Versión:	3.0
Publicado por	Comité GDPR
Estado:	Aprobado
Clasificación:	Interno
Fecha de Creación:	30-12-2021
Actualizado:	10/07/2022

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

ASOCIACIÓN COMITÉ ESPAÑOL DE LA UNRWA
(UNRWA España)

INDICE

1. PROPÓSITO, ALCANCE Y USUARIOS

La ASOCIACIÓN COMITÉ ESPAÑOL DE LA UNRWA (en adelante **UNRWA España**) se esfuerza por cumplir con la normativa vigente en materia de protección de datos personales en el desarrollo de todas sus actividades. Esta política establece los principios básicos del tratamiento de datos personales de la Asociación.

La organización trata en su día a día numerosos datos personales de diferentes colectivos (solicitantes de empleo, trabajadores, Junta Directiva, voluntarios, socios, donantes, proveedores, contactos interesados, colaboradores, etc.) y el presente documento tiene por objeto definir la política, responsabilidades, procesos y medidas aprobadas por el Comité de Protección de Datos de **UNRWA España** para dar cumplimiento a la legislación vigente sobre protección de datos y garantizar la adecuación al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales (en adelante, LOPDGDD).

La Junta Directiva de **UNRWA España**[1], a través del Comité de Protección de Datos, establece la política sobre protección de datos personales, que supone el marco de referencia para el desarrollo del resto de normas y procedimientos que gestionan este tipo de datos.

La Política es de aplicación para todos los tratamientos realizados sobre los datos de carácter personal existentes en la Asociación, tal y como se especifica en el correspondiente Registro de Actividades de Tratamiento existente en la entidad.

Para garantizar el cumplimiento de la legislación y la seguridad de los datos personales, se incluyen todos los activos y recursos necesarios en cualquier fase del tratamiento:

- Sistemas de información que los soportan.
- Instalaciones de **UNRWA España**
- Personal interno y externo que gestione o acceda de algún modo durante el tratamiento de los datos.

Por tanto, la presente política es de aplicación a todo el personal de **UNRWA España** con acceso a datos personales. Igualmente, resulta aplicable al personal externo con acceso a los sistemas de información que se encuentra sometido al presente documento.

La Política de privacidad deberá mantenerse permanentemente actualizada. Cualquier modificación relevante de los sistemas de información (automatizados o no), en la organización de los mismos, o en las disposiciones vigentes en materia de protección de datos conllevará la revisión del presente documento, y su modificación total o parcial.

[1] El apoyo de la Junta Directiva es un aspecto esencial para garantizar el éxito de la Política, dado que este respaldo garantiza no sólo disponer de suficientes recursos, sino que el enfoque está alineado con la filosofía y estrategia de nuestra Asociación.

2. REGISTRO DE ACTIVIDADES DE TRATAMIENTO CON DATOS PERSONALES DE UNRWA ESPAÑA

Tal y como dispone el Considerando 82 RGPD, se requiere con carácter previo identificar los tratamientos y los activos implicados, por lo que se parte de la información reflejada en el registro de actividades de tratamiento, tal y como establece el artículo 30 RGPD.

La necesidad de la llevanza del registro de las actividades del tratamiento afecta a **UNRWA España** su calidad de:

- ✓ Responsable del tratamiento, respecto a los tratamientos propios (art. 30.1 RGPD)

Este inventario detallado de tratamientos constituye el alcance y representa el eje a partir del cual se organiza el resto de los procesos (análisis de riesgos, definición de controles, EIPD, etc.) en la gestión proactiva de la protección de datos.

El registro de actividades del tratamiento es una herramienta que permite al responsable/encargado del tratamiento y a la autoridad supervisora (cuando así se solicite) tener una perspectiva general de todas las actividades de tratamiento de datos personales que se llevan a cabo en la Asociación. Es, por tanto, un requisito previo para el cumplimiento de la normativa, y una medida efectiva de rendición de cuentas.

Los registros de las actividades del tratamiento se mantendrán documentados (incluido el formato electrónico) y deberán ser actualizados cuando se realicen cambios o se añadan tratamientos no registrados en la organización.

