# POLÍTICA DE SCI: POLÍTICA DE PROTECCIÓN DE DATOS

| | |
|---|---|
| Ámbito funcional: | Seguridad de la información y protección de datos |
| Propietaria (nombre y cargo): | Deborah McManamon, responsable de protección de datos |
| Aprobado por: | Gareth Packham, director de la seguridad de la información y la protección de datos |
| Fecha de aprobación: | Octubre de 2022 |
| Versión: | V5.0 |
| Fecha para revisión: | Octubre de 2023 |
| Idiomas (incl. enlaces): | Español |
| Aplicable a: | Los/as empleados/as, trabajadores/as, voluntarios/as, personas que están en prácticas, consultoras de Save the Children International ("SCI") y empleados/as de los miembros en comisión de servicios para SCI. |

## SECCIÓN 1: OBJETO

Save the Children International (SCI) se compromete a utilizar los datos personales de forma responsable y a garantizar que todo el personal entienda y cumpla sus responsabilidades en virtud de esta política de protección de datos y de la ley, incluida la legislación en materia de protección de datos del Reino Unido y cualquier legislación local de protección de datos aplicable. SCA adopta el RGPD como norma, pero cuando exista legislación local que tenga requisitos diferentes o más estrictos que los establecidos en esta política, deberán cumplirse dichos requisitos locales.

SCI reconoce que el tratamiento correcto y legal de los datos personales es una responsabilidad fundamental. La incapacidad de proteger de forma adecuada los datos personales podría perjudicar a otras personas. También podría causar daños a la reputación de Save the Children, pérdida de ingresos o importantes sanciones económicas.

Esta política establece los principios que SCI aplica a la hora de tratar y proteger los datos personales que se nos confían y establece las obligaciones del personal en relación con los

datos que recopilamos y utilizamos. Cada uno de los miembros del personal tiene la responsabilidad de proteger los datos personales que están a cargo de SCI.

Esta política es obligatoria para todo el personal, y todo el personal debe leer y cumplir esta política, así como todos los procedimientos y las orientaciones relacionados.

Si tiene alguna duda acerca de esta política, póngase en contacto con el/la delegado/a de protección de datos (DPD) de SCI en la dirección dpo@savethechildren.org.

## SECCIÓN 2: DECLARACIONES POLÍTICAS

| | |
|---|---|
| **1.** | **Liderazgo y supervisión**<br><br>Un elemento fundamental de la rendición de cuentas es un liderazgo y una supervisión sólidos. Esto incluye garantizar que el personal tenga sus responsabilidades claras en las actividades relacionadas con la protección de datos a nivel estratégico y operativo. Todos/as los/as empleados/as y voluntarios/as tienen la responsabilidad de cumplir esta política cuando traten datos personales.<br><br>El equipo de liderazgo superior (SLT) de SCI y el consejo de administración son los/as responsables estratégicos/as de la protección de datos. El Comité de auditorías y riesgos del consejo de administración recibe reportes trimestrales sobre cuestiones y riesgos relacionados con la protección de datos. El comité directivo de protección de datos, presidido por el/la director/a de operaciones y facilitado por el/la director/a de riesgos, da parte al equipo de liderazgo superior.<br><br>SCI está obligado a contar con un/a delegado/a de la protección de datos, debido a la naturaleza de los datos personales que recopilamos y utilizamos. La función del/de la DPD consiste en asesorar y monitorear el cumplimiento de esta política y de las obligaciones jurídicas de SCI, asesorar sobre las evaluaciones de impacto relacionado con la protección de datos y actuar como punto de contacto para los/as titulares de los datos y la Information Commissioner's Office (Oficina del comisionado de información) del Reino Unido. El/la DPD es el/la secretario/a del comité directivo de protección de datos.<br><br>El equipo de protección de datos cuenta con el apoyo de una red de puntos focales de protección de datos en las Oficinas País que apoyan la implementación a nivel local.<br><br>SCI está registrada en la Oficina del comisionado de información del Reino Unido con el número de registro Z3214775. |
| **2.** | **Principios de protección de datos**<br><br>Cualquier uso de los datos personales debe ajustarse a los principios de protección de datos, y debemos poder demostrar que así lo hacemos. Los principios son:<br><br>a) **Legalidad, equidad y transparencia:** los datos personales deben ser tratados de forma legal, justa y transparente.<br>b) **Limitación del objeto**: los datos personales solo deben recogerse con fines específicos, explícitos y legítimos.<br>c) **Minimización de datos**: los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan. Siempre que sea posible, SCI debe aplicar la anonimización o la |

