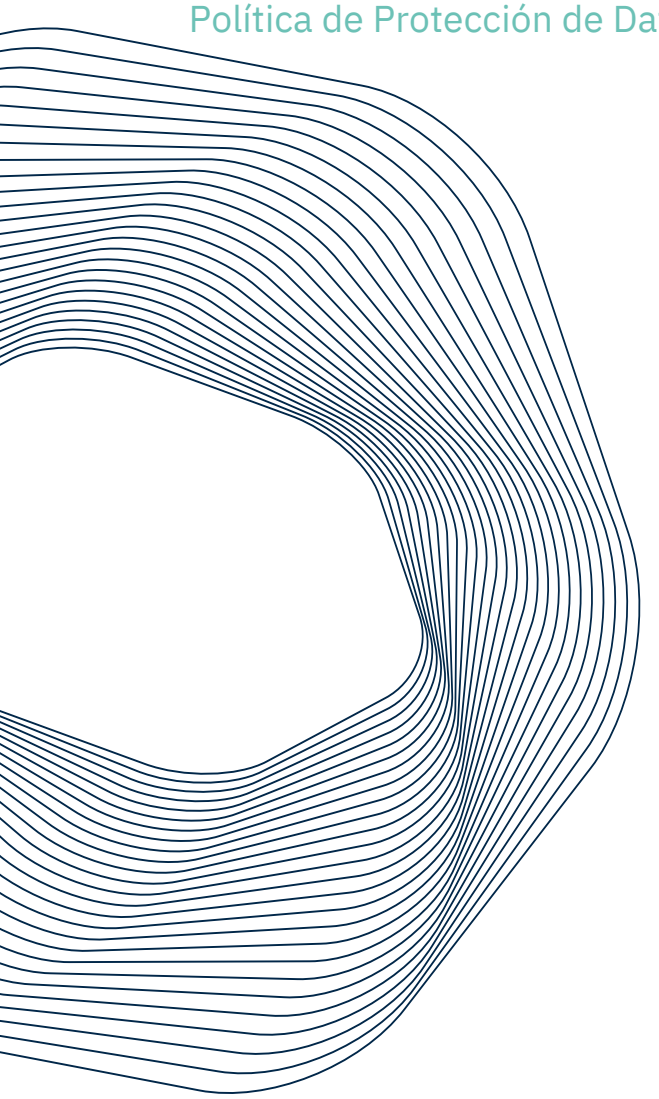
FutureLife

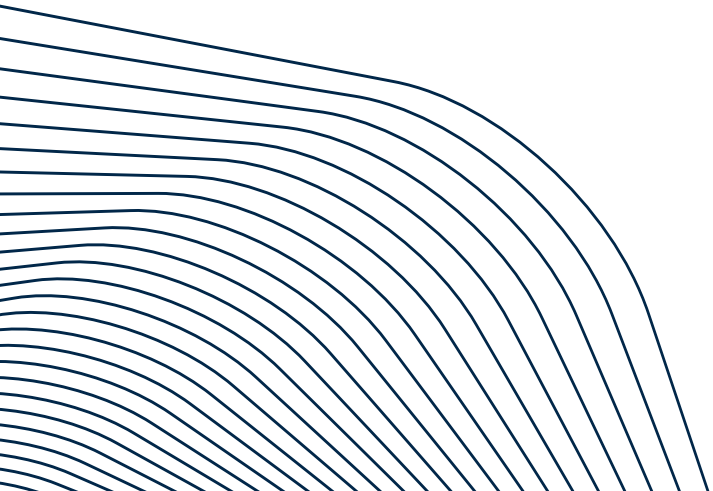
SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

FUTURELIFE A.S.

