gestión de expedientes y archivos del ACNUR*, Anexo B: Resumen de planes de expedientes del ACNUR, Sección 1 (Introducción).

[25] Ídem.

expedientes permanentes. En caso de duda sobre si los expedientes pueden ser destruidos, las operaciones deben comunicarse con la RAS para obtener asesoramiento[26].

4.4.4 De conformidad con la Política de Archivos, la **destrucción de expedientes temporales** debe realizarse de manera segura. La eliminación significa que la recuperación es imposible. Los métodos de eliminación segura para copias impresas incluyen: el uso de trituradoras de corte transversal, la quema segura de papeles o, en el caso de grandes volúmenes, la subcontratación de la eliminación de documentos físicos a un proveedor de servicios especializado. En este caso, las obligaciones contractuales deben garantizar que se respete la confidencialidad en toda la cadena de custodia y disponer la presentación de los documentos de eliminación y la certificación de la destrucción. Para los expedientes electrónicos, se debe tener en cuenta que las funciones de "eliminar" en la gran mayoría de los sistemas informáticos no destruyen la información del disco duro, sino que solo borran la referencia de la dirección mientras que dejan la información en sí en la computadora. Se aconseja al controlador de datos que busque orientación del Oficial de TI sobre la destrucción segura de datos o herramientas de borrado de discos que cumplan con las mejores prácticas de la industria. El Oficial de TI debe supervisar la destrucción física de cualquier medio que contenga documentos electrónicos, incluidos de audio y video y dispositivos portátiles, y asesorar debidamente al personal para que no desechen computadoras, portátiles, tabletas o teléfonos inteligentes que puedan contener datos personales antes de borrar el disco duro. Los **registros de eliminación** que indican la hora y el método de destrucción, así como la naturaleza de los documentos destruidos, deben conservarse y el ACNUR puede solicitarlos, como parte de los informes de proyectos o evaluaciones[27].

4.4.5 Cuando las **agencias implementadoras** procesan datos personales en nombre del ACNUR, las organizaciones socias deben **devolver o destruir** dichos datos personales para respetar el principio de retención limitada. Según el párr. 5.5 de la PPD, todos los Acuerdos de Colaboración para Proyectos (PPA) incluyen disposiciones para la devolución y/o eliminación de datos personales de las personas de interés tras la terminación del acuerdo[28]. En principio, todos los datos personales relacionados con las personas refugiadas y otras personas de interés para el ACNUR se devolverán físicamente al controlador de datos y el socio debe **certificar por escrito** que se han destruido todas las copias, incluidos los datos personales divulgados a sus subcontratistas. Existen dos situaciones excepcionales para esta regla general:

4.4.6 En primer lugar, cuando un **socio está sujeto a la obligación de retener los datos** proporcionados o procesados en nombre del ACNUR de acuerdo con un requisito legal, un procedimiento de auditoría establecido u otro procedimiento acordado previamente con el ACNUR, debe certificar por escrito que (i) se llevó a cabo una revisión de minimización de datos (solo se retienen los datos necesarios), (ii) que los datos ya no se procesarán activamente y se almacenan de tal manera que solo se puede acceder a ellos o utilizarlos para los fines para los cuales están siendo retenidos; y (iii) que los datos se eliminarán

[26] Ídem.

[27] Ídem.

[28] ACNUR, *Acuerdo de Colaboración para Proyectos Bipartitos de Formato Estándar (ACNUR con socios no gubernamentales y otros socios sin fines de lucro)*, disponible en inglés en: https://cms.emergency.unhcr.org/documents/11982/47020/Bipartite+PPA+-+NGO/2ac3aacc-adf6-492c-9ddc-1b8f242f1334, párr. 13.25

debidamente cuando haya transcurrido el período de retención (que debe indicar claramente el socio).

4.4.7 En segundo lugar, el **controlador de datos puede determinar que la eliminación no es necesaria**, por ejemplo, cuando la agencia implementadora continúa la prestación del servicio con otras fuentes de financiamiento. En tales casos, el controlador de datos debe estar satisfecho de que el socio busca el consentimiento explícito de los titulares de los datos y puede solicitar una copia de los datos del socio para fines adicionales de gestión y/o archivo de casos.

4.5. Confidencialidad

4.5.1 Según el párr. 4.1.1 de la PPD, los datos personales son, **por definición, clasificados** como confidenciales.[29] En función de su contenido, ciertos datos personales también pueden clasificarse como "estrictamente confidenciales" si se podría esperar razonablemente que la divulgación no autorizada cause daños excepcionalmente graves.[30] El deber de confidencialidad se extiende a todas las comunicaciones con las personas de interés, y todos los datos proporcionados por ellas u obtenidos en su nombre por el personal y los socios en el curso de las actividades del ACNUR. También es parte del Código de conducta del ACNUR (Principio 6) y el Reglamento del Personal de las Naciones Unidas (véase Regla 1.2 (i)).[31]

4.5.2 De conformidad con el párr. 7.2.2 de la PPD, los controladores de datos, con la asistencia del punto focal de protección de datos, deben implementar, entre otras cosas, medidas destinadas a garantizar la confidencialidad y seguridad de los datos. En el párr. 4.1.2, la PPD explica que, para garantizar y respetar la confidencialidad, los datos personales deben ser archivados y almacenados de manera tal que sean **accesibles solo para el personal autorizado** y transferidos solo a través del uso de medios de comunicación protegidos. Como consecuencia, se asesora a los controladores de datos que se aseguren de que **dicho personal autorizado esté identificado, en función de la "necesidad de conocimiento"**, por ejemplo, en los Procedimientos Operativos Estándar, y que se mantenga actualizado teniendo en cuenta la rotación regular del personal. Con respecto a las transferencias de datos, independientemente de si se ha firmado o no un acuerdo de transferencia de datos entre el ACNUR y el tercero, el ACNUR debe solicitar un acuerdo por escrito de parte del tercero de que los datos personales se mantendrán confidenciales (párr. 6.1.2 (v) de la PPD).

4.5.3 El personal del ACNUR debe saber que los Estados están sujetos a una obligación internacional de respetar los privilegios e inmunidades de la Organización de las Naciones Unidas,[32] de la cual el ACNUR como órgano subsidiario de la Asamblea General es parte.

[29] Véase ACNUR, *Política de clasificación, manejo y divulgación de información*, diciembre de 2010, párr. IV (1) (a) y (b), basado en las Naciones Unidas, *Boletín del Secretario General sobre la sensibilidad, clasificación y manejo de la información*, ST/SGB/2007/6 del 12 de febrero de 2007, disponible en inglés en: https: https://archives.un.org/sites/archives.un.org/files/ST_SGB_2007_6_eng.pdf, Sección 1, párr. 1.2(a) y (b).

[30] Ídem, párr. III (4) y ST/SGB/2007/6, Sección 2, párr. 2.3.

[31] ACNUR, *Código de conducta*, en: http://www.acnur.org/fileadmin/Documentos/BDL/2005/3871.pdf?file=fileadmin/Documentos/BDL/2005/3871,Naciones Unidas, *Reglamento del personal*, disponible en: https://digitallibrary.un.org/record/855429/files/ST_SGB_2017_1-ES.pdf

[32] Véase el Artículo 105 de la Carta de las Naciones Unidas y la *Convención sobre los Privilegios e Inmunidades de las Naciones Unidas,* adoptada por la Asamblea General de las Naciones Unidas el 13 de febrero de 1946, disponible en: http://www.uy.undp.org/content/dam/uruguay/docs/marco-legal-uy/undp-uy-convencion-privilegios-inmunidades-nnuu.pdf.

Los privilegios y las inmunidades también son un elemento estándar de los acuerdos de país de acogida del ACNUR; sirven a la organización para que cumpla su mandato de manera independiente. La inmunidad del ACNUR incluye la inviolabilidad de sus expedientes y archivos, incluidos los datos personales de los que disponen en relación a las personas de interés.[33] Cualquier acto de allanamiento, requisición, confiscación, expropiación u otra forma de interferencia por parte de las autoridades nacionales, ya sea de carácter ejecutivo, administrativo, judicial o legislativo (incluidas las órdenes de divulgación de los tribunales nacionales), constituye una violación de las inmunidades del ACNUR y debe comunicarse de inmediato a los Servicios de Asuntos Jurídicos (LAS) en la Sede.

5. Derechos de la persona de interés como titulares de los datos

5.1. Introducción

5.1.1 Al aplicar un enfoque basado en los derechos, el ACNUR se compromete, a través de la Política de Protección de Datos, a respetar una serie de derechos de las personas de interés, como titulares de los datos, a saber:

(i) El derecho a **recibir información** sobre el tratamiento de datos por parte del ACNUR y sus socios;

(ii) El derecho a **solicitar acceso** a los datos en poder del ACNUR y sus socios;

(iii) El derecho a **solicitar la corrección y/o eliminación** de esos datos; y

(iv) El derecho a **oponerse** al tratamiento de sus datos.

5.1.2 El derecho a la información también se conoce como el **principio de transparencia o apertura** y, en consecuencia, los derechos del titular de los datos solo incluyen los puntos (ii) a (iv)[34]. En otros lugares, un principio de transparencia más amplio aparece junto con el derecho a la información[35] o este último se combina con el derecho al acceso[36]. La formulación del párr. 3.1 de la PPD establece una **obligación proactiva por parte del ACNUR para informar a los titulares de los datos**, mientras que los demás derechos están sujetos a una solicitud. Los diferentes enfoques, por lo tanto, no deben conducir a diferencias en el trato de los titulares de los datos. Los derechos establecidos en la Política del ACNUR están arraigados en el derecho universal a la privacidad y se reflejan en la Observación General No. 16 del Comité de los Derechos Humanos[37].

[33] Artículo II Sección 3 de la Convención de 1946.

[34] Véase, por ejemplo, ICDPPC, *La Resolución de Madrid*, Parte II, párr. 10 y Parte IV, párr. 16 a 18.

[35] Capítulo III, Sección 2, Artículos 12 a 15 del RGPD.

[36] Por ejemplo, en el Artículo 8 (b) del Convenio Modernizado 108.

[37] Véase el Comité de Derechos Humanos de las Naciones Unidas (CDH), *Observación general No. 16 del CCPR: Artículo 17 (Derecho a la privacidad), El derecho al Respeto de la Privacidad, la Familia, el Hogar y la Correspondencia, y la Protección del Honor y la Reputación*, 8 de abril de 1988, disponible en inglés en: http://www.ref-world.org/docid/453883f922.html, párr. 10.

5.2. El derecho a la información

5.2.1 La Política de Protección de Datos del ACNUR combina **varios tipos de información** sobre la cual el ACNUR debe informar a una persona cuando recopila datos personales, incluida la información sobre el tratamiento de los datos previstos y sus propósitos, así como los derechos del titular de los datos, cómo presentar una solicitud y la importancia de proporcionar información precisa (véase la lista completa en el párr. 3.1 (i) a (viii) de la PPD). Además, el personal del ACNUR debe hacer hincapié en que los datos se mantendrán confidenciales, no serán compartidos con el país de origen y explicará, en la medida de lo posible, los beneficios y riesgos del tratamiento de datos y las transferencias en el entorno operativo específico, incluyendo mensajes antifraude adecuados al contexto operacional.[38] Cuando no sea posible proporcionar a las personas de interés toda la información requerida sobre el tratamiento de datos del ACNUR en el primer punto de recopilación de datos, por ejemplo, debido a la magnitud de una emergencia, esta información debe proporcionarse en la siguiente oportunidad práctica.

5.2.2 El acceso a la información sobre el tratamiento de datos es un requisito previo para la adopción de decisiones informadas por parte de las personas de interés con respecto a sus datos personales, incluida la posibilidad de ejercer sus derechos de acceso, corrección y eliminación u objeción. Como regla general, la **información debe proporcionarse antes de que los datos personales se procesen**, oralmente o por escrito, de manera tan transparente como lo permitan las circunstancias y, de ser posible, directamente a la persona interesada.[39] Además, y cuando esto no es posible debido al tamaño de la población de las personas de interés, se recomiendan a las operaciones del ACNUR integrar la provisión de información sobre el tratamiento de datos en sus estrategias de comunicación con las personas de interés, por ejemplo, a través de campañas de información masiva, sitios web, iniciativas de difusión comunitaria, reuniones con líderes y comités comunitarios, folletos y avisos de información. **La información debe proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo**, y debe comunicarse a través de medios apropiados (por ejemplo, visual, audio y fácil de leer) para mejorar el acceso para las personas con impedimentos visuales, auditivas e intelectuales.

5.3. El derecho de acceso a los datos personales

5.3.1 En el párr. 3.2, la Política de Protección de Datos estipula que los titulares de los datos pueden recibir del ACNUR (i) confirmación de si el ACNUR procesa cualquier dato personal sobre ellos y (ii) información sobre los datos personales que se procesan, el (los) propósito(s) para procesar dichos datos y el (los) socio(s) y/o terceros a los que se han transferido, se están transfiriendo o se transferirán dichos datos. Si bien cada solicitud debe considerarse caso por caso, teniendo en cuenta el interés legítimo del titular de los datos en acceder a sus datos personales, generalmente se recomienda a los controladores de datos que adopten un **enfoque según el cual la concesión de acceso debe ser el principio y la negativa la excepción**.

[38] ACNUR, *Política sobre el fraude cometido por personas de interés*, párr. 4.2 a).

[39] CICR, *Manual sobre la protección de datos en la acción humanitaria*, Capítulo 2, párr. 2.10, página 36.

5.3.2 Esto se aplica a los datos personales que se incluyen en los documentos que las personas de interés han proporcionado al ACNUR. Ejemplos de esto incluyen pasaportes, documentos de identidad, certificados de matrimonio o de nacimiento, expedientes académicos, fotos, registros médicos o cualquier evidencia documental de actividades o incidentes en el país de origen presentados en apoyo de una solicitud de la condición de refugiado. El **acceso a las copias de los documentos proporcionados por las personas de interés**, por ejemplo, en caso de pérdida del original por la persona de interés, **en principio no debe estar restringido**. El ACNUR no debe conservar los originales de los documentos proporcionados por las personas de interés.

5.3.3 La situación varía cuando se trata de **datos personales en documentos o registros generados por el ACNUR ("productos de trabajo internos")**, o por una agencia implementadora en nombre del ACNUR, tales como registros de entrevistas o evaluaciones de tratamiento de casos. Si bien se recomienda que los controladores de datos se esfuercen por garantizar un **alto grado de transparencia** hacia las personas de interés, también deben ejercer su discreción y pueden retener documentos o registros específicos, en parte o en su totalidad, por ejemplo, cuando esto revele datos personales de terceros o cuando los documentos se clasifican como "confidenciales" o "estrictamente confidenciales". Las Normas Procedimentales para RDS y el Manual de Reasentamiento contienen consejos más detallados con respecto a los procedimientos respectivos[40].

5.3.4 Cuando el ACNUR ha recibido **datos personales de las personas de interés de un socio de un proyecto o de un tercero**, el ACNUR puede proporcionarle a la persona información sobre la fuente de los datos personales que recibió, con la excepción de la información que se proporcionó bajo la condición de (o con una expectativa razonable de) confidencialidad, o que de otro modo perjudicaría las operaciones del ACNUR o las relaciones con terceros. Si un socio o un tercero posee datos personales, el ACNUR debe explicar el (los) propósito(s) específico(s) de la transferencia del ACNUR a ese socio/tercero y referir al titular de los datos al socio o tercero para obtener más información sobre el tratamiento de datos.

