**Si tiene alguna pregunta, póngase en contacto con la persona responsable de la protección de datos, escribiendo a dpo@tearfund.org.**

| **Título:** | **POLÍTICA DE PROTECCIÓN DE DATOS** |
|---|---|
| **Declaración de la política:** | Tearfund se compromete a cumplir con el Reglamento General de Protección de Datos (RGPD) del Reino Unido, la Ley de Protección de Datos de 2018 del Reino Unido y todas las demás reglamentaciones pertinentes en materia de datos personales y protección de los derechos y libertades de las personas cuya información es objeto de recolección y tratamiento por parte de Tearfund.<br><br>La presente política y las políticas y procedimientos enumerados a continuación describen los procedimientos de Tearfund destinados a velar por el cumplimiento del RGPD del Reino Unido y la Ley de Protección de Datos del Reino Unido. |
| **Procedimientos y otras políticas relacionadas con esta política** | • Data Retention Policy (Política de retención de datos)<br>• Política de seguridad de la información<br>• Guidelines for Handling Personal Data (Directrices para el manejo de datos personales)<br>• Notificación de privacidad para el personal<br>• Política de conducta personal<br>• Política de denuncia de irregularidades<br>• Política sobre la recopilación, el almacenamiento y el uso de contenidos<br>• Procedimiento y política de conducta indebida<br>• Affinis User Guides (Guía de usuario de Affinis)<br>• Use of social media in high risk situations (Uso de los medios sociales en situaciones de alto riesgo) aquí<br>• Key points to consider when sharing data with the Tearfund family (Puntos clave por considerar cuando se comparten datos con la familia Tearfund)<br><br>Todos los documentos citados están disponibles en la unidad compartida de políticas de Tearfund, en la plataforma organizacional de Tearfund, como apéndice de esta política, en la plataforma de Affinis aquí, o bien en la plataforma de marca global y fotografía.<br><br>• Términos de referencia para el Grupo de Protección de Datos<br>• Reporte de incidentes de violación de datos<br>• Procedimiento para solicitar acceso a datos personales<br>• Registro de actividades de tratamiento de datos<br><br>Los documentos citados pueden solicitarse a la persona responsable de la protección de datos, escribiendo a dpo@tearfund.org.<br><br>• Registros de almacenamiento de datos<br><br>Cada equipo dispone de su propio registro de almacenamiento de datos, de cuyo mantenimiento es responsable. |
| **Por qué es necesaria la política** | No garantizar que el tratamiento de los datos personales cumple la legislación, da lugar a se puedan adoptar medidas coercitivas, enjuiciamientos, acciones judiciales y a que las personas que se sientan afectadas eleven reclamos de indemnización. Asimismo, supone problemas de riesgo potencialmente graves para la reputación de la organización. |

| | |
|---|---|
| **Quiénes deben observar esta política** | Todas las personas que forman parte de Tearfund, independientemente de su ubicación o puesto. Todos los empleados de la familia Tearfund, afiliados, voluntarios, consultores o representantes de Tearfund que deben acceder a los servidores y las plataformas de Tearfund para desempeñar sus funciones. |
| **Persona responsable** | Director/a de Finanzas, quien reporta a la Junta Directiva |
| **Versión** | Final |
| **Aprobada por:** | LA JUNTA DIRECTIVA |
| **Fecha de aprobación:** | Julio de 2023 |
| **Próxima revisión formal:** | Julio de 2025 |

## Introducción

La protección de datos tiene por objeto salvaguardar el derecho fundamental a la privacidad, consagrado en leyes y reglamentos. Todo particular debe contar con los medios para ejercer su derecho a la privacidad y protegerse a sí mismo y a sus datos contra cualquier abuso. Tearfund trabaja con un gran número de personas en todo el mundo y necesita recopilar datos personales para poder llevar a cabo sus actividades. Todos los integrantes de Tearfund, sean cuales fueren sus funciones, manejarán en algún momento datos personales, por lo cual es esencial conocer los principios básicos de la protección de datos y nuestras responsabilidades sobre esta cuestión.