Versión: 1.0
Fecha: 15-09-2025
Clasificación: INTERNA





FutureLife

Política de Protección de Datos Personales

Título del documento:	Política de Protección de Datos Personales	FutureLife a.s.
Subtítulo:	Sistema de Gestión de Datos Personales	Na příkopě 859/22
Persona de contacto 1:	Maroš Zuba	Nové Město, 110 00 Praga 1
Departamento:	Digital	República Checa
Persona de contacto 2:	Ilja David	
Departamento:	Digital	
Documento:	FL-DP-P1	
Fecha de emisión:	15-09-2025	

Contenido del documento:

La Política de Protección de Datos Personales describe cómo el Grupo FutureLife trata los datos personales recopilados de sistemas internos, plataformas digitales y otras fuentes relevantes dentro de la organización. Esta política es obligatoria para toda la organización, incluidos todos los empleados, colaboradores, filiales y socios externos que manejan datos personales. La política cumple con el RGPD y otras leyes aplicables, así como con los requisitos de la norma ISO/IEC 27701, que amplía la norma ISO/IEC 27001 mediante la incorporación de mecanismos de control adicionales y directrices para la gestión de datos personales y la información sobre protección de datos personales.

Creado por:	**Verificado por:**	**Aprobado por:**
Ilja David	Maroš Zuba	Ignacio Couto
Gerente de Ciberseguridad	Jefe del Departamento Jurídico	CTO
Digital	Digital	Digital
FutureLife a.s.	FutureLife a.s.	FutureLife a.s.

Palabras clave:

Política de Protección de Datos Personales, tecnologías de la información, tecnologías operativas, protección, RGPD

Confidencialidad del documento:

☐ PÚBLICO. Datos disponibles públicamente relacionados con la actividad diaria de la organización o procesos conocidos públicamente.

☒ INTERNO. Datos confidenciales sobre el funcionamiento habitual del negocio o procesos internos de la organización.

☐ CONFIDENCIAL. Datos relacionados con actividades comerciales estratégicas, contratos, información financiera, datos personales y datos sobre el estado de salud.

SEGUIMIENTO DE CAMBIOS

Versión	Fecha	Motivo del cambio	Creado por	Verificado por	Aprobado por
1.0	15.09.2025	Primera Edición	Ilja David	Maroš Zuba	Ignacio Couto

ÍNDICE

1. INFORMACIÓN INTRODUCTORIA

1.1. PROPÓSITO

Esta Política de Protección de Datos Personales (en adelante, la "Política") establece un marco unificado para garantizar la protección de los datos personales dentro de FutureLife a.s. y de todas sus sociedades afiliadas pertenecientes al mismo grupo empresarial (en adelante, el "Grupo FutureLife"). Su propósito es definir los principios, roles y responsabilidades relacionados con el tratamiento de datos personales conforme a la normativa aplicable, incluido el RGPD (Reglamento General de Protección de Datos) y otras disposiciones nacionales relevantes.

1.2. ALCANCE

Esta Política se aplica a todos los procesos, tecnologías y entidades dentro del Grupo FutureLife que realicen actividades de tratamiento de datos personales, y asegura un enfoque uniforme para la protección de datos personales, la seguridad de la información y el ejercicio de los derechos de los interesados.

1.3. DOCUMENTOS RELACIONADOS

En esta sección se enumeran los documentos internos relacionados que respaldan y complementan la Política de Protección de Datos Personales:

- **FL-CS-P1 – Política de Ciberseguridad (Cybersecurity Policy):** marco normativo para la gestión de la ciberseguridad en la organización.
- **FL-CS-S1 – Ciberseguridad del Usuario Final (End User Cybersecurity):** estándar para el comportamiento seguro y la responsabilidad de los usuarios finales dentro de la organización.
- **FL-CS-S2 – Ciberseguridad de Proveedores (Supplier Cybersecurity):** estándar para la evaluación y gestión de riesgos de ciberseguridad relacionados con proveedores externos.
- **FL-CS-S6 – Plan de Continuidad del Negocio (Business Continuity Plan):** estándar para garantizar la resiliencia operativa y la recuperación ante interrupciones.
- **FL-CS-OP2 – Plan de Respuesta a Incidentes de Ciberseguridad (Cybersecurity Response Plan):** procedimiento para la detección, respuesta y recuperación ante incidentes de ciberseguridad.
- **FL-CS-OP3 – Ciclo de Vida del Desarrollo Seguro del Sistema (Secure System Development Lifecycle):** procedimiento para integrar medidas de seguridad en todo el proceso de desarrollo del sistema.
- **FL-CS-OP7 – Comunicación de Incidentes (Incident Communication):** procedimiento para la comunicación interna y externa durante incidentes de ciberseguridad.
- **FL-CS-OP09 – Nuevos Requisitos de Seguridad del Sistema (New System Security Requirements):** especificación de requisitos de seguridad para el diseño e implementación de nuevos sistemas.
- **FL-CS-S7 – Estándar de Seguridad para IA (AI Security Standard):** estándar para el uso seguro de herramientas de IA, incluyendo la protección de datos personales y organizativos, así como la infraestructura asociada.