5.4. El derecho a solicitar la corrección o eliminación de datos personales

5.4.1 La Política de protección de datos otorga a las personas refugiadas y a otras personas de interés el derecho a solicitar la corrección o eliminación de sus **propios datos personales que sean inexactos, incompletos, innecesarios o excesivos** (párr. 3.2.1). Es necesario verificar si, en efecto, los datos personales son imprecisos o incompletos. Por esta razón, el párr. 3.2.2 de la PPD requiere que el ACNUR solicite pruebas relacionadas con la inexactitud o el estado incompleto. Sin embargo, se reconoce que la prueba no siempre está disponible en el contexto del desplazamiento forzado. Por lo tanto, se recomienda al personal del ACNUR que **aplique técnicas de verificación apropiadas** según se hayan desarrollado en el contexto del registro para evaluar las solicitudes[41].

[40] ACNUR, *Normas Procedimentales para DCR - Representación legal en los procedimientos de DCR del ACNUR*, 2016, ("Normas Procedimentales para DCR"), disponible en inglés en: http://www.refworld.org/docid/56baf2c84.html, Sección 2.7.4 (b) y ACNUR, *Manual de Reasentamiento*, 2011, disponible en: http://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=search&docid=5174e63e4&skip=0&query=Manual%20de%20Reasentamiento, Sección 7.5.7.
[41] Véase ACNUR, *Manual para el registro*, disponible en inglés en: http://www.refworld.org/pdfid/3f967dc14.pdf, Parte 2, Capítulo 20.

5.4.2 Las solicitudes de corrección a menudo pueden producirse en el transcurso del tratamiento de casos de rutina, por ejemplo, cuando a un individuo se le entrega una carta de certificación y se le informa que sus datos personales básicos se registraron incorrectamente. Algunos pueden ser obvios y pueden manejarse rápidamente, otros pueden requerir una verificación exhaustiva de la prueba u otra información que respalde la solicitud. En general, al recibir una solicitud, se aconseja, por lo tanto, al personal encargado del ACNUR que:

(i) **Solicite pruebas** relacionadas con la inexactitud/carácter incompleto de los datos (si corresponde), y

(ii) **Evalúe la legitimidad** de la solicitud y la credibilidad de la prueba o información proporcionada en apoyo de la solicitud, utilizando, por ejemplo, técnicas de verificación en el contexto de los procedimientos de registro.

Si el miembro del personal responsable (basado en su función o responsabilidades asignadas) considera que la solicitud es creíble, los datos deben ser modificados. De acuerdo con las obligaciones del ACNUR de mantener registros (véase la Sección 8.1), se aconseja al personal que registre el hecho de que una persona de interés ha solicitado una corrección y el ACNUR aceptó o no esas solicitudes en el expediente de la persona.

5.4.3 Cuando el personal responsable tenga **motivos para creer que una solicitud es manifiestamente abusiva, fraudulenta u obstructiva**, por ejemplo, una solicitud para corregir partes de una transcripción de una entrevista, o para cambiar información que podría afectar la elegibilidad para la condición de refugiado o el reasentamiento sin justificación, puede estar sujeto a las restricciones establecidas en el párr. 3.7 (ii) de la PDP. Dichas solicitudes deben rechazarse y, además, podrían requerir procedimientos de detección de fraude.[42]

5.5. El derecho a oponerse al tratamiento de los datos personales

5.5.1 Los titulares de los datos tienen derecho a objetar el tratamiento de datos, con la condición de que existan **motivos legítimos relacionados con su situación personal específica**. El tema clave del derecho a objetar es el de evaluar la legitimidad de los argumentos presentados por el titular de los datos en relación con su situación específica. Por ejemplo, una persona solicitante de asilo puede requerir que sus datos personales no se transfieran al país de acogida o a un socio en particular debido a preocupaciones, debido a su determinado perfil, por su seguridad o la de los miembros de su familia.

5.5.2 Si la objeción se considera justificada, el **tratamiento debe limitarse a los fines legítimos restantes**, por ejemplo, el registro o el archivo. Si la objeción se refiere a la transferencia de datos personales a un tercero, los elementos de datos relevantes pueden eliminarse de los sistemas y herramientas del ACNUR o pueden reducirse los derechos de acceso, por lo que es inaccesible para terceros. Sin embargo, algunas solicitudes también pueden resolverse mediante un asesoramiento exhaustivo, formas alternativas de asistencia o protección o planteando el problema subyacente con un socio sin referirse al caso individual. Cuando no sea factible una forma alternativa de asistencia, se debe asesorar al individuo para tal efecto.

[42] Sobre la detección y la respuesta al fraude, véase ACNUR, *Política sobre cómo abordar el fraude cometido por personas de interés*, párr. 4.3.

5.5.3 Al evaluar las objeciones, también se aconseja al personal del ACNUR que (i) verifique la base legítima original porque, si es el consentimiento, la objeción normalmente implicaría la revocación del consentimiento, (ii) si existe una base legítima alternativa para el tratamiento continuo, aunque restringido, por ejemplo, para mantener registros (incluso para archivar) y (iii) si el tratamiento sigue siendo necesario y proporcionado para el propósito. **El derecho a objetar no es otra forma del derecho a la eliminación**. Finalmente, una solicitud de retiro de una solicitud de la condición de refugiado no se consideraría como una objeción, sino más bien como un procedimiento específico dentro de la RSD que conllevaría, tras la asesoría, al cierre del expediente[43].

5.6. Restricciones de los derechos del titular de los datos

5.6.1 El derecho a la privacidad no es un derecho absoluto y debe ponderarse contra otros derechos fundamentales e intereses públicos, de conformidad con el principio de proporcionalidad. En el párr. 3.7 (i), la Política de Protección de Datos se refiere a medidas necesarias y proporcionadas para salvaguardar la seguridad y protección del ACNUR, su personal o el personal de sus socios o las necesidades y prioridades operativas primordiales del ACNUR en el cumplimiento de su mandato. En consonancia con otras políticas[44], esto puede interpretarse como información cuya divulgación podría poner en peligro los derechos de otras personas o perjudicar el trabajo del ACNUR y, por lo tanto, es, o debería ser, clasificado como "confidencial" o "estrictamente confidencial".

5.6.2 En la práctica, esto puede incluir **información sobre la salud física o mental** de la persona u otras personas, donde la divulgación puede causar un daño grave o socavar la prestación de servicios esenciales; la **privacidad** de otras personas de interés, sus familiares o personas con las que están asociadas, a menos que hayan dado su consentimiento, **investigaciones delictivas** o tratamientos en los que el ACNUR haya procesado datos personales por iniciativa propia o en respuesta a una solicitud legítima de las autoridades nacionales, **los esfuerzos de integridad y antifraude** del ACNUR en los casos en que la divulgación podría socavar las investigaciones específicas o el funcionamiento de sus procedimientos de detección e investigación, las **investigaciones de la OIG** con respecto a la mala conducta del personal en relación a las personas de interés, la **información proporcionada por un tercero** a condición de, o con una expectativa razonable de confidencialidad.

5.6.3 Además, el ACNUR puede rechazar las solicitudes de cualquiera de los derechos de los titulares de los datos si existen razones para creer que la solicitud es manifiestamente abusiva, fraudulenta u obstructiva a la finalidad del tratamiento (párr. 3.7 (ii) de la PPD). Las **solicitudes abusivas** incluyen, pero no se limitan a, solicitudes repetidas idénticas o similares de la misma persona (a menos que haya transcurrido un intervalo razonable), o solicitudes que constituyan un obvio intento de abuso del proceso**.** Las **solicitudes fraudulentas** incluyen, pero no se limitan a, situaciones en las que la identidad de la persona o la autoridad de su representante legal no se puede verificar o está en duda. Las solicitudes que generan incoherencias que no pueden ser resueltas por la unidad funcional

[43] Véase ACNUR, *Normas procedimentales para DCR, Unidad 9 - Procedimientos para el cierre de expedientes,* disponible en: http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=49ddbba22, Sección 9.1.

[44] Por ejemplo, ACNUR, *Política para abordar el fraude cometido por personas de interés*, *Política de clasificación, manejo y divulgación de información* y *Papel, funciones y modus operandi de la Oficina del Inspector General*.

del ACNUR o que se consideran de naturaleza significativa deben ser referidas al Punto Focal Antifraude de la operación[45]. Las **solicitudes obstructivas** incluyen, pero no se limitan a, solicitudes u objeciones que no tienen ningún fundamento razonable y "solicitudes masivas" que están claramente diseñadas para frustrar u obstruir la implementación efectiva del mandato del ACNUR.

5.7. Aspectos de procedimiento

5.7.1 Bajo el párr. 7.2.2 (iii) de la PPD, es responsabilidad del controlador de datos establecer procedimientos internos, en particular con relación al respeto de los derechos del titular de los datos. En el párr. 3.5 (modalidades de las solicitudes) y 3.6 (registro y respuesta), la Política de Protección de Datos proporciona alguna orientación con respecto a los aspectos procedimentales. Esto, sin embargo, no es exhaustivo. A continuación, se proporcionan más orientación y propuestas sobre cómo se podrían diseñar tales procedimientos y qué puntos deberían incluir. De acuerdo con el propósito y razonamiento de la Política, dichos procedimientos deben ser **justos y eficientes** con el fin de **permitirles a los titulares de los datos que se respeten sus derechos**.

5.7.2 Los procedimientos para los derechos de los titulares de los datos podrían establecerse en los **Procedimientos Operativos Estándar (SOP, por sus siglas en inglés)** (párr. 7.2.2 de la PPD). Tales SOP podrían cubrir, como se sugiere en la Política, todos los aspectos relevantes de protección de datos, incluida la seguridad y la transferencia de datos. Alternativamente, el (los) procedimiento(s) para las solicitudes de los titulares de los datos se pueden integrar a los procedimientos operativos estándar existentes, por ejemplo, en el registro, la determinación de la condición de refugiado (RSD) y/o el reasentamiento. Sin embargo, **no se deben confundir con los procedimientos generales de quejas** previstos en estas áreas[46]. Si bien pueden haber superposiciones, por ejemplo, una persona solicitante de asilo puede quejarse del personal de registro que se niega a corregir ciertos elementos de datos personales en su expediente, ambos persiguen diferentes objetivos: la queja sobre el funcionario se refiere a un determinado comportamiento, potencialmente la mala conducta, y la forma en que se prestan los servicios, mientras que la solicitud de corrección se refiere al respeto de un derecho específico relacionado con el tratamiento de los datos personales de la persona interesada. Además, el personal encargado de atender quejas generales puede no necesariamente ser responsable de atender una solicitud relacionada con el tratamiento de datos personales.

5.7.3 Los procedimientos para las solicitudes de los derechos de los titulares de los datos pueden abordar de manera útil los aspectos de: (1) cómo se informa a los titulares de los datos sobre sus derechos, (2) quién tiene derecho a presentar una solicitud, (3) cómo presentar una solicitud, y (4) aspectos sobre la gestión y la respuesta a las solicitudes, incluida la persona responsable designada para atender las solicitudes. Estos cuatro

[45] ACNUR, *Política sobre cómo abordar el fraude cometido por personas de interés*, párr. 4.7.

[46] Véase ACNUR, *Manual para el registro*, disponible en inglés en: http://www.refworld.org/pdfid/3f967dc14.pdf, Parte 2, Capítulo 13, Sección 13.3 ('Establecer procedimientos de quejas'), *Normas procedimentales para determinar la condición de refugiado*, disponible en: http://www.refworld.org/cgi-bin/texis/vtx/rwmain?page=search&docid=4f5898a02&skip=0&query=Normas%20Procedimentales%20para%20DCR, Sección 2.6, página 2-22 ('Procedimientos para efectuar reclamos') y *Manual de reasentamiento*, disponible en: http://www.acnur.org/fileadmin/Documentos/Publicaciones/2012/8947.pdf?view=1, Capítulo 4, página 133 ('Mecanismo de reclamos').

aspectos se detallan a continuación, enumerando los puntos que podrían incluirse en los SOP.

5.7.4 **Información de los titulares de los datos** sobre sus derechos (véase también el párr. 3.1 (viii) de la PPD:

(i) Cuando el ACNUR realiza el registro, la RSD y/o el reasentamiento, la información relacionada con los derechos del individuo como titular de los datos, es decir, el acceso y corregir, eliminar u objetar, se integra de manera útil en dichos procedimientos y se proporciona individualmente, por ejemplo, antes de las respectivas entrevistas.

(ii) Cuando el ACNUR no lleve a cabo ninguno de los procedimientos mencionados, pero aun así procesa datos personales, por ejemplo, en el contexto de las actividades de monitoreo, el titular de los datos debe, en la medida de lo posible, ser aconsejado y asesorado individualmente.

(iii) En operaciones grandes, ya sea en campamentos o en contextos urbanos, se aconseja a los controladores de datos que proporcionen información relevante también mediante otras formas de comunicación que sean apropiadas en sus respectivos entornos operativos. Se hace referencia al párr. 8.1.2 arriba.

5.7.5 Las siguientes personas tienen **derecho a presentar una solicitud**:

(i) El titular de los datos;

(ii) Representantes legales, progenitores o personas con tutoría legal en nombre del titular de los datos a quien representan (párr. 3.5.1 de la PPD). En el caso de los padres y tutores legales, el personal responsable del ACNUR debe verificar si existen razones para creer que no responde al interés superior de la niña o niño divulgar dichos datos a sus progenitores o tutores legales;

(iii) Las niñas o niños que pueden expresar su consentimiento o asentimiento al tratamiento de datos también pueden presentar solicitudes por derecho propio (para más detalles, véase más adelante). Aunque los miembros de la familia pueden tener un interés legítimo en tratar de acceder a datos relacionados con sus familiares, estos no tienen derecho a realizar solicitudes en nombre de los titulares de los datos; tales solicitudes deben tramitarse de conformidad con las condiciones para el intercambio de datos con terceros;

(iv) Las personas representantes legales deben presentar una designación de representación legal (poder notarial). Las "solicitudes masivas", en las que una persona representante legal envía solicitudes en nombre de varias personas de interés, deben, en la medida de lo posible, manejarse de la misma manera que las solicitudes individuales (tomando en consideración la capacidad y los recursos disponibles).

5.7.6 Formas y condiciones para **presentar una solicitud**:

(i) Las solicitudes pueden hacerse oralmente o por escrito (párr. 3.5.1 de la PPD).

(ii) Las solicitudes deben enviarse a la oficina del ACNUR en el país donde se están procesando los datos (párr. 3.5.1 de la PPD). Sin embargo, se recomienda a los

controladores de datos que no conciban esto como un requisito formal. La idea es llevar las solicitudes rápidamente a la atención de la persona encargada de responderlas. Las solicitudes verbales o solicitudes dirigidas a una agencia implementadora deben redirigirse a la persona responsable en la oficina del ACNUR que tiene los datos del individuo, incluida la Sección de Archivos y Expedientes (RAS) del ACNUR.

(iii) Las solicitudes y su respuesta son siempre gratuitas;

(iv) En principio, las solicitudes no requieren razones como una condición formal. Cuando se requiere información del titular de los datos, por ejemplo, para verificar su identidad, pero también para responder a las solicitudes de corrección u objeción, se aconseja al personal del ACNUR que solicite dicha información al titular de los datos con el ánimo de abordar la solicitud de manera justa y eficiente.

5.7.7 **Gestión y respuesta a las solicitudes:**

(i) Designación de la **persona responsable** para tramitar y responder a las solicitudes de los titulares de los datos en nombre del controlador. Teniendo en cuenta la responsabilidad de esta función, se aconseja a los controladores de datos que designen a una persona responsable de alto nivel. La práctica recomendada es designar al punto focal de protección de datos, quien, de acuerdo con la Política de Protección de Datos, es, en principio, la persona funcionaria de más alto nivel del personal de protección del ACNUR (párr. 1.4 y 7.2.1). En operaciones de gran envergadura con varias suboficinas y oficinas en el terreno, el controlador de datos puede elegir designar a personas responsables en cada oficina con un sistema de puntos focales secundarios;

(ii) Los SOP pueden identificar **solicitudes manifiestamente fundadas**, que, por razones de eficiencia, podrían ser gestionadas por el personal que trata directamente con los titulares de los datos como parte de los procedimientos rutinarios de gestión de casos, por ejemplo, solicitudes para modificar o actualizar datos biográficos básicos, como información de contacto (dirección, número de teléfono, etc.) o situación personal (nacimientos, defunciones, matrimonios, etc.) en el contexto del registro continuo. Dichos funcionarios generalmente también podrán verificar la identidad de la persona solicitante, por ejemplo, realizando una inspección visual de un documento de identidad o consultando el Sistema de Gestión de Identidad Biométrica (BIMS) del ACNUR.