Los usuarios no podrán llevar a cabo actividades de tratamiento de datos personales diferentes de las indicadas. Si un usuario considerase necesario iniciar una actividad de tratamiento de datos personales distinta, o modificar alguna de las existentes, lo notificará con carácter previo al Delegado de Protección de Datos (quien lo trasladará al Comité de Protección de Datos) y no iniciará la nueva actividad de tratamiento hasta que reciba confirmación de que puede hacerlo.

El registro de actividades de tratamiento actualizado es conocido por todos los usuarios de **UNRWA España**.

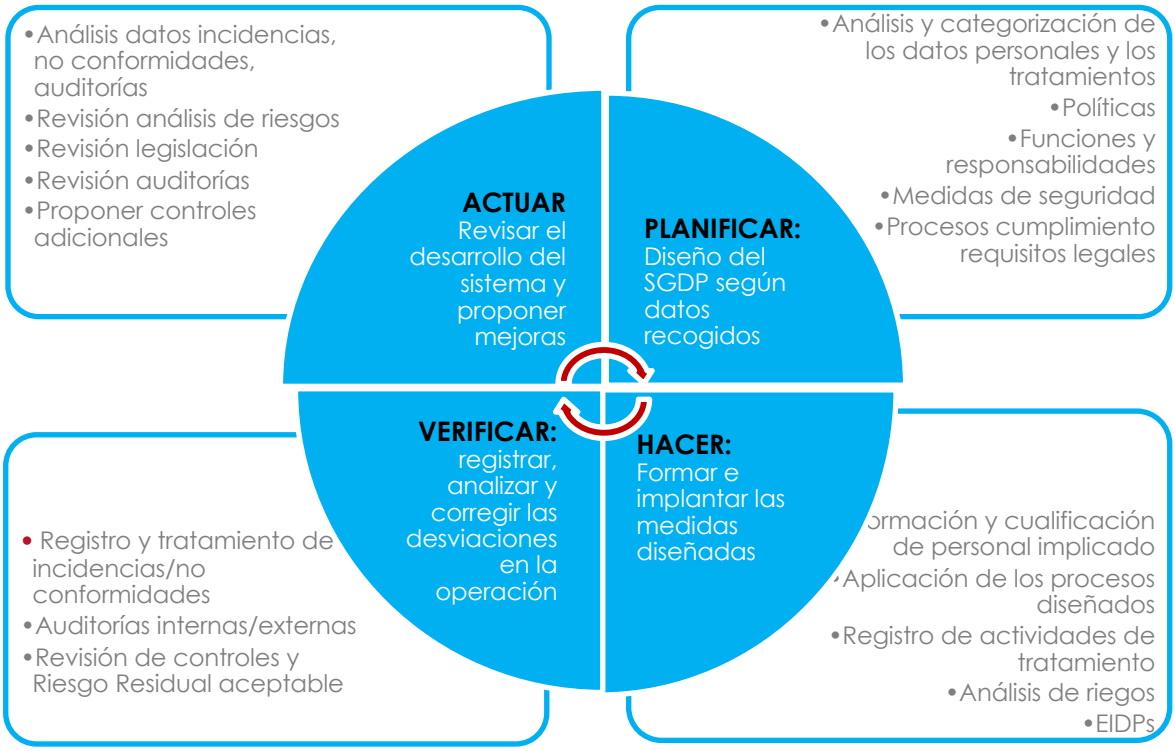
3. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES

3.1. Visión global: Ciclo de mejora de la seguridad de los datos personales

UNRWA España ha definido un Sistema de Gestión de Protección de Datos Personales para garantizar el cumplimiento de la legislación, asegurándose que las medidas y los procesos son los más adecuados en cada momento. Este ciclo de mejora incorpora además medidas que proporcionen información sobre el estado de las medidas de seguridad y de su cumplimento. De esta forma se podrán incorporar las mejoras necesarias y tener evidencia de la aplicación de las normas establecidas.

El sistema de gestión se fundamenta en los esquemas ISO de ciclo de mejora para sistemas de gestión, por lo que básicamente desarrolla las siguientes 4 fases: Planificar, Hacer, Verificar y Actuar. (en inglés se conoce como PDCA: Plan, Do, Check, Act.)