- **FL-CS-S4 – Auditoría Interna (Internal Audit):** define los requisitos y responsabilidades para la auditoría interna como parte del Sistema de Gestión de la Ciberseguridad.

1.4. TÉRMINOS

TÉRMINO	EXPLICACIÓN
Responsable del tratamiento de datos personales	Persona física o jurídica que determina los fines y medios del tratamiento de datos personales.
Encargado del tratamiento de datos personales	Entidad que trata datos personales por cuenta del responsable del tratamiento.
Categorías especiales de datos personales	Información confidencial que, en caso de divulgación, podría causar daño, discriminación o pérdida a individuos u organizaciones, o poner en riesgo la seguridad nacional. Ejemplos: datos personales de salud (PHI), datos financieros, información personal identificable (PII), secretos comerciales y datos potencialmente sensibles.
Categorías especiales de datos	Datos personales sensibles, como datos de salud, datos genéticos, datos biométricos o información sobre origen racial o étnico.
Consentimiento	Manifestación de voluntad libre, específica, informada e inequívoca del interesado.
Cookies	Pequeños archivos de texto descargados y almacenados en el dispositivo del usuario que contienen una cantidad limitada de información.
Anonimización	Proceso de eliminación o modificación de identificadores personales de forma irreversible, para que no sea posible identificar al individuo.
Corresponsables	Dos o más entidades que determinan conjuntamente los fines y medios del tratamiento de datos personales.
Datos personales	Cualquier información relativa a una persona física identificada o identificable.
Datos sanitarios personales	Información médica confidencial que identifica a una persona y está relacionada con su salud física o mental pasada, presente o futura, la prestación de atención sanitaria o al pago de servicios sanitarios.
Uso primario de datos sanitarios	Utilización de la información recopilada directamente durante la prestación de atención sanitaria al individuo.
Uso secundario de datos sanitarios	Información recopilada durante la atención que se utiliza para fines distintos de la atención directa (p. ej., investigación, salud pública, planificación de servicios, mejora de calidad, desarrollo de políticas).

1.5. ABREVIATURAS

ABREVIATURA	EXPLICACIÓN
IA	Inteligencia Artificial (Artificial Intelligence, AI)
CRA	Reglamento de Ciberresiliencia (Cyber Resilience Act)
DPA	Anexo de Protección de Datos (Data Privacy Annexe)
EIPD	Evaluación de Impacto en la Protección de Datos (Data Protection Impact Assessment, DPIA)
DPO	Delegado de Protección de Datos (Data Protection Officer)
EEE	Espacio Económico Europeo (European Economic Area, EEA)
EEHRXF	Formato Europeo para el Intercambio de Historias Clínicas Electrónicas (European Electronic Health Record Exchange Format)
EEDS	Espacio Europeo de Datos de Salud (European Health Data Space, EHDS)
HCE	Historias Clínicas Electrónicas (Electronic Health Record, EHR)
RGPD	Reglamento General de Protección de Datos (General Data Protection Regulation, GDPR)
HDAB	Organismo de Acceso a Datos Sanitarios (Health Data Access Body)
NIS2	Directiva sobre Seguridad de Redes y Sistemas de Información (Network and Information Security Directive 2)
PDE	Producto con elementos digitales (Product with Digital Elements)