(iii) De acuerdo con la Política, el ACNUR debe **registrar** las solicitudes recibidas para el acceso, corrección, eliminación u objeción y la respuesta proporcionada en relación con dichas solicitudes (párr. 3.6.1).

(iv) Antes de cumplir con una solicitud, la persona responsable debe **verificar la identidad** de la persona que realiza la solicitud para asegurarse de que está autorizada (véase arriba y el párr. 3.5.2 de la PPD). En casos particularmente sensibles, o en caso de un presunto fraude, la oficina puede solicitar la certificación de un notario con autoridad legal para confirmar la identidad y/o la validez de la documentación oficial.

(v) El ACNUR debe responder a una solicitud dentro de un **plazo razonable** (párr. 3.6.2 de la PPD), lo recomendado es 30 días;

(vi) La respuesta debe elaborarse de **forma y en un lenguaje que sea comprensible** para el titular de los datos y/o su representante legal o tutor legal, según corresponda, verbalmente o por escrito (párr. 3.6.2 de la PPD). Como norma general, la respuesta debe darse por escrito, en particular si la solicitud es por escrito. Para mayor eficiencia, las respuestas verbales pueden ser más apropiadas en los casos en que las solicitudes pueden responderse de manera inmediata y positiva;

(vii) La **naturaleza de los procedimientos** en las solicitudes de los titulares de los datos debe respetar la dignidad de la persona y la confidencialidad;

(viii) La respuesta debe **explicar la acción tomada** en respuesta a la solicitud y **proporcionar razones** por las cuales no se pueden cumplir las solicitudes, por ejemplo, por qué el acceso no puede ser otorgado o solo se otorga parcialmente, por qué no se puede hacer una corrección (por ejemplo, por falta de evidencia), por qué la eliminación no es posible (por ejemplo, porque los datos están en registros permanentes) o una objeción no puede ser respetada (por ejemplo, debido a las prioridades operacionales y motivos insuficientes relacionados con la situación personal específica). Las excepciones se justifican cuando la exposición de motivos podría poner en peligro o perjudicar el trabajo del ACNUR debido a la naturaleza de una restricción aplicable (por ejemplo, el fraude).

(ix) La **aplicación de una restricción** basada en el para. 3.7 de la PPD debe llevarse a cabo caso por caso con una evaluación individual de cada decisión;

(x) Una respuesta a una solicitud de acceso puede contener documentos relativos a los titulares de los datos solicitantes que también contienen **datos personales de otras personas y/o información clasificada**. En este caso, la redacción de cualquier dato personal de otras personas, incluido el ACNUR o el personal de los socios, bloqueando con negro las partes relevantes puede ser una solución para mantener un alto grado de transparencia. El controlador de datos puede decidir ser consultado en tales casos para asegurarse de que todos los datos relevantes hayan sido excluidos antes de la divulgación. Se debe agregar una copia del material divulgado al expediente del caso individual que muestre las redacciones.

(xi) En el caso de las solicitudes que plantean temas complejos con respecto al mandato del ACNUR, la relación con terceros o posibles implicaciones para la seguridad, el controlador de datos puede solicitar el asesoramiento del Oficial de Protección de Datos (DPO) (párr. 7.2.3 de la PPD).

5.7.8 En el caso de **solicitudes presentadas por niñas, niños o personas con problemas de salud mental o discapacidades intelectuales**, los SOP pueden contemplar lo siguiente: Antes de responder a una solicitud de una niña o niño, la persona responsable, en consulta con el oficial de protección de la infancia, debe estar de acuerdo de que:

(i) La niña o niño puede expresar su consentimiento o asentimiento (véase la Sección 6.7 arriba) y entiende el significado de presentar una solicitud y cómo interpretar cualquier información que reciba como respuesta, y

(ii) La solicitud no se ha realizado bajo coacción.

Si se cumplen estas condiciones, la solicitud se puede gestionar de la misma manera que las solicitudes de los adultos.

5.7.9 Si no se cumplen, se asesora a la persona responsable que inicie un procedimiento de interés superior antes de divulgar cualquier información en respuesta a la solicitud, teniendo en cuenta:

(i) Las determinaciones o evaluaciones del interés superior relacionadas con la patria potestad que ya se aplican al caso de la niña o niño;

(ii) La naturaleza y sensibilidad de los datos personales y las consecuencias de permitir que aquellos con la patria potestad accedan a ellos.

(iii) Cualquier acusación de abuso o maltrato;

(iv) El punto de vista de la niña o niño sobre si sus progenitores/tutores legales deberían tener acceso a información sobre ellos (en la ausencia de los cuales normalmente no se divulgaría);

(v) El posible perjuicio para la niña o niño si se impidiera el acceso a la información a las personas con la patria potestad.

También se debe tomar una determinación sobre el interés superior con respecto a las solicitudes formuladas por un tercero que tiene el derecho de tratar los asuntos de una persona de interés que, debido a problemas mentales o discapacidad intelectual, se cree que carece de la capacidad de comprender adecuadamente el proceso.

5.8. Papel de la Oficina del Inspector General

5.8.1 Como parte del derecho a la información, el titular de los datos también debe ser informado sobre su derecho a presentar una queja ante la OIG (párr. 3.1 (viii) de la DPP). La Política de Protección de Datos no afecta las funciones encomendadas de la Oficina del Inspector General (OIG), que incluyen la investigación de una posible mala conducta del personal del ACNUR o cualquier otra entidad que tenga vínculos contractuales con el ACNUR, incluido el personal de los socios o proveedores de servicios comerciales (párr. 7.4 de la PPD). En el contexto de la protección de datos, esto podría ser, por ejemplo, un funcionario del ACNUR que divulgue o proporcione acceso a datos personales de personas de interés a un tercero no autorizado.

5.8.2 La OIG también tiene el mandato de realizar investigaciones *ad hoc* sobre ataques violentos contra operaciones del ACNUR en las que éstas suponen daños a gran escala a los activos del ACNUR.[47] Esto podría incluir datos personales de personas de interés, por ejemplo, en el caso de una grave filtración de datos. Por lo tanto, la OIG puede, en circunstancias excepcionales, formar parte del Equipo de Trabajo de Filtración de Datos (véase el párr. 10.3.6 abajo).

[47] ACNUR, *El papel, las funciones y el modus operandi de la Oficina del Inspector General*, febrero de 2012, párr. 2 (Mandato).

5.9. Papel de la Oficina de Ética

5.9.1 La Oficina de Ética busca fomentar una cultura de ética, transparencia y responsabilidad en el ACNUR, e identificar posibles dilemas éticos y conflictos de intereses en el lugar de trabajo, de modo que se puedan tomar las medidas apropiadas para prevenir los problemas antes de que surjan. Las principales responsabilidades de la Oficina de Ética son: (a) proporcionar asesoramiento confidencial y orientación al personal y a la alta dirección sobre temas éticos; (b) promover una cultura de integridad y rendición de cuentas, crear conciencia y desarrollar normas y educación sobre asuntos éticos; (c) implementar la política de protección del personal contra represalias ("política de denunciantes"); y (d) fortalecer la respuesta y la prevención de la explotación y el abuso sexual.

5.9.2 En el contexto de la protección de datos, la Oficina de Ética puede proporcionar orientación sobre la protección de los "denunciantes", por ejemplo, si el personal está preocupado por la gestión de datos personales en su operación, especialmente la denuncia de filtración de datos personales, o asesorar el personal sobre cómo abordar los problemas éticos con relación a su conducta personal, por ejemplo, en el contexto de la divulgación de datos personales de las personas de interés. Aunque desde el punto de vista procedimental, la Oficina de Ética no recibe reclamos directamente de las personas de interés, puede brindar apoyo al personal del ACNUR que revisa dichas quejas o tiene dudas sobre las prácticas de protección de datos de su oficina.

6. Seguridad de los datos

6.1. Contexto

6.1.1 En un contexto de creciente recopilación de datos personales, el uso de múltiples activos de TIC, incluidos equipos portátiles, almacenamiento en una amplia gama de bases de datos electrónicas, transferencias a través de diversos medios y herramientas a un número creciente de socios y terceros y, en particular, las amenazas de diversos adversarios, incluidas las organizaciones delictivas, los llamados hackers, agencias estatales y actores no estatales interesados en acceder información confidencial sobre las personas de interés del ACNUR, no se puede subestimar la importancia y el desafío de la seguridad de los datos.

6.1.2 La Política de Protección de Datos reconoce estos desafíos y, teniendo en cuenta la posición particularmente vulnerable de las personas de interés del ACNUR y la naturaleza generalmente sensible de sus datos personales, exige un manejo cuidadoso (párr. 1.2.1), un alto nivel de seguridad de los datos (párr. 4.2.1) y la implementación de medidas organizativas y técnicas apropiadas (párr. 4.2.2), incluido el enfoque de "privacidad desde el diseño" (párr. 4.2.3). Además, la Política toma en cuenta la disponibilidad y calidad del equipo necesario, el costo y la viabilidad operacional (párr. 4.2.1 y 4.2.3).

6.1.3 La Política de Protección de Datos no define las normas de seguridad de datos que debe tener el ACNUR. En términos generales, las medidas de seguridad que sean

apropiadas, a nivel operacional mundial y nacional, dependerán de la naturaleza de los datos personales que se procesarán, el daño potencial a las personas de interés que podría resultar de una filtración de datos personales, la probabilidad de que se materialice una filtración, y la disponibilidad y calidad del equipo requerido, el costo y la factibilidad. La División de Sistemas de Información y Telecomunicaciones (DIST) es responsable de elaborar normas y directrices relacionadas con la TIC.[48]

6.1.4 La Política de Protección de Datos subraya la responsabilidad del controlador de datos, que debe garantizar la aplicación de medidas organizativas y de seguridad (párr. 7.2.2 de la PPD). Independientemente de las medidas organizativas que normalmente corresponden a la esfera de competencia del controlador de datos, la seguridad de los datos es responsabilidad de todo el personal del ACNUR.[49] En este capítulo, se desarrolla y proporciona orientación sobre las nociones de medidas organizativas y técnicas, el enfoque de privacidad desde el diseño, ciertos procedimientos y prácticas de seguridad de datos, comunicación y transferencias de datos seguras y gestión de datos personales en entornos de alto riesgo y situaciones de seguridad en deterioro.

6.2. Medidas organizativas

6.2.1 Las medidas organizativas mencionadas en el párr. 4.2.4 de la PPD no son exhaustivas. Se alienta a los controladores de datos, asistidos por sus puntos focales de protección de datos y otros funcionarios pertinentes, a:

(i) A nivel de país, asegurarse de que las medidas relevantes de seguridad de datos estén incluidas en los Procedimientos Operativos Estándar (párr. 4.2.4 (i) de la PPD), por ejemplo, procedimientos para la gestión de expedientes físicos y electrónicos;

(ii) Asegurarse de que las capacitaciones en protección de datos sean organizadas o atendidas, incluso para las agencias implementadoras (párr. 4.2.4 (ii) y párr. 5.4 de la PPD);

(iii) Sensibilizarse sobre el uso responsable de los activos y recursos de TIC del ACNUR, incluidos el correo electrónico, Internet, dispositivos portátiles y equipos de TIC;

(iv) Asegurarse de realizar evaluaciones de impacto de protección de datos (párr. 4.2.4 (iii) de la PPD);

(v) Implementar métodos de transferencia segura para los datos personales de las personas de interés;

(vi) Revisar y actualizar de manera rutinaria las medidas de seguridad de los datos, por ejemplo, a través de un monitoreo aleatorio e inspecciones y pruebas, evaluando y verificando la efectividad de las medidas existentes;

(vii) Compartir los SOP pertinentes con el Oficial de Protección de Datos y mantenerlo informado sobre las medidas de las organizaciones.

[48] ACNUR, *Directrices operacionales sobre seguridad de la TIC, aprobado por el Director y el Oficial Jefe de Información (CIO), DIST*, octubre de 2014, en inglés.

[49] Ídem, en la Sección 3.

6.3. Medidas técnicas

6.3.1 Bajo medidas técnicas, la Política de Protección de Datos menciona el mantenimiento de la seguridad física de los locales, equipos portátiles, expedientes de casos individuales y registros (párr. 4.2.5 (i) y la seguridad de la TIC a través de una serie de medidas de control (párr. 4.2.5 (ii) de la PPD). Esta sección profundiza en la gestión de expedientes físicos y electrónicos y distingue el almacenamiento, acceso y control del usuario que se aplican a ambas formas de la gestión de archivos. Para la definición del expediente de caso individual, consulte las definiciones en la Sección 4 de esta Guía. Los controladores de datos pueden delegar la implementación de medidas técnicas en sus puntos focales de protección de datos junto, por ejemplo, con el personal de registro y de TI.

Gestión de archivos físicos

6.3.2 **Control de almacenamiento**. Se aconseja al personal responsable observar lo siguiente:

(i) Los expedientes de los casos se guardan en una sala de almacenamiento con cerradura o en una ubicación designada para este propósito dentro de las instalaciones del ACNUR, a salvo de daños ocasionados por agua, fuego y temperatura;

(ii) El acceso a la sala de almacenamiento debe ser controlado, monitoreado o restringido, por ejemplo, por tarjetas de acceso, barreras de control físico, sistemas de monitoreo locales o remotos, o con acceso solo para el personal autorizado para ingresar;

(iii) El lugar de almacenamiento debe mantenerse cerrado con llave cuando está desatendido. Las copias de las llaves/tarjetas de acceso normalmente son guardadas solo por el personal de registro/archivo y el representante y/o el personal de protección superior;

(iv) Fuera de la sala de almacenamiento, los expedientes de casos deben guardarse en un archivador o cajón cerrado con llave cuando el personal que se encarga de ellos no se encuentra en su escritorio o está fuera de la oficina, incluso durante los descansos cortos;

(v) Los archivos no deben mantenerse en las salas de entrevistas a menos que haya personal presente;

(vi) Se debe regular el acceso a las instalaciones del ACNUR, se debe registrar el ingreso y la salida de los visitantes y estos deben ser acompañados por el personal del ACNUR dentro de las instalaciones y oficinas (se puede consultar al Asesor de Seguridad en el Terreno o al Servicio de Seguridad en el Terreno).

6.3.3 **Control del acceso** a los archivos físicos (dentro y fuera del lugar de almacenamiento designado).

(i) Los trabajadores sociales deben tener acceso a los expedientes físicos de los casos que les han sido asignados, de acuerdo con sus funciones y

responsabilidades, por ejemplo, el registro, RSD, BIA/BID, reasentamiento o tareas específicas;

(ii) Los oficiales revisores deben tener acceso a los expedientes de los que son responsables de revisar y cuya calidad deben verificar, de acuerdo con sus funciones y responsabilidades;

(iii) El personal que no es de protección solo puede solicitar acceso a los expedientes de casos a través del Oficial Superior de Protección (o su equivalente) dentro de cada oficina;

(iv) Los intérpretes normalmente no deben tener acceso a los expedientes de casos individuales. Cuando excepcionalmente se les han asignado tareas relacionadas con el tratamiento de casos, según lo aprobado por el controlador de datos, el acceso a los expedientes individuales debe limitarse estrictamente a los documentos necesarios relacionados con las responsabilidades autorizadas, y debe supervisarse de cerca.