| | |
|---|---|
| | seudonimización a los datos personales para reducir los riesgos para los/as titulares de los datos.<br>d) **Precisión:** los datos personales deben ser precisos y, en su caso, estar actualizados, teniendo en cuenta los fines para los que se tratan.<br>e) **Limitación de almacenamiento:** los datos personales no deben conservarse más allá del tiempo necesario para sus fines.<br>f) **Integridad y confidencialidad:** Deben adoptarse medidas técnicas u organizativas adecuadas para garantizar la seguridad de los datos personales, incluida la protección ante la destrucción accidental o ilegal, la pérdida, la alteración, el acceso no autorizado o la divulgación.<br>g) **Rendición de cuentas:** los/as responsables del tratamiento de datos deben cumplir los principios antes mencionados, y poder demostrar dicho cumplimiento. Esto incluye la responsabilidad ante los datos personales tratados en nuestro nombre.<br><br>Todo el personal debe respetar estos principios al recoger y utilizar datos personales. |
| **3.** | **Legalidad del tratamiento**<br><br>Siempre que se traten datos personales, debe hacerse en el marco de una de las siguientes **bases jurídicas**:<br><br>a) el/la titular de los datos ha dado su **consentimiento**<br>b) el tratamiento es **necesario para la ejecución de un contrato** con el/la titular de los datos<br>c) el tratamiento es **necesario** para cumplir **obligaciones legales**<br>d) el tratamiento es **necesario** para proteger los **intereses vitales** del/de la titular de los datos;<br>e) el tratamiento es **necesario** para el desempeño de una labor de interés público; o<br>f) el tratamiento es **necesario** para dedicarse a los **intereses legítimos** de SCI.<br><br>SCI debe identificar la base jurídica en la que se basa cada actividad de tratamiento y documentarla en nuestros registros<br><br>Cuando los datos personales incluyen datos de "categoría especial" (datos personales que requieren medidas reforzadas de protección de datos debido a su naturaleza sensible y personal) también necesitamos tener una justificación adicional (según lo establecido en la legislación) para utilizar esos datos.<br><br>**Consentimiento**<br><br>El consentimiento no siempre será la base jurídica más adecuada, pero cuando se recurra a él, debemos asegurarnos de que se da libremente, con conocimiento de causa, de forma específica e inequívoca. Debe mostrarse claramente mediante una declaración o una acción afirmativa. |