### Capacitación y recursos sobre protección de datos

Tearfund ha asumido el compromiso de garantizar que todo el personal conozca sus obligaciones y responsabilidades en lo relativo al manejo de datos personales. El curso de capacitación en protección de datos es obligatorio para **todo** el personal de Tearfund, independientemente del lugar en que se encuentre. Para cualquier consulta relativa a la protección de datos, escriba en primera instancia a: dpo@tearfund.org.

Tearfund cuenta con una persona responsable de la protección de datos y grupos de protección de datos, integrados por representantes de toda la organización, que se reúnen periódicamente para evaluar nuestro cumplimiento de la normativa de protección de datos.

### ¿QUÉ COSAS SE CONSIDERAN DATOS PERSONALES?

La política de protección de los datos solo es aplicable cuando se realiza el tratamiento de datos personales.

- Los datos personales solo incluyen la información relacionada con las personas físicas que cumplen con las siguientes condiciones:
    - pueden ser identificadas o son directamente identificables basándose en la información en cuestión,
    - pueden ser identificadas indirectamente basándose en dicha información en combinación con otra información.
- Los datos personales también pueden incluir categorías especiales de datos personales o información sobre condenas y delitos penales. Estos datos especiales se consideran más sensibles y solo podemos tratarlos en circunstancias más limitadas.

**¿QUÉ SE ENTIENDE POR TRATAMIENTO?**

- El RGPD del Reino Unido se aplica al tratamiento de datos personales que satisface las siguientes condiciones:
    - se realiza total o parcialmente por medios automatizados, o
    - se realiza por medios que no son automatizados en el que los datos personales tratados forman parte, o se espera que formen parte, de un sistema de archivo.
- El término «tratamiento» tiene un significado muy amplio: incluye las acciones de recopilar, poseer, almacenar y compartir.

**¿QUÉ SON LAS CATEGORÍAS ESPECIALES DE DATOS?**

Las categorías especiales de datos personales (también llamados datos personales sensibles) son aquellos datos personales que dan a conocer o se relacionan con la siguiente información de una persona física:

- Origen racial o étnico
- Opiniones políticas o afiliación sindical
- Creencias religiosas o filosóficas
- Datos genéticos o biométricos
- Estado de salud física o mental
- Orientación/vida sexual

Para el tratamiento de las categorías especiales de datos personales, normalmente necesitaremos basarnos en alguno de los siguientes fundamentos:

1. Consentimiento explícito de la persona interesada.
2. El tratamiento es necesario para cumplir nuestras obligaciones y ejercer nuestros derechos en los ámbitos del derecho laboral y la seguridad social.
3. El tratamiento es necesario por motivos de ciertos fines limitados de salud relacionados con el trabajo.
4. Tratamiento de las excepciones aplicables a ONG basadas en la fe que se llevan a cabo en el ámbito de nuestras actividades legítimas y con las debidas garantías.
5. La información pertinente ya se encuentra en el dominio público.

Con menos frecuencia, podremos alegar la necesidad del tratamiento cuando:

1. El tratamiento es necesario en relación con un procedimiento judicial.
2. El tratamiento es necesario para proteger los intereses vitales de la persona.

Si necesita tratar datos de la categoría especial y no está seguro/a de si puede basarse en uno de estos fundamentos, solicite asesoramiento del equipo jurídico de Tearfund.

- Los datos seudonimizados pueden contribuir a la reducción de los riesgos de privacidad al hacer que sea más difícil identificar a las personas, pero siguen siendo catalogados como datos personales.
- Si los datos personales pueden ser realmente anonimizados, dichos datos anonimizados no se encuentran sujetos al RGPD del Reino Unido. Es importante comprender qué cosas se consideran datos personales para entender si los datos han sido anonimizados.
- La información que se refiere a una persona fallecida no constituye datos personales y, por lo tanto, no se encuentra sujeta al RGPD del Reino Unido.
- La información sobre empresas o autoridades públicas no se considera datos personales.
- Sin embargo, la información sobre personas físicas que actúan como comerciantes individuales, empleados, socios y directores de empresas que permite identificarlos en lo personal y cuya información se refiere a ellos como personas físicas puede constituir datos

personales.