- Planificar (Plan): implica identificar un objetivo o meta, y ponerlo en acción.
- Hacer (Do): en el que se pone en marcha la implementación de lo planeado,
- Verificar (Check): que es en el que se monitorean los resultados para probar la efectividad del plan, los problemas y acciones de mejora.
- Actuar (Act): el cual integra el aprendizaje obtenido en dicho ciclo, lo que nos permite realizar los ajustes necesarios como parte de la mejora continua



De acuerdo con este enfoque, tras el trabajo inicial realizado en la adecuación al RGPD, se añade un posterior proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas implementadas. Se establece así la obligación de adoptar **un proceso de mejora continua** en relación con las medidas de seguridad implantadas para garantizar un tratamiento seguro de los datos personales.

3.2. Responsables y funciones en los procesos de protección de datos en UNRWA ESPAÑA

En **UNRWA España** se ha diseñado una estructura funcional para atender a las tareas y responsabilidades derivadas del Sistema de Gestión de Protección de Datos y del cumplimiento de la legislación en materia de protección de datos. Se dispone de un documento de funciones en el que se identifican las figuras con responsabilidad y sus funciones en materia de protección de datos.

La relación actualizada y completa de las personas de **UNRWA España** que ocupan cargos de responsabilidad en materia de protección de datos personales se ha dado a conocer a todos los usuarios. No obstante, a continuación, se identifican las 2 figuras fundamentales en la estructura de **UNRWA España**, señalando sus principales funciones:

➲ Delegado de Protección de Datos Local (DPO): personalizado en la figura de Internal Management Director (Dirección Gestión Interna), siendo la persona encargada de aplicar la legislación sobre privacidad y protección de datos en **UNRWA España**.

La figura del DPO es asumida en la actualidad por Dª. Cristina Villegas (dpo@unrwa.es)

Las funciones del DPO con carácter de mínimos son las siguientes:

- ✓ Informar y asesorar a la Asociación y a los empleados asignados a los tratamientos, de las obligaciones que les incumben en virtud del RGPD (incluida la implantación de programas de formación y sensibilización del personal).
- ✓ Supervisar el cumplimiento del RGPD y otras disposiciones en materia de protección de datos, además de las políticas de **UNRWA España** al respecto (incluida la asignación de responsabilidades, concienciación, formación y auditorías correspondientes).

  Dicha obligación de supervisión incluye recabar información para determinar, comprobar y analizar actividades del tratamiento para su conformidad con la normativa, su asesoramiento y emisión de recomendaciones en su caso.
- ✓ Supervisar las auditorías realizadas
- ✓ Ofrecer asesoramiento relativo a Evaluaciones de Impacto y su aplicación.
- ✓ Comunicar a la Junta Directiva la existencia de vulneración relevante en protección de datos y proponer medidas necesarias.
- ✓ Cooperar e intervenir ante la Autoridad de Control Nacional (Agencia Española de Protección de Datos o AEPD)
- ✓ Realizar consultas ante la Autoridad de Control (AEPD)
- ✓ Actuar como punto de contacto con un papel de "facilitador" ante la Autoridad de Control (AEPD) para cuestiones relativas al tratamiento de datos.
- ✓ Establecimiento y control del registro de actividades del tratamiento de la Asociación.
- ✓ Asesorar y supervisar, entre otras, en las siguientes áreas:
  - Cumplimiento de los principios generales básicos relativos al tratamiento (limitación de la finalidad, minimización o exactitud de datos, plazos de conservación, etc.)
  - Identificación de la correcta legitimidad del tratamiento (bases jurídicas donde se ampara)
  - Ponderación de los tratamientos amparados en interés legítimo para establecer su prevalencia sobre los derechos y libertades de los afectados.
  - Valoración de compatibilidad de finalidades distintas de las que originaron la recogida de los datos.
  - Determinar la existencia de normativa sectorial aplicable al tratamiento.
  - Diseño e implementación de medidas dirigidas al cumplimiento del deber de información al afectado del tratamiento.
  - Establecer mecanismo de recepción y de gestión de solicitudes de ejercicio de derechos por parte de los interesados.
  - Contratación de encargados del tratamiento (incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado)
  - Identificación de los instrumentos de transferencias internacionales de datos adecuados a las necesidades y características de la organización y las razones que justifiquen dichas transferencias, en caso de existir transferencias.
  - Diseño e implantación de políticas de protección de datos

- Evaluación de los análisis de riesgos realizados en los tratamientos
- Implantación de medidas de protección de datos desde el diseño y por defecto adecuadas a los tratamientos
- Implantación de medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimiento de gestión de violaciones de seguridad (incluida la evaluación del riesgo para los derechos y libertades de los afectados y las necesarias notificaciones a las Autoridades de Control y a los afectados, en su caso.