PHI	Datos personales de salud y categorías especiales de datos personales (Personal Health Information & Sensitive Data)
PII	Información de identificación personal (Personally Identifiable Information)
RACI	Matriz de Asignación de Responsabilidades (Responsibility Assignment Matrix)
SAE	Eventos Adversos Graves (Serious Adverse Events)
SAR	Reacciones Adversas Graves (Serious Adverse Reactions)
Sccs	Cláusulas Contractuales Tipo (Standard Contractual Clauses)
SoHO	Reglamento sobre las Sustancias de Origen Humano (Substances of Human Origins Regulation)

2. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

El Grupo FutureLife realiza todos los esfuerzos necesarios para respetar la privacidad y garantizar la seguridad de los datos personales que trata, conforme al Reglamento General de Protección de Datos (RGPD), la Directiva NIS2, el Espacio Europeo de Datos de Salud (European Health Data Space, EHDS), el Reglamento de la UE sobre Sustancias de Origen Humano (Substances of Human Origin, EU SoHO Regulation), el Plan de Acción de la UE para la Ciberseguridad hasta 2025, la Ley de Inteligencia Artificial de la UE (Artificial Intelligence Act, AI Act), el Reglamento de Ciberresiliencia (Cyber Resilience Act, CRA) y la normativa nacional aplicable en materia de protección de datos.

Esta Política de Protección de Datos Personales contiene información importante sobre los datos personales, los métodos de recopilación, uso y protección de los mismos, por lo que debe ser revisada cuidadosamente.

2.1. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

Los datos personales se tratan, según las circunstancias del caso, por el Grupo FutureLife y/o sus respectivas filiales como responsables del tratamiento para los fines descritos en esta Política de Protección de Datos Personales.

2.2. FUTURELIFE COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

Los datos personales son recopilados y tratados por el Grupo FutureLife como responsable del tratamiento en el marco de sus actividades organizativas, por ejemplo, al suscribirse a boletines informativos o al enviar una solicitud de información mediante formularios de contacto. Los datos identificativos del Grupo FutureLife, como responsable del tratamiento, son los siguientes:

2.2.1. FILIALES DEL GRUPO FUTURELIFE COMO RESPONSABLES DEL TRATAMIENTO

El Grupo FutureLife se considera responsable del tratamiento de los datos personales tratados en el marco de sus propias actividades operativas, incluyendo la prestación de servicios sanitarios, el mantenimiento de historiales médicos de pacientes y otras actividades empresariales autorizadas. La filial que opere un centro médico o clínica y que determine los fines y medios del de los datos personales para los fines anteriores será considerada responsable de dichos datos personales. Una lista completa de las filiales del Grupo FutureLife y sus clínicas sanitarias afiliadas está disponible previa solicitud.

La documentación médica es tratada exclusivamente por la clínica correspondiente del Grupo FutureLife que presta servicios sanitarios. El Grupo FutureLife no tiene, bajo ninguna circunstancia, acceso a información sanitaria personal identificable.

2.2.2. FUTURELIFE Y SUS FILIALES COMO CORRESPONSABLES DEL TRATAMIENTO

Dependiendo de la naturaleza de las actividades específicas, el Grupo FutureLife, junto con sus filiales, puede actuar como corresponsables del tratamiento de los datos personales de los usuarios, en particular para fines de marketing, para el envío de comunicaciones comerciales, relacionadas con el Grupo FutureLife, la realización de encuestas de mercado y de satisfacción, y la ejecución de otras funciones operativas y organizativas a nivel del Grupo.

2.3. GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL GRUPO FUTURELIFE

Los incidentes relacionados con la protección de datos personales se gestionan conforme al **Plan de Respuesta a Incidentes de Ciberseguridad (FL-CS-OP2)** del Grupo FutureLife.

Este plan establece procedimientos para la identificación, evaluación, notificación y resolución oportuna de incidentes de seguridad que puedan dar lugar a una violación de la seguridad de la seguridad de los datos personales.