| | |
|---|---|
| | El personal que elabore declaraciones de consentimiento o gestione procesos basados en el consentimiento debe seguir el Procedimiento de consentimiento y consultar la Orientación sobre consentimiento, que proporcionan información de apoyo.<br><br>**Niñez**<br><br>SCI reconoce que la niñez requiere una protección específica con respecto a sus datos personales y debemos garantizar que el principio de equidad y el interés superior de la niña o niño ocupen un lugar central en todo el tratamiento de los datos personales de la niñez. El consentimiento es una de las bases jurídicas posibles para el tratamiento de los datos personales de los niños, pero SCI reconoce que a veces es más adecuado utilizar un fundamento alternativo.<br><br>Cuando los datos personales se refieran a una **niña o niño menor de 18 años**, debemos asegurarnos de que esta/e pueda comprender las implicaciones de la recogida y el tratamiento de sus datos personales. Si la niña o niño no es capaz de comprender, deberá utilizarse una base alternativa, o deberá solicitarse el consentimiento de las madres, los padres o tutores/as (a menos que esto no sea en el interés superior de la niña o niño). |
| **4.** | **Transparencia**<br><br>La transparencia está fundamentalmente vinculada a la equidad, y al derecho que tienen los/as titulares de los datos a ser informados/as sobre quiénes somos, cómo y por qué utilizamos sus datos personales, y con quiénes los compartimos.<br><br>SCI se compromete a ser clara, abierta y honesta con las personas desde el principio. Esto ayuda a las personas a tomar decisiones informadas sobre el uso de sus datos, cuando sea adecuado, y a ejercer sus derechos.<br><br>Cuando se recojan datos personales de niñez, deberemos proporcionarle información adaptada a su edad para que pueda entender qué pasará con sus datos personales y qué derechos tiene.<br><br>El personal que participe en la recopilación o el uso de datos personales deberá familiarizarse con la información sobre la privacidad y con la forma de explicarla.<br><br>El personal responsable de redactar la información sobre privacidad o de garantizar que se facilite debe asegurarse de que incluye todos los elementos del GDPR del Reino Unido u otra legislación aplicable consultando la Orientación de transparencia y siguiendo el Procedimiento para facilitar avisos sobre privacidad del Marco de calidad. |
| **5.** | **Formación y concienciación** |

| | |
|---|---|
| | Todo el personal debe realizar la formación obligatoria en materia de protección de datos y seguridad de la información en un plazo de 3 meses desde su incorporación a SCI. Esta formación debe renovarse cada 12 meses, o con mayor frecuencia si así se indica.<br><br>El personal que desempeña funciones especializadas puede tener que recibir formación adicional para cumplir con sus responsabilidades.<br><br>Puede encontrar más información y orientaciones en OneNet aquí, y el equipo de protección de datos está disponible para proporcionar asesoramiento y orientación. |
| **6.** | **Derechos de las personas sobre los datos**<br><br>Los/as titulares de los datos (incluida la niñez) tienen derechos sobre sus datos, incluido el derecho a solicitar una copia de sus datos a SCI, lo que se conoce como "solicitud de acceso del titular" o SAT.<br><br>Si recibe una solicitud de acceso del/de la titular o de otro tipo, póngase en contacto con el equipo de protección de datos por correo electrónico a subjectaccessrequest@savethechildren.org. También puede remitir a los/as usuarios/as al Aviso de privacidad de nuestro sitio web, donde encontrarán más información. Mientras tanto, **no debe** revelar ninguna información a la persona.<br><br>Los derechos sobre los datos según la legislación británica de protección de datos son los siguientes:<br><br>• **Derecho a ser informado** Los/as titulares de los datos tienen derecho a conocer las actividades de protección y tratamiento de datos personales de SCI, que se detallarán en los avisos de privacidad de SCI.<br><br>• **Derecho de acceso** Los/as titulares de los datos pueden presentar una solicitud de acceso del/de la titular ("SAT") para pedir una copia de sus datos personales.<br>• **Derecho de rectificación** Los/as titulares de los datos tienen derecho a solicitar que se corrija cualquier información incompleta o inexacta.<br>• **Derecho de supresión (a veces llamado "derecho al olvido")** Los/as titulares de los datos tienen derecho a solicitar que SCI elimine sus datos.<br>• **Derecho a la limitación del tratamiento** Los/as titulares de los datos pueden solicitar que SCI deje de tratar sus datos para un fin determinado.<br>• **Derecho a la portabilidad de los datos** Los/as titulares de los datos pueden solicitar a SCI que les proporcione copias de los datos personales que posea sobre ellos en un formato de uso común y fácil lectura para transferirlos a otra organización (en circunstancias limitadas: consulte al equipo de protección de datos para obtener más detalles). |