➲ Comité GDPR: es el órgano de dirección central de la política de protección de datos en **UNRWA España** que prestará el apoyo y asistencia necesaria al Delegado de Protección de Datos en el cumplimiento de sus funciones.

Las funciones del Comité GDPR consisten en la gobernanza y orientación de la política de protección de datos de **UNRWA España** y la prestación de asistencia en sus funciones al DPO.

Este Comité no asumirá las funciones y competencias propias de la figura del DPO.

En la actualidad, el Comité GDPR de **UNRWA España** se compone de los siguientes miembros:

- ✓ Dª. Raquel Martí Lezana (Directora Ejecutiva)
- ✓ Dª. Cristina Villegas (DPO)
- ✓ D. Daniel Sánchez Muñoz (Responsable IT)
- ✓ D. Carlos García (Asesor Externo)
- ✓ D. Xabier Tizón (Asesor Externo)

Atendiendo a los temas a tratar en el Comité (Orden del día) pueden incorporarse al Comité diferentes responsables de Áreas o Dptos de **UNRWA España**, pudiendo ser los siguientes:

- Dª. Cristina Poveda (Directora de comunicación, fundraising y campañas)
- Dª. Laura Pérez (Técnica de gestión de personas)
- Dª. Paz Pérez (Directora de administración y finanzas)
- Dª. Isabel Miguel (Directora de Educación para luna ciudadanía global)
- Dª. Laura Pérez (técnica de gestión de personas)

3.3. Gestión de riesgos sobre datos personales

La gestión de riesgos permite el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realiza mediante el despliegue de medidas de seguridad, que establecen un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad implementadas

3.3.1. Análisis de riesgos

El enfoque basado en el riesgo es uno de los pilares del RGPD y requiere haber identificado previamente los tratamientos y los activos implicados por la organización, por lo que partimos de la información reflejada en el registro de actividades de tratamiento identificados.

Todas las actividades de tratamiento de **UNRWA España** pueden exponerse a diferentes situaciones que deriven en un compromiso de su confidencialidad, integridad y disponibilidad, siendo sometidas a un análisis para determinar los riesgos que presentan (**Análisis de Riesgo** o **AR**) y, en el caso de suponer un alto riesgo, realizar una evaluación de impacto (**Evaluación de Impacto en la Protección de Datos** o **EIPD**).

La metodología utilizada en el análisis y las evaluaciones de los riesgos en cada tratamiento de datos personales se basa en las siguientes premisas básicas:

- Todo tratamiento de datos implica "per se" riesgos para las libertades y derechos de los interesados.
- Es imposible reducir los riesgos a cero.
- A pesar de lo anterior, debe tenderse siempre a conseguir el riesgo cero.
- Las fases en las que se estructura la presente metodología son:
  - ✓ Identificación de los tratamientos de datos que realiza la entidad.
  - ✓ Identificación de los activos implicados en dichos tratamientos.
  - ✓ Identificación de los riesgos o amenazas.
  - ✓ Evaluación del riesgo inicial (RI).
  - ✓ Identificación y valoración de las medidas de seguridad implementadas.
  - ✓ Medición del riesgo residual (RR).

El proceso para realizar un análisis de riesgos consta de los siguientes pasos:

1. Identificar los activos de información de la organización, cada uno de los cuales estará expuesto a unas amenazas determinadas y tendrá unas vulnerabilidades asociadas.
2. Del paso anterior, que nos describe el estado del activo, obtenemos el Riesgo Inicial (RI). Es decir, el riesgo al que está expuesto el activo «por defecto» antes de la aplicación de los controles específicos.
3. En el paso siguiente, determinamos la probabilidad de materialización del Riesgo Inicial (RI), que dará como resultado un impacto, es decir, las consecuencias que tiene la materialización de la amenaza.
4. A continuación, identificamos aquellos riesgos que, por su probabilidad, impacto o ambos, no son aceptables. Esta decisión es tomada de acuerdo a la estrategia corporativa y en función de los riesgos dispuestos a asumir.
5. Como resultado de la aplicación de los controles, se obtiene el Riesgo Residual (RR) del activo, que indica el grado de exposición del activo a las amenazas después de haber implantado los controles seleccionados así como las consecuencias de la materialización de la amenaza.