6.3.4 **Control de usuario**. Rastreo y registro del movimiento de expedientes físicos:

(i) Se debe implementar un procedimiento de registro de salida/registro de ingreso, con una lista actualizada de quién tiene, y quién ha tenido en el pasado, acceso a expedientes de casos individuales;

(ii) El Archivador de Expedientes debe registrar el número del expediente, la fecha y las iniciales/nombre de la persona funcionaria que solicita el expediente en el registro de movimiento del expediente al momento de su entrega, y anotar su fecha de devolución y las iniciales/nombre de la persona funcionaria que lo devolvió.

(iii) Las solicitudes, entregas, transferencias y devoluciones de expedientes normalmente deben registrarse en una Hoja de Acción de Expediente. Los registros del movimiento de expedientes deben almacenarse electrónicamente en la medida de lo posible (en proGres o en una base de datos alternativa). Las operaciones más grandes también pueden considerar la implementación de un sistema de rastreo electrónico adjuntando códigos de barras a sus expedientes y emitiendo identificación con códigos de barras al personal;

(iv) El personal del ACNUR no puede sacar expedientes de casos individuales de las instalaciones del ACNUR. Las excepciones pueden ser autorizadas por el controlador de datos u oficial superior de protección basado en una solicitud por escrito. Debe haber un límite a la cantidad de expedientes de los que puede disponer un solo trabajador social en cualquier momento dado (normalmente un máximo de 20).

6.3.5 Asesoramiento general sobre la **gestión de expedientes de casos individuales**:

(i) Crear, recopilar y verificar expedientes de casos individuales al momento del registro;

(ii) Marque los expedientes claramente en el exterior con el número del expediente (o con una identificación única);

(iii) En principio, un expediente para una persona de interés en una oficina para su uso de todas las unidades funcionales;

(iv) Inserte una hoja de acción, que incluya todas las acciones y fechas relacionadas con el caso (entrevistas programadas, remisiones, visitas a domicilio, documentos agregados o eliminados, etc.) y manténgalo actualizado;

(v) Mantenga los documentos en orden cronológico (los documentos más recientes colocados en la parte superior);

(vi) Fotografías no digitalizadas recomendadas sujetas a medidas de protección contra la manipulación (tales como los sellos de sello seco o húmedo), con el nombre y el número de registro de la persona de interés en la parte posterior;

(vii) Marque todos los documentos que son copias con "copia" o "copia de copia";

(viii) Guarde solo copias de documentos originales proporcionados por una persona de interés y devuelva el original. La copia debe ser anotada como "copia" y "vista original";

(ix) Las notas internas deben ser fechadas y firmadas, con el nombre y título del trabajador social;

(x) Considere la posibilidad de guardar información estrictamente confidencial, por ejemplo, registros médicos, en un sobre sellado y a prueba de manipulaciones, claramente marcado como tal, dentro del expediente físico.

Gestión de expedientes electrónicos

6.3.6 Los datos personales almacenados en formato electrónico son particularmente vulnerables a la destrucción, pérdida o alteración accidental, ilegal o ilegítima, así como a la divulgación no autorizada, debido a la facilidad con la que pueden copiarse, transferirse e incluso publicarse en Internet. El acceso a tales datos debe, por lo tanto, ser cuidadosamente restringido, administrado y monitoreado. Los controladores de datos, con el apoyo cercano de los oficiales de TI, son responsables de garantizar que las bases de datos y la infraestructura de TI de soporte se establezcan y utilicen conforme a la norma, incluidas las siguientes medidas:

6.3.7 **Control de almacenamiento**

(i) Se recomienda a las operaciones que solo utilicen herramientas corporativas del ACNUR, aplicaciones de gestión de documentos y unidades de red con accesibilidad controlada (en caso de duda, soliciten ayuda y asesoramiento de la DIST). El uso de herramientas no aprobadas por el ACNUR ("TI en las sombras") puede socavar la seguridad de los datos;

(ii) Las ubicaciones de los servidores deben ser físicamente seguras, con una adecuada seguridad eléctrica, de agua y contra incendios. Los oficiales de TI son responsables de los procedimientos de respaldo adecuados;

(iii) Se recomienda a las oficinas con acceso confiable a Internet que almacenen expedientes electrónicos en e-SAFE; las oficinas sin dicho acceso deben establecer una unidad compartida restringida. Los datos personales de las personas de interés no se deben almacenar en las unidades de red personales.

6.3.8 **Control de acceso a expedientes electrónicos**

(i) El acceso a los expedientes electrónicos debe ser escalonado, de modo que el personal solo tenga acceso a lo que necesita para el cumplimiento de sus funciones y responsabilidades;

(ii) Se recomienda que las operaciones establezcan procedimientos para la presentación y revisión de solicitudes de acceso de usuarios para garantizar que los usuarios solo tengan acceso a los datos que necesitan. Los derechos de acceso normalmente son definidos por los Jefes de Unidades, aprobados por el controlador de datos y actualizados por un administrador de la base de datos de conformidad con las instrucciones administrativas sobre la gestión de controles de acceso emitidas por la DIST[50];

(iii) Se recomienda una revisión periódica de los derechos de acceso, por ejemplo, cada 6 meses, para garantizar que se revoquen los permisos del personal que ya no requiere acceso.

Grabación de audio y video al asesorar y entrevistar a las personas de interés

6.3.9 Las operaciones que utilizan la grabación de audio al asesorar o entrevistar deben garantizar que estas grabaciones se almacenen de forma segura (preferiblemente en e-SAFE) con acceso restringido solo para personal autorizado. Los dispositivos de grabación deben mantenerse en una ubicación segura, y todas las copias electrónicas de videos/cintas deben estar claramente vinculadas a un expediente físico, y deben desecharse de manera segura cuando haya transcurrido su periodo de conservación o hayan dejado de ser necesarios. Se recomienda a las operaciones que estén considerando introducir cámaras en salas de entrevistas y/o grabación de video para entrevistar a las personas de interés que consulten al DPO, a la FSS y la DIST en la Sede, para tomar la mejor decisión basada en consideraciones de seguridad, protección de datos y gestión de casos.

6.4. Privacidad desde el diseño y por defecto

6.4.1 Además de la necesidad de implementar medidas organizativas y técnicas apropiadas, la Política de Protección de Datos adoptó el enfoque de privacidad desde el diseño y por defecto, brevemente descrito en la Política como tecnologías y herramientas para mejorar la protección de datos para permitir que los procesadores de datos mejoren la protección de los datos personales (párr. 4.2.3 de la PPD). Desarrollado por el Comisionado de Información y Privacidad de Ontario, respaldado posteriormente por la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC) e incluida en el RGPD (Artículo 25), la privacidad desde el diseño debe entenderse como un concepto holístico aplicable a las operaciones en toda la organización, de principio a fin, incluidas sus prácticas empresariales de tecnología de la información, procesos, diseño

[50] ACNUR, *Instrucción administrativa sobre gestión de controles de acceso para sistemas, aplicaciones y servicios de TIC*, marzo de 2018, en inglés.

físico e infraestructura de red.[51] Por lo tanto, el concepto en la Política de Protección de Datos debe entenderse de acuerdo con la terminología y la práctica establecidas, incluidos los "Principios Fundamentales" de la privacidad desde el diseño adoptado por el ICDPPC: (1) Proactiva no Reactiva; Preventiva no correctiva, (2) Privacidad por defecto, (3) Privacidad incorporada en el diseño, (4) Funcionalidad completa: suma positiva, no suma cero, (5) Protección de ciclo de vida de principio a fin, (6)) Visibilidad y transparencia, (7) Respeto por la privacidad del usuario.[52]

6.5. Procedimientos y prácticas de seguridad de los datos

6.5.1 La seguridad de los datos se trata de tecnología, activos y recursos de TIC, pero aún más sobre su uso. La investigación muestra repetidamente que el error humano es la causa principal de filtraciones de datos e infracciones de seguridad. Las débiles prácticas de seguridad de datos por parte del personal (el factor humano) pueden socavar los esfuerzos del ACNUR para proteger los datos personales, por ejemplo, aumentando los riesgos de ataques cibernéticos o de la “ingeniería social”. Todo el personal con acceso a los activos y recursos de TIC del ACNUR (incluyendo herramientas básicas como computadoras y correos electrónicos) debe, por lo tanto, familiarizarse con los procedimientos y prácticas de seguridad de datos existentes y evitar comportamientos que puedan poner en riesgo los datos personales de las personas de interés y, en sentido más amplio, las operaciones del ACNUR. Un breve resumen de estos procedimientos y prácticas incluye:

Uso seguro de los activos y recursos de TIC (incluido el correo electrónico e Internet)

6.5.2 Todo el personal del ACNUR está obligado por las políticas internas sobre el uso del correo electrónico, Internet, así como el uso personal de computadoras y otros recursos tecnológicos.[53] El Boletín del Secretario General sobre el Uso de los recursos y datos de la tecnología de la información y la comunicación también se ha introducido al ACNUR a través de estas políticas.[54] Este último, entre otras cosas, prohíbe ciertas actividades en línea del personal de las Naciones Unidas y responsabiliza a todos los usuarios por su uso personal de los recursos de TIC (incluidas todas las actividades y contenidos creados, transmitidos o mostrados a través de los servicios de Internet). Todo el personal del ACNUR es llamado a completar los cursos obligatorios básicos y avanzados de Concientización sobre Seguridad de la Información disponibles para el personal y los socios del ACNUR en la plataforma “*Learn and Connect”* del ACNUR.

6.5.3 En términos de prácticas recomendadas, se anima a todo el personal del ACNUR a:

[51] Ver ICDPPC, *Resolución sobre Privacidad por Diseño*,32ªConferencia Internacional en Jerusalén, Israel, 27-29 de octubre de 2010, disponible en inglés en: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf..

[52] Ver arriba. Para obtener más información sobre los Principios Fundamentales, consulte: Comisionado de Información y Privacidad de Ontario, *Privacidad por Diseño*, revisado en septiembre de 2013, disponible en inglés en: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.

[53] ACNUR, *Política de correo electrónico* (2006, revisado en 2012); *Uso personal de computadoras del ACNUR y otros recursos tecnológicos*, junio de 2005 y *Política de uso apropiado de Internet*, diciembre de 2009, en inglés.

[54] Naciones Unidas, *Boletín del Secretario General sobre el uso de los recursos de las tecnologías de la información y la comunicación*, 20 de noviembre de 2004, ST / SGB / 2004/15, disponible en inglés en: https://oios.un.org/resources/2015/01/ST-SGB-2004-15.pdf.

(i) **Mantener una sana desconfianza y una postura defensiva** con respecto a personas y comunicaciones desconocidas, por ejemplo, al no hacer clic en los enlaces o abrir archivos adjuntos en correos electrónicos que provengan de direcciones desconocidas o que parezcan sospechosas, divulgar información confidencial sobre ellos mismos o sus colegas en sitios web inseguros o dar contraseñas a otros;

(ii) **Seguir prácticas seguras de navegación en Internet**. El ACNUR utiliza el filtrado web para proporcionar protección básica a sus usuarios. El personal del ACNUR no debe instalar reproductores de video o extensiones de navegador en sus PC sin el asesoramiento de un Oficial de TI, ya que estos pueden contener *malware/*software malicioso;

(iii) **Mantenerse actualizado**. Las computadoras que no tienen antivirus, parches o firewalls actualizados son mucho más propensas a infectarse por aplicaciones y software malicioso ("malware"). Los Oficiales de TI deben asegurarse de que todas las computadoras de la oficina estén usando software y sistemas operativos actualizados y software antivirus con licencia, para descargar e instalar automáticamente;

(iv) **Reportar cualquier actividad sospechosa** al GSD para permitir medidas rápidas y efectivas. Las potenciales infracciones, como las cuentas o los sistemas comprometidos, las computadoras perdidas o robadas, la liberación no autorizada de información protegida, el tiempo de inactividad del sistema y la detección de software malicioso, también deben notificarse al controlador de datos.

Uso seguro de equipos TIC portátiles (incluidas computadoras portátiles, teléfonos inteligentes y unidades USB)

6.5.4 Las computadoras portátiles, tabletas, teléfonos inteligentes y otros dispositivos portátiles tienen la ventaja de ser utilizados fuera de las instalaciones del ACNUR, pero pueden perderse o ser robados, lo que puede ocasionar la pérdida de datos personales y un posible acceso no autorizado. Los dispositivos portátiles también pueden ser más vulnerables a software malicioso/*malware*, y es menos probable que los usuarios apliquen los últimos parches de seguridad y tengan sistemas operativos menos seguros. Para limitar los riesgos para las personas de interés, se recomienda que todo el personal del ACNUR:

(i) Minimice la cantidad de datos personales de las personas de interés almacenados en sus dispositivos portátiles, incluyendo en teléfonos inteligentes y computadoras portátiles;

(ii) Asegure que todos los dispositivos portátiles estén protegidos con contraseña/PIN, respete la orientación para el uso de contraseñas[55], los configure con 'bloqueo automático' cuando no estén en uso y los mantengan con ellos o en lugares seguros en todo momento;

(iii) Los dispositivos portátiles o extraíbles (como unidades USB y tarjetas de memoria) en principio no deben usarse para almacenar o transferir datos personales. Si su uso es inevitable, los dispositivos deben estar encriptados

[55] ACNUR, *Uso de contraseñas en los sistemas informáticos del ACNUR*, Memorándum de abril de 2009, en inglés.

(solicite asesoramiento del Oficial de TI), mantenerse físicamente seguros y los datos deben ser borrados inmediatamente después de la finalización de la tarea;

(iv) El personal del ACNUR que devuelve un dispositivo al ACNUR debe asegurarse de que borra todos sus correos electrónicos, mensajes y cualquier otro archivo que pueda contener datos personales de las personas de interés;

(v) Los dispositivos perdidos o robados que se han utilizado para datos personales deben enviarse al controlador de datos y al Oficial de TI, y las contraseñas deben modificarse de inmediato.

Uso seguro de los activos de las TIC durante viajes de misión y los acuerdos de trabajo a distancia

6.5.5 El trabajo a distancia y los viajes de misión conllevan riesgos adicionales, ya que las redes y los recursos podrían no ser tan seguros. Todo el personal del ACNUR debe conocer lo siguiente:

(i) Las **redes públicas de Wi-Fi y los puntos de acceso abiertos** (es decir, que no requieren una contraseña) representan el mayor riesgo, ya que los usuarios pueden estar expuestos al '*sniffing*'/"olfateo" (la captura de datos enviados a través de redes inseguras) y '*man in the middle attacks*'/"ataques de intermediarios" (usando puntos de acceso Wi-Fi falsos o maliciosos), y con mayor riesgo de virus, "*spyware*"/programas espías, "*malware*"/software malicioso e intentos de "phishing". Por lo tanto, se advierte al personal que evite tales redes. Si se usa de forma excepcional, el intercambio de archivos debe desactivarse, la configuración de la red inalámbrica se cambia a 'pública' y el personal estará atento a actividades sospechosas. El personal del ACNUR que esté considerando utilizar las aplicaciones de la Red Virtual Privada (VPN, por sus siglas en inglés) debe ponerse en contacto con el GSD o con un Oficial de TI antes de instalar dichas aplicaciones;

(ii) Se recomienda al **personal que trabaja desde su casa** que se asegure de que sus redes inalámbricas sean seguras. Se debe controlar el acceso a las redes, aplicar el protocolo de seguridad WPA2 y reemplazar las contraseñas predeterminadas del administrador del enrutador. Busque el consejo del Oficial de TI;[56]

(iii) **Los guardias fronterizos en cada vez más países** exigen que las personas abran sus computadoras portátiles, enciendan teléfonos móviles e ingresen o entreguen contraseñas para acceder a los datos en dichos dispositivos. En tal situación, se aconseja al personal del ACNUR que cumpla con una solicitud para abrir sus dispositivos electrónicos para permitir una inspección visual no intrusiva (a efectos de verificar que los dispositivos funcionen), pero no para permitir que se abre, lea o descargue documentos. Las solicitudes para la entrega de códigos pin o contraseñas, o para examinar el dispositivo sin que esté en presencia del personal responsable deben ser rechazadas. Si es necesario, el personal debe solicitar ver al supervisor de los guardias para dejar en claro que los dispositivos contienen documentos del ACNUR que son confidenciales e inviolables como parte de los archivos del ACNUR.