| | |
|---|---|
| | • **Derecho de oposición** Los/as titulares de los datos tienen derecho a oponerse al uso de sus datos en algunas circunstancias. Si sus datos se utilizan con fines de mercado y se oponen a ello, el derecho es absoluto y debemos dejar de utilizar sus datos personales para venderles o promocionarles productos, o para recaudar fondos.<br>• **Derechos en relación con el tratamiento automatizado** Los/as titulares de los datos tienen derecho a impugnar decisiones y a solicitar una revisión.<br>• **Derecho a retirar el consentimiento** Si SCI se basa en un consentimiento para el tratamiento de sus datos personales, el/la titular de los datos tiene derecho a retirar su consentimiento en cualquier momento. |
| **7.** | **Contratos e intercambio de datos**<br><br>Cuando SCI recurre a terceros proveedores o prestadores de servicios para procesar los datos personales en nuestro nombre, nos aseguramos de que aplican las medidas adecuadas para proteger nuestros datos. Esto incluye lo siguiente:<br><br>• Realizar una evaluación de sus medidas de protección de datos y de seguridad de la información, cuando proceda<br>• Garantizar que los contratos incluyan cláusulas de protección de datos.<br><br>Los/as directivos/as responsables de las decisiones de contratación deben asegurarse de que siguen los procedimientos acordados y utilizan los modelos de contrato adecuados.<br><br>**Intercambio de datos**<br><br>En el caso del intercambio periódico o sistemático de datos personales con otras organizaciones que no estén sujetas a un contrato, debemos acordar la finalidad del intercambio y las responsabilidades respectivas en relación con los datos, por ejemplo, responder a las solicitudes de acceso de los/as titulares. Todo esto debe establecerse en un acuerdo de intercambio de datos.<br><br>En el caso de las solicitudes de datos personales de otras organizaciones (incluidas las autoridades o las entidades reguladoras) que no estén cubiertas por un contrato o un acuerdo de intercambio de datos, solicite el asesoramiento del equipo de protección de datos. |
| **8.** | **Evaluación del impacto de la protección de datos y los riesgos**<br><br>La evaluación del impacto de la protección de datos (EIPD) es un proceso que ayuda a identificar y minimizar los riesgos de la protección de datos, especialmente cuando se implementan nuevos procesos o sistemas. |

| | |
|---|---|
| | **Debe** efectuarse cuando exista un alto riesgo para las personas y para algunos tipos específicos de tratamiento, como el seguimiento de la ubicación, la prestación de servicios en línea a la niñez y el tratamiento de datos biométricos o genéticos. Encontrará información más detallada al respecto en la Orientación de apoyo y procedimiento DPIA.<br><br>Cuando ya se haya realizado una DPIA que aborde los riesgos de protección de datos y de seguridad de la información para un proyecto o programa similar y se considere aplicable al tratamiento previsto, es posible que no se requiera otra DPIA; no obstante, los/as responsables deben solicitar el asesoramiento del equipo de protección de datos para que esto quede documentado. |
| **9.** | **Gestión y seguridad de registros**<br><br>Una buena gestión de los registros contribuye a una correcta gobernanza y protección de los datos. La seguridad de la información también contribuye a una buena gobernanza de los datos, y constituye, en sí misma, un requisito legal de la protección de datos. Una seguridad de la información deficiente pone en riesgo nuestros sistemas y servicios y puede causar un daño real y dolor a las personas.<br><br>Todo el personal debe cumplir la Política de uso aceptable de las tecnologías de la información de SCI, que establece con más detalle las precauciones pertinentes que el personal debe tomar para garantizar la seguridad de los datos, incluido el uso seguro del correo electrónico, Internet y los dispositivos móviles.<br><br>Llevamos un registro de los usos que hacemos de los datos personales en toda la organización, que gestiona el equipo de protección de datos. |
| **10.** | **Conservación de datos**<br><br>Como principio, los datos personales solo deben conservarse el tiempo necesario en relación con el fin para el que se recogieron y para cumplir cualquier obligación específica de mantenimiento de registros. Este periodo de conservación debe establecerse cuando los datos se recogen o utilizan por primera vez, y debe explicarse a los/as titulares de los datos en el aviso de privacidad.<br><br>A la hora de establecer los periodos de conservación hay que tener en cuenta lo siguiente: |