## PRINCIPIOS DE PROTECCIÓN DE DATOS

**¿Qué son? ¿Por qué el personal debe cumplirlos?**
Tearfund ha asumido el compromiso de acatar los principios del Artículo 5 del RGPD del Reino Unido y establece siete principios claves que deben aplicarse siempre que se realice el tratamiento de datos personales. Tearfund llevará un registro constante de sus actividades de tratamiento de datos personales y de la base en la que dicho tratamiento se fundamenta en relación con cada una de esas actividades.

**Principio 1: Los datos personales serán tratados de manera lícita, leal y transparente**

***Lícita y leal:*** Nuestro tratamiento de los datos personales estará fundamentado en una base legal que una persona pueda entender. Todo tratamiento de los datos personales se realizará sobre uno de los siguientes fundamentos jurídicos:

- Consentimiento
  - ***El consentimiento*** *debe ser:*
    - ★ *otorgado mediante un acto* ***afirmativo*** *y* ***claro****, que refleje una manifestación de voluntad* ***libre, específica, informada*** *e* ***inequívoca*** *de la persona interesada de aceptar el tratamiento de sus datos personales para uno o más* ***fines específicos****.*
    - ★ *Necesitamos tener pruebas del consentimiento obtenido sobre las cuales podamos fundamentarlo.*
- Necesidad contractual
- Cumplimiento de obligaciones legales (por ejemplo, dar a conocer detalles a HMRC, el organismo de impuestos y de aduanas del Reino Unido)
- Legítimo interés comercial (por ejemplo, facultad legítima para investigar)

*Si se pretende alegar un interés comercial legítimo como base legal para el tratamiento de datos personales, primero debe realizarse una evaluación de legítimo interés comercial. Esto se debe a que las necesidades en materia de intereses comerciales legítimos de Tearfund deben contrapesarse con los intereses o derechos y libertades fundamentales de la persona cuyos datos se recopilan. Encontrará un enlace a esta plantilla en el Apéndice 1.*

Con menos frecuencia, podremos fundamentarnos en lo siguiente:

- Interés público (impedir o detectar actos ilícitos)
- Intereses vitales

***Transparente:*** En el momento de **recopilar** sus datos personales, debemos comunicar a los interesados con un lenguaje claro y comprensible **cómo** utilizaremos sus datos. Esta comunicación podría realizarse a través de los siguientes medios:

- Políticas de privacidad en nuestro sitio web *www.tearfund.org*.
- La notificación de privacidad para el personal, cuyo enlace puede encontrarse en el Apéndice 1.
- Redacción explícita en formularios de consentimiento impresos o formularios web en línea (por ejemplo, plantillas de permisos de los participantes, formularios de inscripción en eventos, formularios en línea, etc.)
- Explicaciones verbales, que deben grabarse
- Texto contractual

***Evaluación de Impacto de la Protección de Datos:*** *debe realizarse una evaluación del impacto relativa a la privacidad de los datos antes de llevar a cabo tipos de tratamiento que puedan suponer un alto riesgo para los derechos y libertades de las personas. Esto incluye el uso a gran escala de datos personales sensibles, datos concernientes a personas vulnerables o el tratamiento en el que se utilice un nuevo tipo de tecnología. En el Apéndice 1, encontrará una plantilla de Evaluación del Impacto de la Protección de Datos, la cual debe ser autorizada por el equipo jurídico y la persona Responsable de la Protección de Datos de Tearfund. Una vez autorizada, los resultados deben*

*integrarse en el plan para el tratamiento de los datos. La plantilla de evaluación se someterá a una revisión continua y se la volverá a considerar cuando sea necesario.*

**Principio 2: Restricciones en cuanto a los fines**

**Los datos personales solamente se recopilarán para fines determinados, explícitos y legítimos y se prohíbe que sean tratados posteriormente de una manera incompatible con esos fines**

Tearfund no debe obtener datos personales para un fin y luego utilizarlos para otro fin. Debemos ser claros en cuanto al uso haremos de los datos personales.