[56] Para obtener más información, consulte, por ejemplo: https://support.microsoft.com/es-es/hub/4099151/windows-security-help, o https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/securing-your-home-network.

6.6. Comunicaciones y transferencias de datos seguras

6.6.1 Existe un alto riesgo de filtraciones de datos cuando los datos personales se comunican o se transfieren, por ejemplo, del ACNUR a un tercero. Los correos electrónicos y mensajes SMS pueden ser interceptados durante la transmisión y/o retenidos por programas de vigilancia, poniendo así a las personas de interés en riesgo de sufrir daños, en particular si son accedidos por los países de origen. Sobre este tema, la Política de Protección de Datos establece que "con el fin de garantizar y respetar la confidencialidad, los datos personales deben (...) transferirse sólo a través del uso de medios de comunicación protegidos (párr. 4.1.2 y 6.1.2 (v)).

6.6.2 A fin de reducir el riesgo de filtraciones de datos personales durante la comunicación y transferencia de datos personales, se recomienda al personal de ACNUR que:

(i) En principio, use solo **herramientas desarrolladas y aprobadas por el ACNUR** para transferir datos personales;

(ii) Tenga **cuidado** con el uso de herramientas de intercambio de archivos de terceros;

(iii) Es imposible garantizar la confidencialidad de cualquier mensaje electrónico transmitido fuera del sistema del ACNUR a través de Internet. **Ninguna información de carácter confidencial debe ser enviada por correo electrónico a través de Internet**.[57] Las alternativas más seguras incluyen el uso de e-SAFE, el servicio de transferencia segura de archivos (FTP) del ACNUR y los dispositivos de medios portátiles encriptados;

(iv) Los datos personales **no deben ser transferidos usando cuentas de correo electrónico personales** (por ejemplo, Gmail, Yahoo o Hotmail), o a través de cuentas de redes sociales (por ejemplo, Facebook, Twitter);[58]

(v) Si se usa el correo electrónico, asegurarse de que **se tomen medidas adicionales para proteger el contenido,** como el cifrado del correo electrónico o su archivo adjunto. Al compartir archivos protegidos con contraseña, la contraseña debe enviarse a través de un medio alternativo de comunicación (como una llamada telefónica o un mensaje de texto);

(vi) Los **SMS deben evitarse como un medio para comunicar datos personales**, tanto internamente dentro del ACNUR, como externamente y con personas de interés. Los servicios de mensajería de texto encriptados de principio a fin son más seguros que los mensajes SMS y deben usarse en su lugar;

(vii) **Solicite asesoramiento** del Oficial de TI, GSD o la Sección de Seguridad de TIC de la DIST sobre qué herramientas usar para diferentes propósitos y en diferentes escenarios operativos.

Comunicación con las comunidades a través de "SMS masivos" y aplicaciones de mensajería

[57] ACNUR, *Política de correo electrónico*, junio de 2006, párr. 5.5.3, en inglés.
[58] ACNUR, *Instrucción administrativa sobre el uso de las redes sociales*, septiembre de 2014, párr. 5.1.6, en inglés.

6.6.3 Los SMS masivos y las aplicaciones de mensajería presentan oportunidades para mejorar la comunicación con las comunidades desplazadas, en particular en áreas que son de difícil acceso para el ACNUR.[59] Sin embargo, el personal del ACNUR debe estar consciente de la posible falta de seguridad relacionada con estas herramientas, que pueden revelar la identidad y ubicación de individuos o comunidades a terceros, así como recopilar datos personales y metadatos, y facilitar el acceso para los organismos encargados de hacer cumplir la ley y otras autoridades estatales. Estos riesgos se exacerban aún más en el caso de las plataformas basadas en la web, la encriptación inadecuada o los proveedores de servicios radicados en países diferentes a los remitentes y/o destinatarios.[60]

6.6.4 Para minimizar los riesgos de protección, el ACNUR recomienda el uso de tales herramientas solo para fines como transmisiones de emergencia o seguridad, la gestión de distribución de asistencia y monitoreo. Deben, en la medida de lo posible, evitarse para proteger la información sensible. Además, se debe consultar al Oficial Superior de Seguridad de Información (CISO, por sus siglas en inglés) y, cuando corresponda, al OPD sobre la elección de la aplicación y el proveedor del servicio. Normalmente, se requeriría de una Evaluación de impacto de protección de datos (DPIA, por sus siglas en inglés) para tales iniciativas.

[59] ACNUR, *Conectar a los refugiados: Cómo el internet y la conectividad móvil pueden mejorar el bienestar de los refugiados y transformar la acción humanitaria*, 2016, disponible en: http://www.acnur.org/fileadmin/Documentos/Publicaciones/2018/11442.pdf.

[60] Véase también CICR, *Manual sobre la protección de datos en la acción humanitaria*, Capítulo 11 y CICR, *Futuros humanitarios para aplicaciones de mensajería: Comprendiendo las oportunidades y los riesgos para la acción humanitaria*, enero de 2017, disponible en inglés en: https://www.icrc.org/en/publication/humanitarian-futures-messaging-apps.

El uso de herramientas de encuestas electrónicas

6.6.5 El uso de herramientas de encuestas y dispositivos móviles para recopilar datos de personas de interés permite evaluaciones más eficientes que los sistemas en papel. A la luz de los posibles desafíos de protección de datos, se recomienda encarecidamente al personal que consulte con la FICCS y el Oficial de TI (o el CISO) para seleccionar herramientas y modalidades de encuesta que garanticen que los datos personales solo se recopilen, procesen y retengan de acuerdo con los requisitos de la Política.

6.7. Entornos de alto riesgo y situaciones de seguridad en deterioro

6.7.1 La Política de Protección de Datos reconoce que el tratamiento de datos personales por parte del ACNUR puede tener lugar en situaciones de seguridad en deterioro o entornos de alto riesgo (párr. 4.2.6). Por lo tanto, el controlador de datos debe tomar medidas para la gestión de datos personales en caso de una posible evacuación o reubicación. Esto podría hacerse en varios niveles, incluido el plan de contingencia, seguridad o respuesta, así como los procedimientos operativos estándar (SOP) internos. Se recomienda hacer ***asignaciones claras de responsabilidad para la decisión y la implementación*** de la eliminación o destrucción de todos los activos y registros que contengan datos personales de las personas de interés en archivos físicos y electrónicos. También se recomienda incluir el tema en las capacitaciones de seguridad y la lista de verificación de inducción estándar para el personal recién llegado.

6.7.2 En el caso de una **reubicación o evacuación**, el controlador de datos, con el apoyo del Oficial de TI y el Asesor de Seguridad en el Terreno, es responsable de supervisar que todas las computadoras, servidores, sistemas de respaldo y archivos en papel se transfieran a una **ubicación segura**, de ser posible. Cuando esto no se pueda lograr, el controlador de datos también puede decidir, **como último recurso, destruir** los activos y registros para evitar que los datos personales caigan en manos de personas que puedan causarles daño a las personas de interés del ACNUR.

6.7.3 Para evitar que ocurra lo anterior y, en general, para reducir el riesgo de filtraciones de datos como resultado de una evacuación o un posible incidente de seguridad, se recomienda a los controladores de datos que consideren la digitalización de los documentos impresos que contienen datos personales en consulta con la RAS[61]. Otras medidas de seguridad de datos, incluido el uso de encriptación, también pueden reducir el riesgo de exposición no autorizada como resultado de una evacuación, reubicación o incidente de seguridad. Solicite el apoyo del Oficial de TI, o CISO en la Sede, cuando sea necesario.

[61] Véase ACNUR, *Directrices operativas para la digitalización (para la conversión de registros analógicos a formato digital)*, 2015, junio de 2015, en inglés.

7. Filtraciones de datos personales y su notificación

7.1. Concepto de filtraciones de datos personales

7.1.1 La Política de Protección de Datos define una filtración de datos personales como "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" (párr. 1.4)[62]. Por lo tanto, las filtraciones de datos personales pueden ser el resultado de errores internos o intrusiones externas. A menudo, implicarán también una violación de la confidencialidad, es decir, personas no autorizadas que acceden a los datos personales de las personas de interés. La gravedad y el impacto de una filtración de datos personales pueden variar. Además, si se comunican al público u a otras partes interesadas, las filtraciones de datos personales pueden minar la reputación y la confianza en la integridad de las operaciones del ACNUR. De ahí la **importancia de manejar las filtraciones de datos personales de manera ordenada, incluida la notificación** de dichas filtraciones, tal como se ha visto en la Política de Protección de Datos y se complementa con esta Guía.

7.1.2 Como se ve en la definición, el concepto de filtración de datos personales abarca una serie de situaciones. **El acceso no autorizado a datos personales** puede ser el resultado de negligencia, tal como credenciales de inicio de sesión comprometidas, causado por ataques a activos de TIC diseñados para minar u obstruir deliberadamente las actividades del ACNUR u obtener una recompensa financiera, o una consecuencia de la vigilancia o la interceptación de las comunicaciones o transferencias. También existen "amenazas internas" vinculadas con el fraude y la corrupción, y el robo y la confiscación de dispositivos portátiles de TIC. Además, **la pérdida o el daño a los datos personales** pueden ser el resultado de que las computadoras portátiles, los servidores o los dispositivos portátiles se pierden o son robados, infectados con "*malware*"/software malicioso o dañados debido a peligros naturales o provocados por el hombre. La negligencia también puede conducir a una filtración de datos, por ejemplo, copias de seguridad inadecuadas o cuando los documentos, incluidos los datos personales se imprimen y se dejan desatendidos.

7.2. Categorización de filtraciones de datos personales

7.2.1 A efectos de las medidas de seguimiento y presentación de informes, las filtraciones de datos personales pueden clasificarse como menores, importantes o graves en función de los siguientes criterios: (i) la cantidad de personas de interés del ACNUR y otras personas afectadas; (ii) el riesgo de daño grave a la(s) persona(s) afectada(s); (iii) la indicación de cualquier problema sistémico o de gran escala en los sistemas físicos o de

[62] Esta definición corresponde con el artículo 4 párr. 12 del RGPD.

seguridad de TIC del ACNUR; y (iv) el potencial de atención de los medios u otras partes interesadas como resultado de la filtración.

7.2.2 Las **filtraciones de datos menores** representan un riesgo mínimo para las personas de interés y la integridad de las operaciones del ACNUR**,** por ejemplo, negligencia por parte del personal, dispositivos móviles perdidos que pueden ser manejados adecuadamente por la operación, teniendo en cuenta el desempeño del personal y los procedimientos disciplinarios, según proceda.

7.2.3 Las **filtraciones de datos importantes** representan un riesgo significativo para la protección, la seguridad o los derechos fundamentales de las personas de interés o las comunidades afectadas, o para la integridad de las operaciones del ACNUR, por ejemplo, las fallas en la seguridad de los datos que conducen al acceso a datos personales por parte de personas ajenas al organización, infracciones menores de los sistemas de gestión de seguridad de las TIC o computadoras robadas o dispositivos móviles que contengan datos personales.

7.2.4 Las **filtraciones de datos graves** afectan a un gran número de personas de interés o representan un riesgo importante para la protección, la seguridad o los derechos fundamentales de las personas de interés, sus familiares y asociados y/o las comunidades afectadas, o para la integridad general de las operaciones del ACNUR, por ejemplo, el saqueo o la evacuación de las oficinas de ACNUR, las infracciones graves de los sistemas de gestión de seguridad de la TIC o la publicación de datos personales de las personas de interés en Internet.

7.3. Cómo responder a la filtración de datos personales

7.3.1 Con respecto a la respuesta a las filtraciones de datos personales, la Política de Protección de Datos menciona el registro y la notificación por parte del personal del ACNUR al controlador de datos, del controlador de datos al Oficial de Protección de Datos (DPO) y la comunicación con el titular de los datos (párr. 4.4.1. La Política también se refiere a medidas de mitigación e implica una evaluación de las consecuencias adversas conocidas y previsibles de una filtración de datos personales (párr. 4.4.2 y 4.4.3). Al responder a filtraciones de datos personales, uno puede distinguir los pasos claves: evaluación, mitigación, registro y notificación.

7.3.2 **Evaluación**. Al darse cuenta de una filtración de datos personales real o potencial se deben evaluar varios factores:

(i) Registros de datos y tipo de datos personales afectados;

(ii) Fecha, hora, duración y ubicación;

(iii) Causa de la filtración de datos;

(iv) Lista de titulares de datos afectados;

(v) Riesgo de daño grave a los titulares de los datos;

(vi) Riesgo de otras consecuencias adversas (operativas, de seguridad, financieras, daños a la reputación).

7.3.3 **Mitigación**. La prioridad es de tomar medidas para poner fin a la filtración y prevenir nuevas infracciones. Según la evaluación, es posible que se necesiten varias medidas:

(i) Si es probable que se produzcan daños o perjuicios personales, comunique la filtración de los datos personales al titular de los datos (párr. 4.4.2 de la PPD). Los riesgos para el titular de los datos pueden, en el mejor de los casos, evaluarse junto con las personas afectadas, por ejemplo, si los detalles de la identidad, ubicación o solicitud de asilo de una persona solicitante de asilo se han comunicado a las autoridades del país de origen. El asesoramiento debe comunicar la filtración de datos de manera objetiva, resaltando cualquier incertidumbre relacionada con los eventos de manera clara y transparente, e intentar responder a cualquier pregunta o inquietud del individuo(s) con la debida consideración a sus circunstancias, situación y antecedentes individuales;

(ii) Preparar o implementar medidas de seguimiento para la protección de los titulares de los datos. Esto podría incluir el cambio de números de teléfono o tarjetas SIM, pero también medidas de protección física inmediatas, tales como la reubicación o apoyo de la policía local, con el consentimiento de las personas involucradas y en cooperación con el Asesor de Seguridad en el Terreno;

(iii) Medidas relacionadas con la TIC hasta la activación del Plan de Respuesta a incidentes de las TIC;

(iv) Establecer sistemas de monitoreo de seguridad.

7.3.4 **Registro y Notificación**. Las filtraciones de datos personales deben registrarse y notificarse (párr. 4.4.1 de la PPD) por razones de rendición de cuentas, una comprensión adecuada de las causas y consecuencias y para prevenir futuras filtraciones. El registro y la notificación deben incluir los elementos mencionados en el párr. 4.4.3 de la PPD junto con los puntos mencionados anteriormente bajo 'Evaluación'. Las siguientes acciones deben observarse:

(i) Todo el personal del ACNUR debe notificar una filtración de datos personales real o interrumpida al controlador de datos. El controlador de datos también puede designar el punto focal de protección de datos para recibir tales notificaciones. Debe entenderse que tales notificaciones iniciales podrían no contener todos los elementos mencionados en el párr. 4.4.3 de la PPD. El registro puede completarse a medida que la evaluación continua;

(ii) De acuerdo con la Política de Protección de Datos, el controlador de datos debe notificar al Oficial de Protección de Datos si es probable que una filtración de datos personales resulte en perjuicios o daños personales a un titular de datos (párr. 4.4.2). En cuanto a las categorías mencionadas arriba, esto significa que se debe notificar al Oficial de Protección de Datos sobre todas las infracciones importantes y graves. La notificación al Oficial de Protección de Datos debe tener lugar dentro de un plazo de 72 horas tras conocerse una filtración importante y 24 horas después de conocerse una infracción grave.[63] Con el fin de facilitar la función de monitoreo del Oficial de Protección de Datos, también se promueve

[63] Véase también en este sentido el artículo 33 (1) del RGPD (Reglamento General de Protección de Datos).

la notificación de filtraciones menores y, en cualquier caso de duda con respecto a si las infracciones son importantes o graves.