Tras la identificación de los riesgos se establece y documenta el nivel de riesgo aceptable: el valor umbral que determina los riesgos que deben ser tratados y los riesgos que son asumibles.

En resumen, el análisis de riesgos está enfocado principalmente a identificar aquellos riesgos que exceden unos límites aceptables para la organización.

Las fórmulas utilizadas para el cálculo de la probabilidad y la severidad finales, y por tanto del riesgo residual (RR), son las mismas que para el cálculo del riesgo inicial (RI), pero con los nuevos valores obtenidos una vez reducidos los primeros valores en el porcentaje que corresponda a cada uno en función de las medidas de seguridad implementadas.

En todo caso, se establece con carácter general que:

- ✓ No es política de **UNRWA España** asumir conscientemente riesgos que pudieran erosionar la reputación de la Asociación como consecuencia del incumplimiento de normas y contratos.
- ✓ Tampoco lo es desarrollar actividades que por su naturaleza o características pudieran entrañar un alto riesgo para los derechos y libertades de los individuos.
- ✓ **UNRWA España** no lleva a cabo ningún tratamiento de datos personales cuyo riesgo no hubiera podido ser reducido hasta niveles aceptables conforme a lo anteriormente expuesto.
- ✓ **UNRWA España** no delega tratamientos de datos personales a terceros localizados fuera de la Unión Europea o que no hubieran adoptado las medidas necesarias para asegurar el cumplimiento de lo previsto en esta Política.

  La entidad lleva a cabo la posterior revisión continua o periódica de los riesgos derivados de los tratamientos de datos y de las medidas de seguridad implementadas en relación con cada uno de ellos, conforme exige el artículo 32 RGPD.

3.3.2. Evaluación de impacto sobre protección de datos

Una Evaluación de Impacto sobre protección de datos (en adelante **EIPD**) no se requiere siempre en cada actividad de tratamiento. La EIPD solo se realizar cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.

El Comité GDPR se mantendrá informado de las recomendaciones publicadas al respecto por la Agencia Española de Protección de datos (la AEPD ya ha publicado listas de los tipos de operaciones de tratamiento que requieran y que no requieren realizar una evaluación de impacto relativa a la protección de datos, según el art. 35.4 y 35.5 del RGPD) procediendo al estudio de cómo puede ser afectado el análisis de riesgo y EIPD en **UNRWA España**.

En la actualidad no existe ningún tratamiento de datos personales que requiera una EIPD.

3.3.3. Protección desde el diseño y por defecto

Se establece el principio de protección de datos desde el diseño (definiendo desde el inicio las medidas de seguridad técnicas y organizativas que deberán aplicarse para garantizar los derechos y libertades de las personas físicas en el tratamiento de los datos) y por defecto (sólo serán objeto de tratamiento los datos necesarios para cada uno de los fines específicos del tratamiento, garantizando por defecto su plazo de conservación y su accesibilidad).

Cuando se vaya a establecer un nuevo tratamiento de datos personales, una vez realizado el análisis de riesgos previo, se considerarán medidas preventivas de protección de datos que se incorporen desde el propio diseño de los sistemas y procesos de trabajo.

Este análisis se realiza por el responsable IT con el apoyo de expertos en materia y los responsables de los departamentos implicados, bajo la supervisión del Comité GDPR y del DPO.

En general, esta visión de protección desde el diseño y por defecto, se integra dentro de las medidas de control de los riesgos establecidas en el proceso de gestión de riesgos descrito anteriormente.

4. MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

UNRWA España ha adoptado medidas técnicas y organizativas apropiadas contra el uso indebido, no autorizado, procesamiento ilegal, pérdida accidental, destrucción o daño de los datos personales. En la toma de dichas medidas, se consideran las limitaciones establecidas para tales medidas por el desarrollo tecnológico y los costes de implementación, los riesgos y la naturaleza de los datos personales que deben protegerse.