*En mayor detalle…*

*Tearfund ha identificado los siguientes «fines» para los cuales recopilamos datos:*

- *Administración:*
  - *Fines comerciales*
  - *Empleados (incluyendo postulantes, voluntarios, consultores y profesionales independientes)*
  - *Personas que nos apoyan*
- *Verificación de datos*
- *Márquetin directo:*
  - *Solicitudes de ayuda financiera y actualizaciones de noticias*
  - *Campañas*
  - *Eventos de recaudación de fondos*
  - *Donaciones planeadas, diferidas o legadas (herencias)*
  - *Eventos de trabajo voluntario*
- *Investigación de mercado*
- *Elaboración de perfiles*
- *Prospección*
- *Prestación de servicios*

*Si se recopilan datos personales para un fin que no considere que pueda incluirse en alguna de las categorías precedentes, escriba a dpo@tearfund.org.*

*Ejemplo:*

*Una persona se postula a un empleo en el sitio web de Tearfund y proporciona datos personales con el objeto de que sean utilizados solo para ese fin (la categoría sería Administración: Empleados). La dirección de correo electrónico que ha facilitado no podrá utilizarse para enviar correos electrónicos de márquetin, salvo que haya dado su consentimiento expreso para ese fin.*

**Principio 3: Minimización de datos**

**Necesitamos poder demostrar que solo sean objeto de tratamiento los datos personales adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados**

Se trata de un ejercicio de equilibrio entre recopilar la información suficiente para el fin previsto, pero también de asegurarnos que no obtengamos datos «por si acaso» llegasen a ser útiles. Este principio es pertinente cuando diseñamos herramientas tales como formularios web o encuestas. Debemos considerar qué datos recopilamos y por qué los necesitamos. También tenemos que ser cuidadosos al recopilar opiniones o información excesiva acerca de las personas. Tenemos que recordar que la persona interesada puede solicitar ver aquellos datos suyos que obran en nuestro poder y que, por consiguiente, tenemos que poder explicarle por qué tenemos esa información.

*Ejemplo:*

*A efectos de monitoreo y evaluación, es posible que Tearfund recopile comentarios de un conjunto de participantes de los proyectos para medir el impacto de esos proyectos. La encuesta solicita información sobre el núcleo familiar, lo cual corresponde a datos personales. No obstante, no es necesario que las personas que responden a la encuesta proporcionen información personal adicional, como su dirección, por lo que no debería solicitarse dicha información adicional. Esto garantizará que la información se recopile solamente para satisfacer las necesidades de medición del impacto. Sin embargo, si Tearfund quisiese incluir un estudio de caso no anónimo como parte del informe de impacto, necesitaríamos el consentimiento explícito de esa persona participante.*

**Principio 4: Exactitud**

**Los datos personales deben ser exactos y, si es necesario, se deben mantener actualizados. Debemos adoptar todas las medidas razonables para garantizar que los datos personales incorrectos, en consideración de los fines para los que se realiza su tratamiento, sean eliminados o rectificados sin demora**

En la medida de lo posible, el personal recurrirá a fuentes de información centralizadas para registrar y recopilar datos (Affinis, SelectHR, IBIS, etc.), ya que estas proveen mayores garantías de actualización y exactitud. El personal no debe crear copias innecesarias. La ubicación en la que se guarden los datos personales se deberá incluir en el registro de almacenamiento de datos del equipo.

El personal realizará las modificaciones necesarias en los datos en cuanto tenga conocimiento de cualquier cambio o se detecte cualquier error. La información obsoleta debe destruirse.