| | |
|---|---|
| | • Si existe alguna obligación legal sobre la conservación de datos o registros durante un periodo mínimo específico.<br>• Si tenemos alguna obligación contractual que establezca el tiempo que debemos conservar los registros y cómo deben tratarse al final del periodo.<br>• Si existe una necesidad operativa específica que deba satisfacerse.<br><br>Al revisar los datos y los registros para su eliminación, los/as responsables de la toma de decisiones también deben considerar si los datos o los registros pueden tener un valor permanente para la organización, o para la sociedad en general, que pudiera justificar su conservación.<br><br>Los periodos de conservación de los datos deben incluirse en los contratos o acuerdos con los proveedores u organizaciones socias que actúan en nuestro nombre, y los/as responsables de los contratos deben asegurarse de que se siguen las instrucciones de SCI y de que los datos se nos devuelven o se eliminan al final del contrato, a menos que se acuerde lo contrario.<br><br>Si desea una orientación más detallada, consulte el programa y la política de conservación de registros, que establece los periodos mínimos de conservación de determinados tipos de registros. |

| | |
|---|---|
| **11.** | **Transferencias internacionales de datos**<br><br>SCI debe asegurarse de que existen las garantías adecuadas antes de transferir los datos personales a nivel internacional. Esto incluye los casos en los que SCI actúa como procesadora de datos en nombre de los miembros de SC.<br><br>Los nuevos procesos que puedan incluir transferencias de datos personales no deben iniciarse sin consultar previamente al equipo de protección de datos. |
| **12.** | **Control y respuesta ante violaciones**<br><br>Por "violación de los datos personales" se entiende una violación de la seguridad que provoque la destrucción accidental o ilegal, la pérdida, la alteración, la difusión no autorizada o el acceso a datos personales transmitidos, almacenados o tratados de otro modo.<br><br>Una violación puede ser consecuencia de la pérdida o el robo de los propios datos, o del equipo o dispositivo en el que están almacenados, como un ordenador portátil o un teléfono.<br><br>El equipo de seguridad de la información y la protección de datos gestiona los incidentes relacionados con los datos.<br><br>Las violaciones relacionadas con los datos, o las sospechas de violaciones, deben notificarse a través del sistema de gestión de incidentes de Datix lo antes posible e, idealmente, en un plazo de 12 horas. De este modo, podemos adoptar rápidamente medidas para reducir el riesgo para las personas y cumplir nuestras obligaciones de notificación a los organismos reguladores del Reino Unido y/o de otras jurisdicciones, en su caso. |
| **13.** | **Incumplimiento de la política**<br><br>Si sospecha de algún tipo de incumplimiento respecto a esta política, póngase en contacto con el/la DPD en dpo@savethechildren.org. Si lo prefiere, puede seguir la política y los procedimientos de denuncia anónima (silbato de alarma) de irregularidades de SCI.<br><br>El incumplimiento de esta política puede dar lugar a medidas disciplinarias. |