El objetivo de estos procedimientos es minimizar el impacto sobre los interesados, garantizar la adopción de medidas correctivas adecuadas y cumplir con las obligaciones legales, incluida la obligación de notificación a la autoridad de control competente y a los interesados afectados.

3. ROLES Y RESPONSABILIDADES

Esta sección define los roles clave dentro del Grupo FutureLife y las responsabilidades en la protección de datos personales.

Para una descripción detallada de la asignación de roles y responsabilidades en el cumplimiento de esta Política de Protección de Datos Personales, se incluye una matriz RACI en el Anexo B.

3.1. DELEGADO DE PROTECCIÓN DE DATOS (DATA PROTECTION OFFICER, DPO)

En materia de protección de datos personales, el **DPO** debe:

- Monitorizar el cumplimiento de los principios y requisitos del RGPD y demás normativa aplicable en materia de protección de datos.
- Actuar como punto de contacto con la autoridad de control competente.
- Proporcionar directrices metodológicas y formación en protección de datos personales.
- Realizar auditorías internas y evaluaciones relacionadas con el tratamiento de datos personales.
- Asesorar en la realización de la Evaluación de Impacto en la Protección de Datos (Data Protection Impact Assessment, DPIA).
- Revisar y actualizar el Registro de Actividades de Tratamiento.
- Revisar y actualizar la documentación relativa a las actividades de tratamiento, incluyendo el mapa de procesos y los diagramas asociados.
- Mantener y conservar los registros de las actividades de tratamiento de datos personales.

3.2. DIRECTOR DE TRANSFORMACIÓN (CHIEF TRANSFORMATION OFFICER, CTO)

En materia de protección de datos personales, el **CTO** debe:

- Aprobar y supervisar la implementación de la Política de Protección de Datos Personales.
- Liderar iniciativas estratégicas relacionadas con la protección de datos en toda la organización.
- Garantizar la alineación de los procedimientos de protección de datos con los objetivos de transformación empresarial.
- Fomentar la coordinación interdisciplinaria en asuntos relacionados con la protección de la privacidad.
- Asegurar la implementación y ejecución de programas de formación y concienciación sobre protección de datos personales.
- Apoyar la aplicación de medidas disciplinarias adecuadas en casos de incumplimiento.

3.3. JEFE DEL DEPARTAMENTO JURÍDICO (HEAD OF LEGAL)

En materia de protección de datos personales, el Head of Legal asume el rol de Group Data Protection Officer (DPO del Grupo) y debe:

- Implementar y mantener medidas técnicas de seguridad para la protección de datos personales.
- Gestionar incidentes de ciberseguridad y violaciones de la seguridad de los datos personales.
- Apoyar los procesos de retención y supresión de datos.
- Colaborar con el Local DPO para garantizar el cumplimiento normativo a nivel de sistema.
- Realizar pruebas de seguridad, pruebas de penetración y análisis de riesgos periódicos.

- Proporcionar formación en ciberseguridad y el manejo seguro de datos personales.
- Colaborar con proveedores externos para garantizar la seguridad de los sistemas y los flujos de datos.
- Garantizar el cifrado, el control de acceso y otras medidas técnicas para proteger los datos personales.

3.4. Local Security Officer

En materia de protección de datos personales, el **Local Security Officer** debe:

- Garantizar el cumplimiento local de la Política de Protección de Datos Personales y del RGPD.
- Supervisar el manejo seguro de la documentación médica y otras categorías especiales de datos personales.
- Formar al personal de la clínica en los procedimientos de protección de datos.
- Reportar incidentes relacionados con datos personales a la unidad central de gestión.
- Asumir también el rol de Local DPO, si así lo establece la dirección.
- Coordinar con el DPO y el IT Manager la gestión de riesgos a nivel de clínica.