**Principio 5: Limitación del plazo de conservación**

**Los datos personales no deben almacenarse durante un plazo mayor de lo necesario para los fines para los que se realiza su tratamiento.**

Tenemos que asegurarnos de poder justificar por qué es necesario continuar el tratamiento (término que incluye el almacenamiento) de datos personales, sea electrónicamente o en copia impresa.

Es necesario garantizar que los datos se almacenen de conformidad con los plazos estipulados en la política de retención de datos (Data Retention Policy), y que estamos familiarizados con las directrices relativas al manejo de datos personales. El Apéndice 1 contiene los enlaces a ambos documentos.

*En mayor detalle, usted…*

- *Debe asegurarse de asignar a los documentos de Google que contienen datos personales un nombre que permita entender fácilmente (i) de qué trata el documento; y (ii) cuándo debe ser borrado; y (iii) que dichos documentos tengan acceso restringido para que no haya varias copias de datos personales en Google Drive.*
- *Debe borrar los datos personales de los buzones de mensajes recibidos y enviados del correo electrónico en cuanto ya no se requieran.*
- *Debe asegurarse de que el Registro de Almacenamiento de Datos del equipo sea revisado y actualizado trimestralmente. Puede considerar agregar este tema para ser discutido durante las reuniones periódicas del equipo.*
- *Debe asegurarse de saber cómo borrar y archivar datos.*
- *Debe asegurarse de borrar periódicamente el contenido de la carpeta de descargas.*
- *Debe anonimizar los datos personales si desea conservarlos para fines estadísticos o de investigación*.

**Principio 6: Integridad y confidencialidad (seguridad)**

**Se adoptarán medidas técnicas y organizacionales adecuadas contra el tratamiento no**

**autorizado o ilícito de datos personales, así como para evitar la pérdida accidental, destrucción o daño de los datos personales**

Estas son potencialmente las principales causas de riesgo para Tearfund, mientras que el pirateo informático y la usurpación de identidad (*phishing*) constituyen un importante peligro para todas las organizaciones internacionales. Todos los empleados de Tearfund son responsables de asegurarse de que los datos a los que acceden se mantengan seguros y protegidos en todo momento, de velar por el cumplimiento de la Política de seguridad de la información, y de haber leído y entendido las Directrices de seguridad digital.

*En mayor detalle…*

*Tearfund ha implementado medidas técnicas y organizacionales. Entre algunos ejemplos de ellas merecen mencionarse las siguientes:*

***Organizacionales***

1. *Capacitación del personal en protección de datos*
2. *Políticas en materia de protección de datos y seguridad de la información*
3. *Directrices de seguridad digital*
4. *Capacitación y orientación sobre el uso de documentos Google*
5. *Provisión de armarios con candado*

***Técnicas***

1. *Copias de seguridad del sistema*
2. *Cifrado*
3. *Permisos de acceso a la base de datos*
4. *Google Drive*
5. *Software de terceros*

*Cada uno de nosotros tiene un papel que desempeñar, desde asegurarnos de cerrar con llave los armarios y bloquear las computadoras hasta no enviar mensajes de correo electrónico a direcciones incorrectas, o permitir el acceso a datos personales a usuarios que no tienen necesidad de verlos. Todo el personal debe familiarizarse con la Política de seguridad de la información, que se distribuye anualmente y que puede consultarse en todo momento en la plataforma corporativa de Tearfund.*

**Principio 7: Rendición de cuentas**

**El principio de rendición de cuentas exige que Tearfund se responsabilice por los datos personales que maneja y que se dé cumplimiento a los otros seis principios.** Asimismo se exige que existan medidas y registros adecuados a fin de demonstrar el cumplimiento. Tearfund proporciona capacitación obligatoria sobre protección de datos como parte del proceso de inducción y en el repaso frecuente virtual obligatorio para todo el personal. El Grupo Central de Protección de Datos se reúne a intervalos frecuentes para rever las respuestas a cualquier violación de la seguridad de los datos experimentada y el cumplimiento por parte de la organización de las políticas y procedimientos, mientras que el grupo más amplio de Protección de Datos, que tiene representantes de todos los equipos de Tearfund, proporciona una oportunidad adicional para difundir recordatorios sobre las buenas prácticas.