7.3.5 Además de los pasos claves mencionados anteriormente, esta Guía recomienda a los controladores de datos conformar un **Equipo de Respuesta a Filtraciones de Datos** compuesto por personal con la antigüedad, experiencia técnica y diversidad necesarias para responder de manera efectiva a las filtraciones de datos personales. Un Equipo de Respuesta a Filtraciones de Datos incluiría el controlador de datos, el punto focal de protección de datos, el personal de protección y registro, el asesor de seguridad en el terreno y el oficial de TI (o Asistente), y en la medida de los recursos disponibles en una operación en el terreno y pertinentes para la filtración de datos específica, la gestión de información o datos, el programa y el personal de programas y relaciones externas. Podría activarse en infracciones importantes y graves.

7.3.6 En el caso de filtraciones de datos graves, un Equipo de Respuesta a Filtraciones de Datos a nivel de país también podría ser respaldado por colegas pertinentes a nivel de la Sede, incluido el

(i) Oficial de Protección de Datos;

(ii) El Oficial Jefe de Seguridad de la Información de ICT (toma la iniciativa para contener las filtraciones de seguridad cibernética que afectan los sistemas y las herramientas TIC corporativas del ACNUR y para rectificar los problemas sistémicos en los sistemas de gestión de seguridad de TIC del ACNUR);

(iii) La Sección de Seguridad en el Terreno (FSS, por sus siglas en inglés), (lidera las infracciones de las estructuras físicas de seguridad o el acceso a las instalaciones, y puede brindar apoyo en situaciones donde la filtración causa riesgos de seguridad para las personas de interés o el personal, así como para apoyar las investigaciones);

(iv) Sección de Gestión y de la Identificación y Registro (IMRS), (en el caso de que una filtración esté relacionada con las herramientas de registro corporativo del ACNUR, tales como ProGres, BIMS, etc.);

(v) División de Protección Internacional (DIP) y personal regional de protección (en el caso de filtraciones de datos que puedan causar riesgos de protección a personas de interés individuales o a comunidades de personas de interés);

(vi) El Servicio de Asuntos Jurídicos (LAS), (si la filtración es causada por un proveedor de servicios comerciales o una agencia implementadora y se deben tomar medidas para suspender o rescindir el contrato o asociación pertinente, o existe una solicitud de indemnización de daños y perjuicios);

(vii) Oficina Regional (para la supervisión y evaluación de riesgos operativos o de reputación);

(viii) Relaciones externas (si se requiere una estrategia de comunicación); y

(ix) Oficina del Inspector General (OIG) (obligatorio si existe alguna sospecha de mala conducta del personal del ACNUR, potencialmente también para consultas *ad hoc* sobre ataques graves a los activos del ACNUR).

7.3.7 El abordar firmemente las filtraciones de datos personales es una de las mejores maneras en que una operación puede construir una "cultura de protección de datos" y **prevenir filtraciones en el futuro**. En los casos en que la evaluación de la filtración de datos personales haya mostrado una debilidad en los procedimientos, herramientas o sistemas del ACNUR, es posible que se requiera su revisión y mejora, por ejemplo, planes y/o Procedimientos Operativos Estándar actualizados de seguridad y respuesta. Del mismo modo, una filtración que ha indicado un grado de conciencia inadecuado entre el personal relacionado con la protección de datos, incluidos los procedimientos y las prácticas de seguridad de datos, puede requerir que la operación haga mayores esfuerzos en capacitación/fortalecimiento institucional.

7.4. Filtraciones de datos personales con agencias implementadoras y terceros

7.4.1 Cualquiera de las posibles filtraciones de datos enumeradas anteriormente también podría ocurrir con los socios o terceros, a quienes el ACNUR ha transferido datos personales. Por lo tanto, es esencial que todos los contratos de servicio, MDE, Acuerdos de Colaboración para Proyectos, Acuerdos de Transferencia de Datos y otros compromisos por escrito relacionados con el tratamiento de datos de las personas de interés incluyan disposiciones estándar sobre la notificación de filtraciones de datos al ACNUR, y cooperación con respecto a posibles medidas de mitigación.[64]

7.4.2 Los pasos claves para responder a las infracciones de datos personales enumerados anteriormente también pueden ser relevantes para las filtraciones de datos que ocurren con las agencias implementadoras del ACNUR o terceros. Cuando sea necesario, el ACNUR debe ayudar a las agencias implementadores a crear o mejorar su capacidad para prevenir o mitigar el riesgo de filtraciones de datos que afecten los datos personales de las personas de interés (véase también el párr. 5.4 de la PPD). El Servicio de Gestión de Agencias Implementadoras (IPMS) y el Servicio de Asuntos Legales (LAS) deben ser consultados sobre medidas de mitigación en el caso de una filtración de datos con un socio o proveedor de servicios comerciales.

8. Evaluaciones de impacto de protección de datos

8.1. Una herramienta y un proceso

8.1.1 En el párr. 4.5, de la Política de Protección de Datos se introduce el concepto de Evaluaciones de Impacto de Protección de Datos (DPIA). Según la definición en el párr. 1.4 de la Política, una DPIA es "**una herramienta y un proceso** para evaluar los impactos sobre la protección de los interesados en el tratamiento de sus datos personales y para identificar acciones correctivas según sea necesario, con el fin de evitar o minimizar tales

[64] ACNUR, *Acuerdo de asociación de proyecto bipartito de formato estándar (ACNUR con organizaciones no gubernamentales y otras organizaciones sin fines de lucro)*, para. 13.22, en inglés.

impactos". Las DPIA, también conocidas como Evaluaciones de Impacto de Privacidad (PIA), son hoy en día una característica común en numerosas leyes de privacidad y protección de datos[65] y las autoridades nacionales de protección de datos y otros organismos han desarrollado un amplio material de orientación sobre DPIA/PIA.[66] A la luz de la práctica existente, **una DPIA puede servir para varios propósitos**:

(i) Determinar y evaluar los posibles impactos o riesgos relacionados con el tratamiento de datos personales;

(ii) Identificar y evaluar procesos alternativos para mitigar dichos riesgos;

(iii) Mejorar la toma de decisiones informadas para los controladores de datos (gerentes);

(iv) Implementar el enfoque de privacidad desde el diseño y por defecto;

(v) Demostrar el cumplimiento de los principios de protección de datos y que la protección de datos se tome en serio;

(vi) Contribuir a la confianza y seguridad en la organización.

8.1.2 Estos propósitos de una DPIA son igualmente válidos para el ACNUR. Las DPIA como herramienta de rendición de cuentas y un proceso para construir y demostrar el cumplimiento son particularmente importantes en una organización internacional que, debido a su estructura institucional y los mecanismos limitados de recursos y sanciones, debe enfocarse en acciones preventivas para garantizar el cumplimiento. Además, la posición particularmente vulnerable de las personas de interés del ACNUR y la naturaleza generalmente sensible de sus datos personales (véase el párr. 1.2.1 del DPP) hablan a favor de la **importancia de las DPIA en el contexto del tratamiento de datos del ACNUR[67]**. Finalmente, existe un fuerte vínculo entre las DPIA y el enfoque de privacidad desde el diseño y por defecto (párr. 4.2.3 de la PPD) en el sentido de que una DPIA puede proporcionar un sistema de alerta temprana, una forma de detectar problemas de protección de datos y crear salvaguardas antes y no después de realizar inversiones importantes, por ejemplo, en costosos sistemas tecnológicos.

8.2. ¿Cuándo llevar a cabo una evaluación de impacto de la protección de datos?

8.2.1 Con respecto a la **programación**, la Política sugiere que una DPIA se debe llevar a cabo "Al elaborar nuevos sistemas (...) o antes de firmar (...) acuerdos" (párr. 4.5.1. Solo cuando se realiza **durante las etapas de planificación y diseño de nuevas iniciativas de tratamiento de datos**, es decir, antes de comprar y poner en marcha un sistema o

[65] Véase, para todos los Estados miembros de la UE, el artículo 35 de la RGPD; véase también la Sección 208 (b) de la Ley de Gobierno Electrónico de los Estados Unidos de 2002, disponible en inglés en: https://www.gpo.gov/fdsys/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf.

[66] Véase también el Grupo de trabajo sobre protección de datos del artículo 29, *Directrices sobre la evaluación del impacto de la protección de datos (DPIA)*, WP 248 del 4 de abril de 2017, disponible en inglés en: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, página 4; Comisión Nacional de Información y Libertades (CNIL, por sus siglas en francés), *Software PIA, herramienta y guías,* 2018, disponible en inglés en: https://www.cnil.fr/en/tag/Privacy+Im-Pacto + Evaluación + (PIA); Comisionado de Información Australiano, *Guía para realizar evaluaciones de impacto de privacidad*, disponible en inglés en: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments; Gobierno de Canadá, *Directiva sobre la evaluación del impacto de la privacidad*, disponible en: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308; y la Organización Internacional de Normalización (ISO), *Pautas para la evaluación del impacto de la privacidad*, ISO/IEC 29134:2017, en: https://www.iso.org/standard/62289.html (para la compra).

[67] Véase también, con respecto a los titulares de datos vulnerables, el Grupo de Trabajo del Artículo 29 de Protección de Datos, *Directrices sobre la Evaluación de impacto de la protección de datos (DPIA)*, página 9.

firmar un acuerdo, puede una DPIA cumplir su propósito no solo de evaluar sino también de prevenir riesgos. Sin embargo, una DPIA aún puede llevarse a cabo para evaluar y mitigar los riesgos de protección de datos que surgen de proyectos que ya están en funcionamiento.

8.2.2 Con respecto al **alcance material**, se deduce de la lógica sobre la importancia de la DPIA en el entorno de tratamiento de datos del ACNUR que es **ampliamente interpretada y aplicada**. Al mismo tiempo, no todos los actos de tratamiento de datos o asociación requerirán de una DPIA. El párr. 4.5.1 de la PPD se refiere a "nuevos sistemas, proyectos o políticas o (...) acuerdos de transferencia de datos con agencias implementadoras o con terceros", así como a "la recopilación y el tratamiento o la transferencia de datos personales (que) es probable que sean extensiva, repetida o estructural". Además, solo se requiere una DPIA **cuando el tratamiento pueda tener un impacto negativo sobre la protección de los titulares de datos**. Con base en la Política, esta Guía brinda el siguiente asesoramiento para determinar si una DPIA es necesaria (análisis del umbral):

8.2.3 **Las nuevas tecnologías** o sistemas, herramientas, módulos o plataformas de tratamiento de datos, incluidas las bases de datos interoperables o compartidas, que se perciben o se espera que conlleven riesgos de privacidad inherentes, deben, por una cuestión de principios, someterse a una DPIA. Esto incluye, por ejemplo, la recopilación de datos biométricos, el almacenamiento en la nube, la analítica de datos masivos, la inteligencia artificial, los drones, los sistemas automatizados de toma de decisiones, las comunicaciones bidireccionales utilizando medios sociales, los teléfonos inteligentes o SMS masivos.

8.2.4 Una DPIA es muy recomendable en caso de **transferencias de conjuntos de datos personales a una socio o tercero**, ya sea una ONG, una agencia o un proveedor de servicios comerciales, con presuntas debilidades de protección de datos y/o cuando la evaluación del nivel de protección de datos (requerida en base al párr. 6.1.4 de la PPD) es difícil, por ejemplo, debido a la ausencia de estatutos y políticas internas de protección de datos o la falta de trayectoria y experiencia en cooperación, teniendo también en cuenta las leyes aplicables, la cultura local y el contexto de funcionamiento específico y de seguridad.

8.2.5 También se puede recomendar una DPIA en el caso del tratamiento de **datos personales particularmente sensibles,** en particular cuando el ACNUR recibe o transfiere esos datos a socios o terceros. Esto puede incluir expedientes médicos, incidentes de VSG o de protección, orientación sexual y/o necesidades de protección graves, datos sobre un grupo particularmente vulnerable, por ejemplo, una minoría étnica o religiosa.

8.2.6 En el caso de una combinación de lo anterior, por ejemplo, el tratamiento de datos personales particularmente sensibles que involucra transferencias a un tercero con un presunto historial débil de protección de datos y/o en un entorno arriesgado usando nueva tecnología, una DPIA sería necesariamente requerida.

8.3. ¿Cómo llevar a cabo una evaluación de impacto de la protección de datos?

8.3.1 Al tiempo que enfatiza la naturaleza de una DPIA como un **proceso**, la Política elabora menos en este aspecto. De acuerdo con los estándares de la industria, la orientación para el proceso de DPIA consiste en varios pasos.[68]

(i) Análisis del umbral, es decir, si es necesaria una DPIA;

(ii) Preparación de la DPIA, que incluye conformar un equipo, planificar, asignar recursos, identificar y consultar a las partes interesadas;

(iii) Llevar a cabo la DPIA, incluida la identificación de los flujos de datos personales, la determinación de los requisitos de salvaguarda de protección de datos, la identificación del riesgo, el análisis y la evaluación y definición de opciones o alternativas;

(iv) Seguimiento, incluida la preparación del informe y un resumen público, implementar planes de manejo de riesgos y revisar o actualizar la DPIA.

8.3.2 Un resultado clave de una DPIA es la presentación de un **informe**. La PPD incluye una reseña bastante detallada cuando establece que "Una DPIA debe contener una descripción general del sistema, el proyecto, la política o el acuerdo de intercambio de datos previsto que implica el tratamiento 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" (párr. 4.5.2).

8.3.3 Una DPIA se puede llevar a cabo internamente por el ACNUR o externamente. El informe DPIA debe constar de 6 partes:

(i) Información sobre la persona responsable de la DPIA

(ii) Descripción de la iniciativa

(iii) Mapeo de las partes interesadas

(iv) Mapeo de flujos de datos y entorno operacional

(v) Identificar y evaluar los riesgos

(vi) Recomendaciones y revisión

8.3.4 Se recomienda una DPIA externa para desafiar las iniciativas de tratamiento de datos que involucran datos particularmente sensibles, tecnologías complejas y/o múltiples actores. También podría recomendarse después de una DPIA interna que ha identificado riesgos importantes de protección de datos. Una DPIA externa normalmente se diseñaría con el apoyo de la Oficina Regional y/o la Sede. También puede ser apropiado llevar a cabo una evaluación externa, utilizando expertos calificados en protección de datos, teniendo en cuenta el contexto operativo y los recursos disponibles. Los términos de referencia deben diseñarse en estrecha consulta con el Oficial de Protección de Datos.

[68] Véase ISO/IEC 29134: 2017, Sección 6 (Orientación sobre el proceso para llevar a cabo una Evaluación de Impacto de Privacidad (PIA))

8.3.5 Una DPIA puede referirse a una sola operación de tratamiento de datos a nivel de país o un conjunto de operaciones de tratamiento similares (véase el párr. 4.5.3 de la PPD). Una sola operación de tratamiento de datos, por ejemplo, el asunto de la firma y el acuerdo de transferencia de datos con un tercero específico en una operación específica del país normalmente se haría internamente. Sin embargo, existen varias situaciones en el contexto del ACNUR donde puede ser razonable, económico y de acuerdo con el enfoque de privacidad desde el diseño realizar DPIA a nivel global que cubran un conjunto de operaciones de tratamiento similares. Esto se aplicaría al uso por parte del ACNUR de una serie de productos tecnológicos combinados en el Ecosistema de Registro y Gestión de Identidad de la Población (PRIMES). Los módulos principales (p. ej., BIMS) y las herramientas (p. ej., GDT o RAIS) están desarrollados y aprobados por el ACNUR para ser utilizados globalmente, incluso con organizaciones socias. También podría aplicarse cuando el ACNUR considere utilizar un sistema de tecnología desarrollado por un tercero. En ambos casos, una DPIA externa podría ser más apropiada.