3.5. Gerente de Ciberseguridad

En materia de protección de datos personales, el **Gerente de Ciberseguridad** debe:

- Diseñar, implementar y mantener medidas de seguridad para la protección de datos personales.
- Monitorizar ciberamenazas y vulnerabilidades que puedan comprometer los datos personales.
- Coordinar la respuesta ante incidentes de seguridad y violaciones de seguridad de datos personales en colaboración con el Local DPO y el Head of Legal.

3.6. Business Owner (BO)

En materia de protección de datos personales, el **Business Owner** (BO) debe:

- Garantizar que las actividades de tratamiento de datos personales en su área cumplan con la Política de Protección de Datos Personales y la normativa aplicable (por ejemplo, RGPD).
- Colaborar con el DPO en la identificación y mitigación de riesgos relacionados con la protección de datos personales.
- Asegurar que los proveedores y los sistemas utilizados en su área cumplan con los requisitos de protección de datos y seguridad de la información.

Es responsable del uso legítimo de los datos personales en las aplicaciones y servicios bajo su gestión.

3.7. Funcional Owner (FO)

En materia de protección de datos personales, un **Functional Owner** (FO) debe:

- Garantizar la conformidad operativa con los requisitos de protección de datos dentro de su área funcional.
- Liderar la realización de la Evaluación de Impacto en la Protección de Datos (EIPD) en colaboración con el Business Owner y el Delegado de Protección de Datos (DPO).
- Asegurar que los procedimientos de tratamiento de datos personales estén documentados y cumplan con los estándares internos de protección de datos.

- Apoyar la ejecución de auditorías, revisiones y actualizaciones de sistemas y aplicaciones que traten datos personales.
- Iniciar y supervisar la elaboración de la EIPD para nuevas actividades de tratamiento o para aquellas que hayan sufrido cambios significativos.

Coordina con el área de TI y el departamento jurídico la implementación de medidas técnicas y organizativas para la protección de datos personales.

3.8. Departamento de Recursos Humanos (HR Department)

En materia de protección de datos personales, el Departamento de Recursos Humanos debe:

- Garantizar el tratamiento lícito de los datos personales de los empleados.
- Gestionar la protección de datos durante los procesos de selección, incorporación y extinción de la relación laboral.
- Asegurar la confidencialidad y el almacenamiento seguro de los registros de personal.

3.9. Todos los empleados

En materia de protección de datos personales, todos los empleados deben:

- Cumplir con la Política y los procedimientos relativos a la protección de datos personales.
- Participar en las formaciones obligatorias sobre protección de datos y ciberseguridad.
- Informar sin demora cualquier sospecha de vulneración o uso indebido de datos personales.
- Tratar los datos personales de manera responsable y conforme a los principios de seguridad.

3.10. Proveedores externos y terceros

En materia de protección de datos personales, todos los proveedores externos y terceros deben:

- Tratar los datos personales exclusivamente conforme a las instrucciones de FutureLife.
- Cumplir con todas las obligaciones contractuales en materia de protección de datos.
- Implementar y mantener medidas técnicas y organizativas adecuadas.
- Suscribir y respetar acuerdos de confidencialidad y acuerdos de tratamiento de datos (DPA).
- Colaborar en la realización de auditorías, controles y evaluaciones de conformidad.

4. GESTIÓN DE DATOS PERSONALES

Algunos servicios pueden utilizarse sin necesidad de proporcionar datos personales. Sin embargo, para acceder a funciones como el registro, la suscripción a boletines o la comunicación personalizada, es indispensable facilitar datos personales.

Los datos personales pueden recopilarse:

- Directamente, por ejemplo, mediante formularios, llamadas o correos electrónicos.
- Indirectamente, a través de cookies y otras tecnologías de seguimiento.

Los campos obligatorios están marcados con un asterisco (*); sin su cumplimentación no es posible prestar el servicio. La información detallada sobre las categorías de datos personales, los fines de su tratamiento y los plazos de conservación se encuentra disponible en el **Anexo A: Categorías de datos personales y fines del tratamiento**.