Tearfund ha nombrado a un/a Responsable de la Protección de Datos, quien actúa como punto de contacto con el comisionado para asuntos de información del Reino Unido (Information Commissioner’s Office, ICO) y los interesados.

## Otras cuestiones importantes

### Los derechos de las personas en materia de privacidad y protección de datos

Tearfund respetará los derechos de las personas reconocidos por las leyes de protección de datos, entre los que se incluyen los siguientes:

- Derecho a acceder a sus datos
- Derecho a restringir el uso de sus datos
- Derecho a rectificar la información incorrecta contenida en sus datos
- Derecho a que se eliminen sus datos
- Derecho a restringir el contacto no solicitado
- Derecho a que se les notifique de las violaciones de la seguridad de los datos personales
- Derecho a que se les informen los criterios para cualquier toma de decisiones automatizada sobre ellas
- Derecho a presentar una queja.

Si desea obtener más detalles, escriba al correo electrónico dpo@tearfund.org

### Violación de la seguridad de los datos personales

En las grandes organizaciones que trabajan a nivel internacional, habrá ocasiones en las que, quizás accidentalmente, los datos personales se borren, pierdan, modifiquen sin permiso o divulguen, o que personas no autorizadas accedan a ellos para ver o acceder a esta información. Esto se denomina violación de la seguridad de los datos personales. Esta definición abarca una enorme variedad de incidentes, como por ejemplo:

- ★ envío accidental de los datos de una de las personas que nos apoyan a una dirección de correo electrónico errónea;
- ★ extravío de plantillas de permisos de los participantes durante un viaje;
- ★ robo de una computadora portátil que contiene datos personales;
- ★ notificación de un proveedor comunicándonos que se ha producido un acceso ilícito a sus sistemas;
- ★ pirateo informático de los sistemas o de la red de Tearfund;
- ★ otorgamiento incorrecto a miembros del personal de permisos de acceso a documentos o bases de datos que contienen datos personales sensibles.

Tearfund cuenta con un plan de respuesta a incidentes de violación de la seguridad de los datos personales para responder a este tipo de situaciones (y a otras situaciones de violación de la seguridad). El mensaje más importante para todos los miembros del personal es que **deben informar de inmediato** cualquier violación de la seguridad de los datos de la que esté al tanto, enviando un correo electrónico a databreach@tearfund.org (*Nota: si la violación se relaciona con la pérdida o el robo de equipos informáticos, asuntos de seguridad o cualquier otro tipo de incidente, en lugar de dicho correo, deberá enviar un informe de dicho incidente por correo electrónico a incident.reporting@tearfund.org, quienes notificarán la violación de la seguridad de los datos a databreach@tearfund.org*). Esto se debe a que la obligación de comunicarlas a la ICO estipula la necesidad de hacerlo sin demoras indebidas y, en la medida de lo posible, dentro de las 72 horas siguientes al momento de tener conocimiento de la violación. Por consiguiente, el plazo es muy corto. Para obtener información más detallada, consulte el proceso adjunto sobre cómo comunicar una violación de la seguridad de los datos.

### Privacidad por diseño y de forma predeterminada

Antes de adoptar nuevos tratamientos de datos o actividades que pudieren generar grandes riesgos a la privacidad y seguridad de los datos personales, Tearfund realizará y documentará una Evaluación de Impacto de la Protección de Datos.

Tearfund empleará procesos tales como la seudonimización (con miras a reducir los riesgos de

privacidad que pudieren correr los interesados) o la anonimización para reducir al mínimo la recopilación, la utilización, el almacenamiento o cualquier otra forma de tratamiento de los datos personales.