## SECCIÓN 3: DEFINICIONES

| Término | Definición |
|---|---|
| Tenga en cuenta que los términos utilizados o definidos en el RGPD se han trasladado a la legislación sobre datos de otras jurisdicciones. | |
| Anonimización | Como se utiliza en el RGPD y en el RGPD del Reino Unido<br>El proceso de eliminar información o características de los datos que permitirían utilizarlos para identificar a los/as "interesados/as". Si los datos se procesan de tal forma que el/la interesado/a no es identificable, o deja de serlo, no se aplica la legislación sobre protección de datos.<br>Al considerar si los datos se han anonimizado, debemos tener en cuenta todos los medios que sea razonablemente probable que utilicemos, nosotros mismos o una tercera parte, para identificar a una persona a la que se refiera la información.<br>El proceso de eliminar de los datos información o características que permitirían utilizarlos para identificar al interesado del que se obtuvieron. Los datos se presentan de tal forma que el/la interesado/a deja de ser identificable.<br>Tenga en cuenta que debemos ser conscientes de la posibilidad de reidentificación y del riesgo que suponen los datos para grupos y comunidades, incluso cuando no se pueda identificar a ninguna persona. |
| Disponibilidad | Los datos son accesibles y utilizables por quienes están autorizados a acceder a ellos siempre que sea necesario. La pérdida de disponibilidad de los datos, incluso si no son revelados o accedidos por terceras personas, podría constituir una violación de datos. |
| Datos biométricos | Tal como se define en el RGPD y en el RGPD del Reino Unido<br>Datos personales resultantes de un tratamiento técnico específico relativo a las características físicas, fisiológicas o de comportamiento de una persona física, que permitan o confirmen la identificación única de dicha persona física, como imágenes faciales o datos dactiloscópicos*.<br>*fingerprint |

| | |
|---|---|
| Datos confidenciales | Datos que no son de dominio público y que se comparten o divulgan en circunstancias que crean la obligación de mantenerlos confidenciales (por ejemplo, sujetos a un acuerdo de no divulgación o debido a la relación entre las partes implicadas).<br><br>Tenga en cuenta que marcar los datos o documentos como "confidenciales" puede ser un indicador útil de cómo deben tratarse, pero no necesariamente protegerá la información de su divulgación en todas las circunstancias (por ejemplo, si una persona realiza una solicitud de acceso bajo el RGPD u otra legislación de protección de datos). |
| Consentimiento | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Por consentimiento del/de la interesado/a se entenderá toda manifestación de voluntad, libre, específica, informada e inequívoca, mediante la que el/la interesado/a consienta, por declaración o mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernan; |
| Datos relativos a la salud | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Datos personales relacionados con la salud física o mental de una persona física, incluida la prestación de servicios sanitarios, que revelen información sobre su estado de salud. |
| Responsable de los datos: | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>La persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o conjuntamente con otros, determine los fines y medios del tratamiento de datos personales |
| Procesador/a de datos | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Persona física o jurídica, autoridad pública, agencia u otro organismo que trate datos personales por cuenta del/de la responsable del tratamiento; |
| Datix | Datix es un sistema de gestión de casos y notificación de incidentes basado en la nube. Todos los incidentes relacionados con el fraude, la protección de menores, la protección de personas adultas, la seguridad, la seguridad médica, la seguridad informática y la protección de datos. en SCI deben notificarse en Datix. |
| Evaluación del impacto de la protección de datos y los riesgos (DPIA) | Como se utiliza en el RGPD y en el RGPD del Reino Unido<br><br>Un proceso para identificar y mitigar los riesgos para las personas derivados del tratamiento de datos personales, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como las fuentes del riesgo. |

| | |
|---|---|
| Responsable de la protección de datos | Como se utiliza en el RGPD y en el RGPD del Reino Unido<br><br>Persona responsable designada para monitorear el cumplimiento de las obligaciones en materia de protección de datos, asesorar sobre la evaluación de impacto de la protección de datos y otros procesos, y actuar como punto de contacto para los interesados y las autoridades supervisoras. La propia organización sigue siendo responsable del cumplimiento de la legislación sobre protección de datos.<br><br>Puede ponerse en contacto con el/la responsable de protección de datos del SCI en dpo@savethechildren.org<br><br>La legislación de algunas otras jurisdicciones también exige el nombramiento de un/a responsable de protección de datos o función similar. |
| Sistema de archivo | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Cualquier conjunto estructurado de datos personales accesibles con arreglo a criterios específicos, ya sean centralizados, descentralizados o dispersos sobre una base funcional o geográfica. |
| Datos genéticos | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan información única sobre la fisiología o la salud de dicha persona física y que resultan, en particular, de un análisis de una muestra biológica de la persona física en cuestión. |
| Activo de información | Conjunto de información que puede gestionarse como una sola unidad, con un contenido y un valor reconocibles. Un activo de información puede tener cualquier formato. |
| Propietario/a de activos de información | El/la propietario/a de un activo de información con la responsabilidad de garantizar que se maneja de acuerdo con las políticas de SCI y las orientaciones y procedimientos de apoyo.<br><br>El IAO debe ser un/a alto/a responsable de la dirección o función correspondiente. |
| Seguridad de la información | Según la definición del NIST (Departamento de comercio de EE. UU.)<br><br>Proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de proporcionar:<br><br>• Integridad, es decir, protección contra la modificación |