Cada empleado es responsable de garantizar el cumplimiento de las reglas de seguridad de datos al procesar datos personales, con independencia de si los datos se encuentran en formato electrónico o en soporte papel.

4.1. Gestión de brechas de seguridad de los datos personales

Se entiende por "brechas de seguridad" a los incidentes que pueden afectar o afectan a la seguridad de información y los datos personales.

Se entiende por incidencia a cualquier evento que pueda suponer un riesgo para la seguridad de los datos de carácter personal, entendida bajo sus vertientes de autenticación, confidencialidad, integridad y disponibilidad de los datos.

Incluimos dentro de la gestión de brechas de seguridad las denominadas por el RGDP violaciones de seguridad de los datos personales, cuya definición responde a: "*Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*"

La gestión de incidentes de seguridad y la gestión de brechas de seguridad se encuentran reguladas internamente.

5. PROCESOS DE CUMPLIMIENTO NORMATIVO

En el proceso de gestión de riesgos es importante asegurar una correcta identificación de las amenazas a los que está expuesta una actividad de tratamiento teniendo en cuenta que entre los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas se pueden diferenciar dos dimensiones:

- Los riesgos asociados a la protección de la información con el foco central en la integridad, disponibilidad y confidencialidad de los datos
- Los riesgos asociados al cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

A modo expositivo y sin ánimo de ser exhaustivos se establecen las siguientes medidas de cumplimiento normativo:

- ✓ Existencia de compromisos de confidencialidad y deber de secreto para todo el personal de **UNRWA España** y personal de servicios subcontratados que tengan acceso a datos personales de la Asociación. Este acceso puede ser por requisitos del propio servicio prestado, pero también puede ser de forma accidental (documentación sin archivar, documentos en las impresoras, etc.). También en estos casos se garantiza la confidencialidad respecto a la información a la que se ha tenido acceso.
- ✓ En cada tratamiento de datos personales titularidad de **UNRWA España** se sopesa las finalidades concretas a las que se destinan los datos, la licitud o legitimidad (base jurídica) de cada tratamiento, y en su caso, la necesaria obtención del consentimiento ("inequívoco" mediante una manifestación del interesado o

mediante una clara acción afirmativa), tratamiento de categorías especiales de datos[2], identificación de los concretos cesionarios de la información, plazos de conservación de los datos, posibilidad de ejercitar los derechos del titular (acceso, rectificación, y el resto de requerimientos que establece el RGPD para el derecho de información en sus artículos 13 y 14.[3]

- ✓ En cada tratamiento de datos se cumple con el principio general de limitación del plazo de conservación de los datos (art. 5.1.e RGPD).
- ✓ La existencia de un correcto y eficaz procedimiento para la atención al ejercicio de los derechos de los afectados. Estos derechos son: derecho de acceso (artículo 15 RGPD), derecho de rectificación (artículo 16 RGPD), derecho de supresión (artículo 17 RGPD), derecho de limitación del tratamiento (artículo 18 RGPD), derecho de oposición (artículo 21 RGPD), el derecho de portabilidad (artículo 20 RGPD) y derecho de elaboración de perfiles (artículo 22 RGPD) y todos ellos se centralizan en un canal de entrada común: rgpd@unrwa.es.
- ✓ Correcta regulación de las relaciones con encargados del tratamiento contratados por **UNRWA España** donde se accede a datos personales con adecuación de los contratos suscritos a los requerimientos del artículo 28 RGPD.
- ✓ Transferencias internacionales de datos: en aquellos casos en los que, de acuerdo a la información recogida en el Registro de Actividades de Tratamiento, pueda existir transferencia internacional de datos (a países fuera de la UE), **UNRWA España** velará porque la transferencia se realice con un nivel de seguridad adecuado y que los datos de los interesados son tratados con el mismo nivel de protección que el que hubiera correspondido en caso de haber permanecido en la jurisdicción de la Unión Europea.

[2] En **UNRWA España**, sólo se tratan datos de categorías especiales cuando sea necesario para el cumplimiento de las obligaciones y el ejercicio de los derechos específicos de la organización o del interesado en el ámbito del derecho laboral.
[3] Todos estos aspectos legales se recogen de forma expresa en el Registro de Actividades de Tratamiento de la Asociación.