**Ámbito de aplicación del RGPD del Reino Unido**

Debido a que nuestras oficinas de país de Tearfund no se consideran personas jurídicas separadas y comparten datos personales en el marco de los fines de Tearfund, asumimos que este tratamiento está sujeto a lo dispuesto por el RGPD del Reino Unido. Por consiguiente, el RGPD del Reino Unido se aplica a los datos de las personas participantes de los proyectos que son recopilados en el país en cuestión, a los expedientes del personal nacional, etc., y es por este motivo que todo el personal debe cumplir esta política.

**Transferencias internacionales**

Todo acceso a datos personales en otro país se considera una «transferencia» de los datos a dicho país. Por ejemplo, si un miembro del personal abre en India un documento Google que contiene datos personales, esto se considera una transferencia de dichos datos a India. En virtud del RGPD, la postura predeterminada es que los datos personales no pueden transferirse ni consultarse desde fuera del Reino Unido a menos que se cumpla por lo menos una de las siguientes condiciones: (i) que la Comisión Europea haya declarado que el país importador de datos es un «país que garantice un nivel adecuado de protección» o bien (ii) que se hayan estipulado garantías adecuadas, como por ejemplo, normas corporativas vinculantes o cláusulas contractuales tipo (cláusulas estandarizadas aprobadas por la Comisión Europea). El Reino Unido ha establecido que las leyes de protección de datos de la Unión Europea son adecuadas y, a su vez, la Unión Europea ha establecido que las leyes de protección de datos del Reino Unido son suficientemente robustas. Esto significa que los datos pueden fluir de manera segura del Reino Unido a la Unión Europea y viceversa.

Tearfund cuenta con acuerdos de transferencia de datos que incluyen cláusulas contractuales tipo para permitir la transferencia de datos entre miembros de la familia Tearfund junto con una Declaración de garantía («Declaración») con respecto a la transferencia de datos personales desde Tearfund Reino Unido a otras oficinas de país de Tearfund.

**Legislación local**

Además de esta política, deben cumplirse las leyes aplicables en los países donde trabaja Tearfund cuando se recopilen y traten datos personales. Allí donde dichas leyes aplicables exijan protecciones más estrictas para los datos personales, Tearfund deberá cumplir plenamente dichas exigencias y, cuando sea necesario, implementar políticas y procesos adicionales.

**Datos personales compartidos**

Los datos personales (incluyendo información básica, como los nombres) no podrán compartirse con terceros externos a Tearfund (lo cual incluye a contratistas, proveedores, organizaciones socias, donantes, etc.) a menos que la acción de compartirlos satisfaga los principios de protección de datos, se haya formalizado un contrato y se otorguen garantías (que deben constar en el contrato) de que dichos terceros cuentan con las medidas técnicas y organizacionales adecuadas para proteger los datos personales. Puede solicitar al equipo jurídico de Tearfund las cláusulas de protección de datos compatibles con el RGPD para su inclusión en los contratos. Para solicitar la cláusula estándar de Tearfund compatible con el RGPD escriba a legal@tearfund.org.

**Protección de datos de niños y niñas**

Cuando nos basamos en el consentimiento como motivo para el tratamiento de los datos

personales de niños y niñas, debe tenerse en cuenta de que solo se admitirá el consentimiento de niños y niñas mayores de 13 años (en el Reino Unido). En otros países de la Unión Europea, la edad mínima puede ser 16 años. En cuanto a los niños y niñas menores de 13 años, necesitaremos el consentimiento de la persona que asume la responsabilidad parental, y deberemos adoptar las medidas necesarias para verificarla.

## Apéndice 1

1. Notificación de privacidad para el personal
2. Legitimate Business Interest Assessment (Evaluación de legítimo interés comercial)
3. Retention Policy (Política de retención de datos)
4. Guidelines on Handling Personal Data (Directrices para el manejo de datos personales)
5. Data Privacy Impact Assessment (Evaluación de Impacto de la Protección de Datos)