| | |
|---|---|
| | o destrucción indebidas de la información, e incluye garantizar el no repudio y la autenticidad de la información.<br>• Confidencialidad, que significa preservar las restricciones autorizadas de acceso y divulgación, incluidos los medios para proteger la intimidad personal y la información sujeta a derechos de propiedad.<br>• Disponibilidad, lo que significa garantizar el acceso y uso oportunos y fiables de la información. |
| Servicio de la sociedad de la información | Tal como se define en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo<br><br>Todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un/a destinatario/a de servicios. |
| Organización internacional | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Una organización y sus órganos subordinados regidos por el Derecho internacional público, o cualquier otro órgano creado por un acuerdo entre dos o más países o sobre la base de dicho acuerdo. |
| Oficina del Comisario de Información (ICO) (Reino Unido) | La Oficina del Comisario de Información (ICO) es el organismo público independiente del Reino Unido que regula los derechos de información en interés público.<br><br>Además de la legislación de protección de datos (RGPD del Reino Unido y la Ley de protección de datos de 2018), regula la legislación relativa a PECR (comunicaciones electrónicas), eIDAS (transacciones electrónicas), NIS (seguridad de la infraestructura nacional), reutilización de la información pública y poderes de investigación. En Inglaterra, Gales e Irlanda del Norte, la ICO también regula la libertad de información, la información medioambiental y la legislación INSPIRE. |
| Secreto profesional<br><br>(Inglaterra y Gales) | La protección frente a la divulgación de determinadas comunicaciones confidenciales (incluido el correo electrónico):<br>• Entre abogados/as (incluidos/as los/as internos/as) y clientes con el propósito exclusivo o dominante de dar o recibir asesoramiento jurídico (secreto profesional del asesoramiento jurídico).<br>• Entre abogados/as (incluidos/as los/as internos/as) o sus clientes y cualquier tercera parte con el fin exclusivo o principal de obtener asesoramiento o información en relación con un litigio en curso o razonablemente previsto (secreto profesional en litigios). |

| | |
|---|---|
| | Algunas disposiciones de la legislación británica sobre protección de datos, incluido el derecho de acceso, no se aplican a la información legalmente privilegiada. |
| Datos personales<br><br>(Aunque a veces se utilizan indistintamente, los términos "datos confidenciales" y "datos personales" no son lo mismo). | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Cualquier información relativa a una persona física identificada o identificable ("interesado/a"); una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física. |
| Violación de datos personales | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Por "violación de los datos personales" se entiende una violación de la seguridad que provoque la destrucción accidental o ilegal, la pérdida, la alteración, la difusión no autorizada o el acceso a datos personales transmitidos, almacenados o tratados de otro modo. |
| Tratamiento | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Cualquier operación o conjunto de operaciones, efectuadas con datos personales o conjuntos de datos personales, por medios automatizados o no, como su recogida, registro, organización, estructuración, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de puesta a disposición, limitación, supresión o destrucción. |
| Perfil | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Cualquier forma de tratamiento automatizado de datos personales consistente en la utilización de datos personales para evaluar determinados aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relativos al rendimiento laboral, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de dicha persona física. |
| Seudonimización | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>El tratamiento de datos personales de tal forma que los datos personales ya no puedan atribuirse a un interesado concreto sin utilizar información adicional, siempre que dicha información adicional se conserve por separado y esté sujeta a medidas técnicas y organizativas que garanticen que los datos personales no se atribuyen a una persona física identificada o identificable. |