8.4. Implementación

8.4.1 La persona responsable de la decisión de realizar una DPIA es el controlador de datos (párr. 4.5.3 de la PPD). Él o ella también tiene que aprobar el informe DPIA y, con base en los hallazgos, decidir si procede con la iniciativa de tratamiento de datos y, de ser así, cómo proceder. Él o ella puede asignar al punto focal de protección de datos el análisis del umbral, si se requiere una DPIA y/o puede consultar al Oficial de Protección de Datos para obtener más información. Si, y una vez que se toma la decisión para una DPIA, también se designaría normalmente al punto focal de protección de datos para la organización del proceso y la entrega del informe DPIA. El punto focal de protección de datos puede contar con el respaldo de un equipo multifuncional, compuesto por servicios de protección, registro, programas y servicios comunitarios, personal de TI y seguridad. Tras su finalización, el controlador de datos debe validar el informe DPIA. Como se establece en la PPD, y para verificar la calidad y adecuación de las DPIA, se requiere que los controladores de datos mantengan al Oficial de Protección de Datos plenamente informado y le compartan una copia del informe. También se recomienda que los hallazgos se compartan con las partes interesadas y los proveedores de servicios, según proceda, a fin de asistir con la implementación de sus recomendaciones y por motivos generales de transparencia y rendición de cuentas (véase arriba en propósitos de una DPIA).

9. Intercambio y transferencias de datos

9.1. Contexto y concepto de intercambio y transferencias de datos

9.1.1 La Política de Protección de Datos reconoce que, **en el ejercicio de su mandato de proporcionar protección internacional y soluciones, a menudo se requiere que el ACNUR** procese datos personales de personas de interés, incluso **para compartir datos personales con las agencias implementadoras y/o terceros** (párr. 1.2.1). Si bien las

agencias implementadoras se definen en términos concretos, la noción de tercero incluye una persona física o jurídica distinta del titular de los datos, el ACNUR o una agencia implementadora (véase las definiciones en el párr. 1.4 de la PPD). Esto refleja la gran variedad de actores con los que el ACNUR colabora, incluidos gobiernos, organizaciones intergubernamentales, no gubernamentales, agencias de la ONU, organizaciones comunitarias, universidades, el poder judicial y el sector privado[69]. Las alianzas y la cooperación con otros actores están incorporadas en el Estatuto del ACNUR, han sido el tema de varias iniciativas y ocupan un lugar destacado en las Direcciones Estratégicas del ACNUR 2017-2021[70]. El ACNUR actualmente mantiene más de 900 alianzas y confía alrededor del 40% de sus gastos anuales a sus socios.

9.1.2 La Política de Protección de Datos aborda la transferencia de datos personales a terceros en su Capítulo 6. La transferencia de datos personales es una forma de tratamiento de datos (consulte la definición de tratamiento de datos personales en el párr. 1.4) pero la Política no define transferencias. Además, la Política también utiliza ocasionalmente el término intercambio de datos (párr. 1.2.1, 4.5.1, 6.2.1 y 7.3.1). Una visión contextual del uso de ambos términos permite concluir que la Política no los distinguen.[71] Considerando el uso del término transferencias en otros instrumentos, en particular el RGPD,[72] las transferencias de datos personales normalmente implicarían los elementos de **comunicación, divulgación o la puesta a disposición de datos personales, realizadas con el conocimiento o la intención del remitente de que los destinatarios tendrán acceso** a ellos.[73]

9.2. Requisitos generales para transferencias de datos

9.2.1 Si bien la Política de Protección de Datos reconoce la necesidad de compartir datos personales con las agencias implementadoras y terceros (párr. 1.2.1), también reconoce los posibles riesgos de protección de datos involucrados en las transferencias a terceros (párr. 6.1.2). Por un lado, el mandato de protección del ACNUR requiere que minimice los riesgos de filtraciones de datos personales debido a las transferencias; por otro lado, el ACNUR debe ser pragmático y tener en cuenta, por ejemplo, los diferentes niveles de capacidades de protección de datos de terceros, así como las diferentes jurisdicciones nacionales a las que pueden estar sujetos. Por lo tanto, el enfoque con respecto a los datos personales debe tener principios con un nivel de flexibilidad. Esta es la razón por la cual la Política de Protección de Datos exige que los **terceros brindan un nivel de protección de datos igual o comparable a la Política del ACNUR** (párr. 6.1.1).

9.2.2 Con respecto al significado de "normas iguales o comparables", la Política de Protección de Datos no contiene una definición fija. Sin embargo, teniendo en cuenta el

[69] Véase solo http://www.unhcr.org/partnerships.html.

[70] ACNUR, *Direcciones estratégicas del ACNUR 2017-2021*, 16 de enero de 2017, disponible en: http://www.acnur.org/fileadmin/Documentos/BDL/2017/11039.pdf?file=fileadmin/Documentos/BDL/2017/11039 pág. 13/14.

[71] Por ejemplo, 6.2.1 de la PPD usa ambos términos. El Manual del CICR también utiliza ambos términos sin distinción, véase el Capítulo 2, párr. 2.12 en la página 49.

[72] Véase el Capítulo V de la RGPD sobre la Transferencia de datos personales a terceros países u organizaciones internacionales y la Resolución de Madrid de la ICDPPC utilizando el término transferencias internacionales.

[73] Véase el Supervisor Europeo de Protección de Datos (SEPD*), La transferencia de datos personales a terceros países y organizaciones internacionales por instituciones y organismos de la UE*, Documento de posición de 14 de julio de 2014, disponible en inglés en: https://edps.europa.eu/sites/edp/files/publica-tion / 14-07-14_transfer_third_countries_en.pdf, a página 7; El Manual del CICR adopta una definición muy similar del término (internacional) de intercambio de datos, véase el Capítulo 2, párr. 2.12 en la página 49 y en el Capítulo 4 (Intercambio internacional de datos).

objeto y el propósito de la Política, cada tercero debe, en principio, respetar los **principios básicos del tratamiento de datos personales como se establece en el párr. 2.1 de la PPD**, es decir, tratamiento legítimo y justo, especificación de objetivos, necesidad y proporcionalidad, precisión, respeto de los derechos de los titulares de los datos, confidencialidad, seguridad y rendición de cuentas y supervisión. En el párr. 6.1.2 punto (v) y (vi), la PPD destaca la **confidencialidad** ("acuerdo por escrito") **y seguridad de datos** ("alto nivel de seguridad de datos").

9.2.3 El **nivel de protección de datos proporcionado por un tercero debe evaluarse antes de comprometerse a transferir datos personales**. Esto es lo que el párr. 6.1.4, junto con el párr. 7.2.2 de la PPD requiere del controlador de datos. La misma disposición también proporciona orientación para tales evaluaciones al referirse a "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". **La mejor manera de llevar esto a cabo esta evaluación es a través de una DPIA** (véase párr. 6.1.4 con referencia al párr. 4.5 de la PPD). Se hace referencia al párr. 11.2 de esta Guía.

9.2.4 Además del nivel de protección de datos ofrecido por el tercero, el **acto de la transferencia de datos personales en sí debe cumplir las condiciones establecidas por la Política de Protección de Datos**. Según el párr. 6.1.2 (i) a (iv) de la PPD, las transferencias de datos deben basarse en una base legítima, para uno o más propósitos específicos y legítimos, se limitará a los datos personales que sean adecuados, pertinentes, necesarios y no excesivos en relación con el o los propósitos y el titular de los datos debe ser informado. Al registrar instancias específicas de intercambio de datos con terceros (véase el párr. 7.3.1 (ii) de la PPD), se asesora al personal del ACNUR referirse a estas condiciones. Adicionalmente, el párr. 6.1.2 (v) y 4.1.2 de la PPD requieren que los datos personales solo se transfieran mediante el uso de medios de comunicación protegidos.

9.2.5 Finalmente, basado en el párr. 6.1.3, " 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 un 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 apolítica". Estas consideraciones son de carácter general y no están estrictamente relacionadas con los principios de protección de datos. Esto también se aplica a los **privilegios e inmunidades del ACNUR**. Según el párr. 6.5, las transferencias de datos personales se efectúan sin perjuicio de los privilegios e inmunidades del ACNUR y no deben interpretarse como si lo fueran.

9.3. Consejos prácticos para transferencias a terceros

9.3.1 Al plantear la necesidad de cumplir al menos con un nivel de protección de datos comparable a la Política del ACNUR, el ACNUR podría enfrentar una falta de comprensión,

apreciación y/o capacidad entre los terceros. El asesoramiento en tales situaciones es el de abordar el problema de manera positiva al explicar la justificación de la protección de datos y ofrecer medidas para mejorar las capacidades de protección de datos, por ejemplo, al:

(i) Brindar a todos los socios y terceros información sobre los fundamentos de los requisitos de la Política, por qué la protección de los datos personales redunda en el interés común tanto del ACNUR como de sus socios, y lo que esto significa en la práctica;

(ii) Incluir la protección de datos como parte del proceso de selección para socios, y como parte de la evaluación intermedia, para que cualquier inquietud pueda abordarse de manera oportuna;

(iii) Buscar confirmación por escrito de que existen salvaguardias apropiadas ya en las primeras etapas de la negociación de un Acuerdo de Transferencia de Datos;

(iv) Incluir la creación de capacidad de protección de datos y/o capacitación en la agenda de grupos de trabajo temáticos de organizaciones humanitarias involucradas en el intercambio amplio de datos (por ejemplo, grupos de trabajo de protección o efectivo).

9.3.2 Con respecto al tema de la evaluación de terceros, en particular la verificación de las normas de seguridad de información de los proveedores de servicios comerciales se asesora al personal del ACNUR que:

(i) Use solamente proveedores de servicios reconocidos y conocidos;

(ii) Solicite información sobre el uso de, e idealmente, la certificación en estándares de la industria en procesos y procedimientos de seguridad, estándares de la nube, SMS masivos, encriptación/criptología y estándares de servicios financieros;[74]

(iii) Se asegure de que la protección de datos y la seguridad de la información estén claramente establecidas en las solicitudes de propuestas y en las evaluaciones de los posibles proveedores de servicios;

(iv) Solicite el apoyo del Oficial de TI y, si es necesario, el Director de Seguridad de Información (CISO) en la Sede, para la selección de proveedores de servicios;

(v) Siempre pregunte a los proveedores de servicios comerciales sobre la ubicación de sus centros de datos y sobre cualquier transferencia transfronteriza que se lleve a cabo como parte de su tratamiento de los datos de las personas de interés (incluido el país de origen de las personas refugiadas);

(vi) Pregunte sobre la legislación nacional en los países en los que la empresa almacena y procesa datos, y en qué medida reciben y cumplen con las solicitudes de datos de las autoridades nacionales encargados de hacer cumplir la ley u otras autoridades.

9.3.3 Un cierto nivel de riesgos debido a la falta de capacidad o legislación nacional puede ser compensado a través de acuerdos contractuales con el tercero, la implementación de

[74] A saber, familia ISO/IEC 27000 - Sistemas de gestión de la seguridad de la información, disponible en inglés en: https://www.iso.org/isoiec-27001-in-formation-security.html.

procedimientos estrictos de minimización de datos y la limitación de los derechos de acceso basados en las recomendaciones de una DPIA y en consulta con el Oficial de Protección de Datos y el Servicio de Asuntos Legales (LAS). Sin embargo, si el nivel de las normas de protección de datos ofrecidas por un tercero no puede ser verificado o mitigado satisfactoriamente a través del fortalecimiento institucional y/u otros esfuerzos, el ACNUR no debe aceptar la transferencia de datos personales.

9.4. Acuerdos de transferencia de datos

9.4.1 Cuando es probable que las transferencias de datos personales sean grandes, repetidas o estructurales, es decir, cuando el mismo tipo de datos se comparte con el mismo tercero para el mismo fin durante un cierto período de tiempo, el controlador de datos debe tratar de firmar un acuerdo de transferencia de datos (párr. 6.2.1 de la PPD). Por lo tanto, a menos que las transferencias sean esporádicas e impredecibles, los **acuerdos de transferencia de datos son la regla**. Al referirse a "A menos que existan motivos suficientes para no hacerlo", la Política reconoce que la firma de un acuerdo podría no ser posible o, en situaciones muy excepcionales, no ser apropiado. Ejemplos de esto incluyen las primeras etapas de una emergencia y la renuencia de un tercero con el que el intercambio de datos es, sin embargo, necesario para fines de protección más amplios.

9.4.2 En el párr. 6.2.2, la PPD menciona una serie de puntos que deben ser incluidos en un acuerdo de transferencia de datos. Esta lista, sin embargo, no pretende ser exhaustiva. El Servicio de Asuntos Legales y el Oficial de Protección de Datos han desarrollado **muestras de acuerdos de transferencia de datos** que incluyen disposiciones sobre los siguientes temas: objeto y propósito, datos personales a transferir, transferencia de elementos de datos adicionales, medios de transferencia de datos, propósitos específicos de transferencia, transferencia a terceros, seguridad de datos, notificación de filtración, resolución de conflictos, privilegios e inmunidades. Se puede contactar al Servicio de Asuntos Legales y al Oficial de Protección de Datos en la Sede para obtener copias de dichos acuerdos y mayor orientación. El Oficial de Protección de Datos y el Servicio de Asuntos Legales también deben revisar y eliminar todos los acuerdos de transferencia de datos antes de la finalización (párr. 6.2.3 de la PPD). Se recomienda a los controladores de datos que mantengan un inventario actualizado de todos los acuerdos de transferencia de datos en su operación y presenten copias finales con el Oficial de Protección de Datos.

9.5. Acceso a las bases de datos del ACNUR y bases de datos compartidas

9.5.1 Cuando los terceros o agencias socias requieren un acceso continuo a los datos personales de las personas de interés, puede ser eficiente proporcionarles **acceso a una base de datos del ACNUR** o establecer una base de datos compartida o interoperable, en lugar de transferir regularmente grandes cantidades de datos. Si bien el ACNUR en principio está abierto a tales arreglos, debe hacerse dentro de las condiciones y requisitos para la transferencia de datos como se describe anteriormente y como se establece en la Política. Por ejemplo, dicho acceso siempre debe estar regulado por un acuerdo formal, ya sea un Acuerdo de Transferencia de Datos independiente o un anexo al Acuerdo de Colaboración para Proyectos (PPA), que establezca, como mínimo, los términos y el

propósito de uso, el personal autorizado para acceder a los datos, los conjuntos de datos a acceder y cualquier mecanismo de supervisión y rendición de cuentas. El acceso debe limitarse a los conjuntos de datos que sean necesarios y proporcionales para que el socio cumpla con el propósito especificado únicamente.

9.5.2 En el caso de bases de datos compartidas o interoperables, se recomienda una DPIA para identificar y mitigar los riesgos para las personas de interés y que se verifique que la base de datos esté protegida de acuerdo con la Política. Se recomienda buscar cualquier orientación adicional que sea necesaria del Oficial de Protección de Datos, la Sección de Gestión y Registro de Identidad (IMRS) y la División de Sistemas de Información y Telecomunicaciones (DIST) en la Sede.

9.6. Datos personales recibidos de terceros

9.6.1 El ACNUR puede recibir datos personales de socios o terceros, de acuerdo con su mandato. En tales situaciones, el ACNUR debe tratar de recibir tales datos a través de transferencias de datos seguras, siempre que sea posible, solo conservar esos datos si tienen una base legítima para hacerlo y registrar claramente la fuente de dichos datos, si es que se conservan. Los datos personales que no cumplan con estos estándares deben eliminarse de forma segura.

10. Tratamiento de datos personales por parte de las agencias implementadoras

10.1. Agencias implementadoras como procesadores de datos

10.1.1 Considerando la importancia de la cooperación del ACNUR con las agencias implementadoras (definición estándar en párr. 1.4 de la PPD), incluido el tratamiento de los datos personales de las personas de interés por parte de las agencias implementadoras, la Política de Protección de Datos aborda esta situación en un capítulo separado. En el párr. 5.1, la Política aclara que "cuando la recopilación y tratamiento de datos personales es una de las responsabilidades de las agencias implementadoras, los datos personales están siendo recopilados y procesados **en nombre del ACNUR**". En otras palabras, y de acuerdo con la definición en el párr. 1.4, las agencias socias son procesadores de datos.

10.1.2 Esto significa que una serie de **responsabilidades que incumben al controlador de datos**, por ejemplo, el determinar la base legítima aplicable y los fines específicos y legítimos del tratamiento de datos, sigue siendo tarea del ACNUR. También significa que se espera que las agencias socias respeten las **normas iguales o comparables y principios básicos de protección de datos personales** como figura en la Política del ACNUR (párr. 5.1 de la PPD). Por estas razones y basado en el párr. 5.3 de la PPD, el Acuerdo de Colaboración para Proyectos Estándar (PPA) contiene una serie de cláusulas

específicamente relacionadas con la protección de información personal.[75] Estos acuerdos también deben indicar la base legítima y el o los propósitos específicos para el tratamiento de datos y los acuerdos para la terminación de la asociación. Cuando se proporciona acceso a las agencias socias a una base de datos del ACNUR, se recomienda un anexo al PPA para regular los derechos de acceso y las condiciones del usuario del socio.

10.2. Verificación y asistencia a las agencias implementadores

10.2.1 La estrecha relación entre el ACNUR y sus agencias implementadoras también conlleva la responsabilidad del ACNUR de verificar que el tratamiento de datos personales por parte de la agencia implementadora cumpla con los estándares y principios de protección de datos del ACNUR (párr. 5.2 de la PPD) y para asegurar que las agencias implementadoras tengan la capacidad necesaria para cumplir y puedan necesitar proporcionar la asistencia pertinente (véase el párr. 5.4 de la PPD). Las preocupaciones o deficiencias en la capacidad de protección de datos de las agencias socias se pueden abordar a través de asistencia técnica y/o capacitación proporcionada, o respaldada por, el ACNUR. A modo de ejemplo, se pueden implementar las siguientes medidas:

(i) Asesoramiento sobre medidas para mejorar la seguridad física de sus oficinas;

(ii) Asesoramiento sobre posibles medidas para mejorar sus prácticas de seguridad de TI/datos, gestión de archivos físicos y transferencia de datos;

(iii) Organizar capacitación sobre protección de datos y su importancia para las personas de interés;

(iv) Apoyo para establecer o ajustar los procedimientos para obtener el consentimiento de las personas de interés;

(v) Asistir al socio en el desarrollo de procedimientos para garantizar los derechos básicos de las personas de interés;

(vi) Alentar al personal asociado a acceder a y completar el programa eLearning sobre conciencia de la seguridad de la información en Learn & Connect (HQInfoSec@unhcr.org);

(vii) Apoyar el desarrollo de Procedimientos Operativos Estándar (SOP) para abordar problemas específicos de protección de datos, como el uso de dispositivos electrónicos portátiles o herramientas de encuestas.

[75] ACNUR, *Acuerdo de asociación de proyecto bipartito de formato estándar (ACNUR con organizaciones no gubernamentales y otras organizaciones sin fines de lucro)*, párr. 13.17 a 13.25.

11. Rendición de cuentas y supervisión

11.1. Principio y estructura de rendición de cuentas

11.1.1 Numerosos instrumentos de protección de datos reconocen **la rendición de cuentas como un principio**.[76] En sus Directrices de 1990, la Asamblea General pidió a los países que designaran a la autoridad para ser responsable de supervisar el cumplimiento de los principios.[77] El fundamento de un principio de rendición de cuentas se basa en la suposición de que, a menos que la protección de datos se convierta en parte de los valores y prácticas compartidos de una organización, y sus responsabilidades estén claramente asignadas, el cumplimiento de los principios de protección de datos estará en riesgo continuo.[78] En otras palabras, la rendición de cuentas se ve como un **impulsor para la implementación efectiva de los principios de protección de datos**. En el párr. 2.9, la Política de Protección de Datos del ACNUR sigue esta tendencia.

11.1.2 Según el párr. 7.1 de la PPD, la estructura de rendición de cuentas y supervisión del ACNUR se compone de tres actores claves, **controladores de datos en cada oficina de país/operación, puntos focales de protección de datos y un Oficial de Protección de Datos (DPO)** en la Sede. A continuación, esta Guía elabora el concepto y la noción del controlador de datos en el contexto del ACNUR, el papel de los puntos focales de protección de datos y del Oficial de Protección de Datos.

11.2. Controlador de datos y puntos focales de protección de datos

11.2.1 El concepto de controlador de datos está intrínsecamente vinculado con el principio de rendición de cuentas. En consonancia con los instrumentos claves de protección de datos, el ACNUR introdujo la noción de controlador de datos y le asignó la **responsabilidad principal de cumplimiento de la Política** (párr. 7.2.1 de la PPD). Basado en la **autoridad de un Representante en el país**, entre otras cosas, para definir las estrategias y prioridades del país, aprobar la estrategia de protección del país y garantizar el cumplimiento local de las normas de protección mundiales del ACNUR, incluidos los procedimientos operativos de registro, determinación de la condición de refugiado y reasentamiento, de acuerdo con las necesidades y el contexto operacionales,[79] la Política define al controlador de datos como "El miembro del personal del ACNUR, por lo general el Representante de una oficina de ACNUR en el país, que tiene la autoridad para

[76] OECD, *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, septiembre de 1980, revisado en julio de 2013, disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf ; ICDPPC, *La resolución de Madrid*, Principio 11; Artículo 5 (2) del RGPD.
[77] Asamblea General de las Naciones Unidas, *Directrices para la regulación de archivos de datos personales computarizados*, adoptada por la Resolución 45/95 de 14 de diciembre de 1990, disponible en inglés en: http://www.refworld.org/pdfid/3ddcafaac.pdf, párr. 8.
[78] Véase el artículo 29 del Grupo de trabajo sobre protección de datos, *Dictamen 3/2010 sobre el principio de responsabilidad*, WP 173 del 13 de julio de 2010, disponible en inglés en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf, página 2.
[79] Manual del ACNUR, Capítulo 2, *Estructura Organizacional y Responsabilidades, Responsabilidades y Autoridades*, Presencia en el terreno de ACNUR, ARA generales – oficinas de país.

supervisar la gestión y determinar los propósitos del tratamiento de datos personales (párr. 1.4 de la PPD).

11.2.2 Por lo tanto, el concepto del controlador de datos sigue el **control fáctico sobre el tratamiento de datos personales basado en la estructura organizacional y la rendición de cuentas, responsabilidades y autoridades establecidas** en el ACNUR. Al insertar el término 'generalmente', la política toma en cuenta la naturaleza fáctica y no formal del controlador de datos, que también puede estar a nivel regional o de la Sede, así como delegado, para responsabilidades específicas, por ejemplo, a un Representante Adjunto o Auxiliar. La noción de controlador de datos en la Política del ACNUR sirve para fines internos de rendición de cuentas, no tiene ninguna incidencia en la calidad como controlador de datos del ACNUR como entidad organizacional desde la perspectiva de terceros. Además, aunque no se menciona explícitamente, la Política de Protección de Datos no excluye situaciones de **controladores de datos conjuntos**, donde dos o más controladores de datos determinan conjuntamente los propósitos y medios del tratamiento de datos personales.[80] Para los controladores de datos conjuntos, es importante determinar claramente sus respectivas responsabilidades para el cumplimiento de los principios de protección de datos. En el caso de cooperación con terceros y/o el uso de bases de datos conjuntas, esto podría hacerse en acuerdos o protocolos.

11.2.3 Los controladores de datos son asistidos por **puntos focales de protección de datos**. La función del DPFP es ayudar al controlador de datos a cumplir sus responsabilidades con respecto a la Política (véase el párr. 1.4); el DPFP debe ser, en principio, la persona funcionaria de protección de más alto rango en una oficina/operación de país (párr. 7.2.1 de la PPD). Con este enfoque pragmático, la Política de Protección de Datos busca colocar la **función del DPFP en un área y en un nivel** (personal de protección de más alto rango) **donde muchas otras funciones relevantes para la protección de datos**, por ejemplo, la supervisión de las unidades de registro, RSD y/o reasentamiento, **ya están asignados**. Los controladores de datos deben designar a un DPFP (párr. 7.1 (iii) y 7.2.1); también pueden solicitar a los Jefes de las Suboficinas u Oficinas en el Terrero que designen a un DPFP a nivel de Suboficina u Oficina en el Terreno, asumir ellos mismos esta función y/o pedir a los DPFP que conformen un equipo de protección de datos con una composición similar o igual al equipo de respuesta a la filtración de datos (véase arriba en el párr. 10.3.5).

11.2.4 A solicitud del controlador de datos, y de acuerdo con el Capítulo 7 de la PPD, el o la DPFP puede asumir las siguientes t**areas**:

(i) Determinar la base legítima para el tratamiento, en particular cuando se requiere el consentimiento del titular de los datos y garantizar que existan procedimientos de consentimiento adecuados (7.2.2 (i));

(ii) Asegurar que los procedimientos para los derechos de los titulares de los datos estén vigentes, atender y responder a las solicitudes de los titulares de los datos (7.2.2 (iii) y anteriores, párr. 8.6.7);

(iii) Coordinar la implementación de medidas organizacionales y de seguridad (7.2.2 (ii));

[80] Véase, por ejemplo, el Artículo 26 del RGPD.

(iv) Llevar a cabo o coordinar las DPIA y las evaluaciones de seguridad de datos de terceros (7.2.2 (iii));

(v) Actuar como primer punto de contacto para el Oficial de Protección de Datos con respecto a las solicitudes de asesoramiento, presentación de informes y solicitud de aprobación de los acuerdos de transferencia de datos.

(vi) Mantener un inventario actualizado de información sobre actividades relevantes de tratamiento de datos personales (párr. 7.3.1 (ii)) incluyendo todas las bases de datos, sistemas de información, asociaciones y acuerdos contractuales. Este inventario debe incluir (según corresponda a cada operación):

a. Procedimientos para crear y probar copias de seguridad, y el personal responsable de esto;

b. La ubicación física de todos los servidores en el terreno y copias de seguridad;

c. Una visión general de los procedimientos de derechos de acceso para expedientes físicos y electrónicos;

d. Acuerdos de transferencia de datos con socios y otros terceros (vigentes y vencidos);

e. DPIA realizadas por la operación;

f. Una visión general de las responsabilidades del personal con respecto a cada sistema de TIC (es decir, el personal responsable de mantenimiento, gestión, apoyo y seguridad de datos);

g. Registros de solicitudes de los titulares de los datos para el acceso, la corrección y eliminación y objeción;

h. Registros de filtraciones de datos personales y respuestas de la operación.

11.3. Oficial de Protección de Datos (DPO)

11.3.1 El párrafo 7.1 de la PPD menciona al Oficial de Protección de Datos (DPO) dentro de la División de Protección Internacional como uno de los actores claves de la estructura de rendición de cuentas y supervisión del ACNUR. Las tareas del Oficial de Protección de Datos se enumeran en el párr. 7.3.1 de la PPD y pueden caracterizarse como asesoramiento, apoyo, capacitación, monitoreo y presentación de informes. La Política sigue la creciente práctica a nivel nacional y regional de requerir Oficiales de Protección de Datos en las autoridades públicas, en particular en cada institución y órgano de las Comunidades Europeas.[81]

11.3.2 Además de las tareas tradicionales de un Oficial de Protección de Datos, la Política de Protección de Datos del ACNUR también confía al Oficial de Protección de Datos la responsabilidad, conjuntamente con el Servicio de Asuntos Legales (LAS), la de revisar y aprobar todos los acuerdos de transferencia de datos (párr. 6.2.3) y brindar asesoría, en

[81] Véase la Sección 8 (Artículos 24 a 26) de la Regulación (CE) No 45/2001 del Parlamento Europeo y el Consejo del 18 de diciembre 2000 sobre la protección de individuos en relación al tratamiento de datos personales por las instituciones y los órganos de la Comunidad y sobre la libre circulación de tales datos. Véase también los artículos 37 a 39 del RGPD y el Grupo de trabajo sobre protección de datos del artículo 29, *Directrices sobre Oficiales de Protección de Datos*, DT 243 adoptado el 13 de diciembre de 2016 (revisado por última vez el 5 de abril de 2017), disponible en inglés en: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

consulta con la Unidad de Protección y Seguridad Nacional dentro de la División de Protección Internacional, el Servicio de Asuntos Legales y la o las Oficinas correspondientes, previo a la transferencia de datos personales a un organismo nacional encargado de hacer cumplir la ley o a un tribunal nacional (párr. 6.3.3). Además, el Oficial de Protección de Datos puede unirse, previa invitación del personal responsable del ACNUR, a los órganos o comités establecidos por otras políticas en áreas de especial relevancia para el tratamiento de datos personales de las personas de interés.

12. Referencias

La Declaración Universal de Derechos Humanos, Artículo 12, disponible en: https://www.un.org/es/universal-declaration-human-rights/

El Pacto Internacional de Derechos Civiles y Políticos, Artículo 17, disponible en: https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Naciones Unidas, *Directrices para la regulación de archivos de datos personales computarizados,* A/RES/45/95, 14 de diciembre de 1990, disponible en inglés en: http://www.un.org/documents/ga/res/45/a45r095.htm

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), *Informe del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital A/HRC/27/37*, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/068/74/PDF/G1406874.pdf?OpenElement

Consejo de Derechos Humanos, *Resumen de la mesa redonda del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital*, A/HRC/28/39, disponible en: http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/39&Lang=S

Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC), *Estándares internacionales sobre protección de datos personales y privacidad (La*

resolución de Madrid), disponible en: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

Organización para la Cooperación y el Desarrollo Económicos (OCDE), *Directrices de privacidad*, disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf

Consejo de Europa, *Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos de Carácter Personal*, 28 enero 1981, ETS No. 108, ya que será modificado por su Protocolo, 25 junio 2018, ETS No. 223 (Convenio modernizado 108), disponible en inglés en: https://rm.coe.int/16808ade9d

Agencia de los Derechos Fundamentales de la Unión Europea (FRA) y el Consejo de Europa, *Manual de legislación europea en materia de la protección de datos* Edición 2018, disponible en: https://rm.coe.int/16806ae663

Organización Internacional para las Migraciones (OIM)*, Manual de protección de datos (2010),* disponible en inglés en: https://publications.iom.int/books/iom-data-protection-manual

Programa Mundial de Alimentos (PMA), *Guía de Protección y Privacidad de Datos Personales*, disponible en inglés en: https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

Comité Internacional de la Cruz Roja (CICR), *Normas del CICR en materia de protección de datos personales*, disponible en: https://www.icrc.org/es/publication/normas-del-cicr-en-materia-de-proteccion-de-datos-personales

El Comité Internacional de la Cruz Roja (CICR) y el Centro de privacidad de Bruselas (VUB), *Manual sobre protección de datos en la acción humanitaria internacional,* disponible en: https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), *Normas de protección de datos y flujos internacionales de datos: Implicaciones para el comercio y el desarrollo*, abril 2016, disponible en inglés en: http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468

GUÍA SOBRE LA PROTECCIÓN DE DATOS PERSONALES DE LAS PERSONAS DE INTERÉS DEL ACNUR

2018

Publicado por
ACNUR
División de Protección Internacional
Apartado postal 2500
1211 Ginebra 2