| | |
|---|---|
| Destinatario/a | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Una persona física o jurídica, autoridad pública, agencia u otro organismo al que se comuniquen los datos personales, ya sea una tercera parte o no. No obstante, las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con[el Derecho interno del Reino Unido o el Derecho de la Unión o de los Estados miembros] no tendrán la consideración de destinatarios/as; el tratamiento de dichos datos por dichas autoridades públicas deberá ajustarse a las normas de protección de datos aplicables en función de los fines del tratamiento. |
| Restricción del tratamiento | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>El marcado de los datos personales almacenados con el fin de limitar su tratamiento en el futuro. |
| Datos de categoría especial<br><br>(a veces denominados datos personales sensibles) | Como se utiliza en el RGPD y en elRGPD del Reino Unido<br><br>Subcategoría de datos personales que requiere medidas reforzadas de protección de datos debido a su naturaleza sensible y personal.<br><br>Datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos destinados a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual de una persona física.<br><br>**Tenga en cuenta** que en otras jurisdicciones la categoría especial o los datos personales sensibles pueden incluir otras categorías - por ejemplo, en la Ley de protección de datos y Privacidad de Uganda de 2019 se incluyen los datos financieros; y en la Ley de protección de datos de Kenia de 2019 incluye detalles de propiedad, estado civil, detalles familiares, incluidos los nombres de los hijos, padres, cónyuge o cónyuges de la persona. |
| Terceras partes | Tal como se define en el RGPD y en el RGPD del Reino Unido<br><br>Persona física o jurídica, autoridad pública, agencia u organismo distinto del interesado, responsable del tratamiento, encargada del tratamiento y personas que, bajo la autoridad directa del/de la responsable o del/de la encargado/a del tratamiento, estén autorizadas a tratar datos personales. |
| Registros de actividades de tratamiento | Como se utiliza en el RGPD y en el RGPD del Reino Unido<br><br>Resultado de un ejercicio de mapeo de datos. Documentación formal conservada por un/a |

| | |
|---|---|
| | responsable o encargado/a del tratamiento de datos sobre los usos de los datos personales en toda la organización.<br><br>Los registros de las actividades de tratamiento deben incluir información significativa sobre el tratamiento de datos, incluidas las categorías de datos, el grupo de personas interesadas, la finalidad del tratamiento y los/as destinatarios/as de los datos. Debe ponerse a disposición de las autoridades que lo soliciten.<br><br>En algunas otras jurisdicciones existen requisitos similares para conservar y/o presentar detalles del tratamiento a las autoridades de supervisión. |
| Formulario de solicitud de acceso para titulares | Como se utiliza en el RGPD y en el RGPD del Reino Unido<br><br>Solicitud de un/a "interesado/a" de una copia de sus datos personales en poder de un/a responsable del tratamiento. |

## SECCIÓN 4: DOCUMENTACIÓN RELACIONADA

| DOCUMENTO | UBICACIÓN |
|---|---|
| SCI_IT_DP_DPIA_Guidance_EN | Marco de calidad de SCI |
| SCI_IT_DP_DPIA_Procedure_EN | Marco de calidad de SCI |
| SCI_IT_DP_Transparency_Guidance_EN | Marco de calidad de SCI |
| SCI_IT_DP_Privacy_Notice_Procedure_EN | Marco de calidad de SCI |
| SCI_IT_DP_Consent_Guidance_EN | Marco de calidad de SCI |
| SCI_IT_DP_Consent_Procedure_EN | Marco de calidad de SCI |
| SCI_IT_DP_Records_Retention_Procedure_EN | Marco de calidad de SCI |
| Política de uso aceptable de las tecnologías de la información | |
| Política de seguridad informática | |
| Aviso de privacidad de SCI | Sitio web de SCI |