4.1. SEGURIDAD

La seguridad y la confidencialidad de los datos personales en el Grupo FutureLife se garantizan mediante un conjunto de medidas técnicas y organizativas recogidas en la **Política de Ciberseguridad (FL-CS-P1)**. Estas medidas se han implementado para prevenir la pérdida, el uso indebido, el acceso no autorizado o cualquier otro tratamiento ilícito de datos personales, en conformidad con el RGPD y la normativa nacional aplicable en materia de protección de datos.

El titular de los datos también es responsable de proteger su información personal y debe actuar con cautela al compartir contenido. El Grupo FutureLife no supervisa el contenido ni la información que el titular decida compartir con terceros y no asume responsabilidad por las consecuencias derivadas de dicho intercambio.

4.2. COOKIES

Gran parte de la información mencionada en esta Política de Protección de Datos Personales se recopila mediante cookies. Las cookies son pequeños archivos de texto que contienen una cantidad limitada de información y se descargan en el dispositivo del usuario —por ejemplo, ordenador, teléfono inteligente o tableta— al visitar un sitio web.

Las cookies se utilizan principalmente para recordar la configuración de la cuenta, el idioma y el país preferidos, así como para analizar el comportamiento del usuario en el sitio web y mostrar publicidad personalizada tanto en el propio sitio como en sitios de terceros.

Cuando la normativa lo exige, se solicitará el consentimiento del usuario para el uso de cookies. Para más información sobre cómo se emplean las cookies y cómo gestionarlas o desactivarlas, consulte nuestra **Política de Cookies (Cookie Policy)**.

4.3. DERECHOS DE LOS USUARIOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Los titulares de los datos cuyos datos personales se tratan pueden ejercer en cualquier momento sus derechos conforme a la normativa aplicable, incluidos los derechos de acceso, rectificación, limitación del tratamiento, supresión, oposición y portabilidad de los datos personales.

La gestión y tramitación de las solicitudes para el ejercicio de derechos corresponde a las siguientes funciones:

- **Delegado de Protección de Datos (DPO):** Responsable de la administración y verificación de todas las solicitudes de ejercicio de derechos.
- **Responsable del Departamento Jurídico:** Garantiza el cumplimiento normativo y presta apoyo en casos complejos.
- **Local Security Officer:** Coordina la implementación local de medidas de seguridad y la elaboración de informes relacionados con las solicitudes.
- **Departamento de Recursos Humanos:** Atiende las solicitudes relativas a los datos personales de los empleados.
- **Business Owner:** Responsable de la correcta gestión de solicitudes vinculadas a los sistemas bajo su control.
- **Functional Owner:** Apoya la ejecución técnica, incluida la restricción de datos cuando sea posible.

Tras recibir una solicitud válida:

- El tratamiento de los datos personales afectados debe suspenderse de inmediato.
- Los datos personales deben bloquearse durante el proceso de verificación.
- Si el sujeto de datos formula una objeción, los datos personales no podrán seguir tratándose, salvo que el responsable demuestre motivos legítimos imperiosos para continuar con el tratamiento.

Las solicitudes deben enviarse por correo electrónico a **dpo@futurelifegroup.com** con el asunto "Sujeto de protección de datos personales" e indicando claramente el derecho que se desea ejercer.

Los sujetos de datos también tienen derecho a presentar una reclamación ante la autoridad de control competente si consideran que sus datos personales se están tratando en contravención de la normativa aplicable.

4.4. Tipos y Actividades de Tratamiento de Datos Personales

En el siguiente listado se indican los principales tipos y actividades de tratamiento de datos personales realizados en el Grupo FutureLife. Todas estas actividades se llevan a cabo en conformidad con el RGPD y la normativa nacional aplicable en materia de protección de datos:

- **Gestión de datos de pacientes:** recopilación, almacenamiento y tratamiento de datos personales y datos de salud con el fin de prestar servicios sanitarios, mantener historiales médicos y cumplir con obligaciones legales.
- **Planificación de citas:** tratamiento de datos de contacto e identificación para gestionar reservas, programar visitas y garantizar la comunicación con los pacientes.
- **Comunicación y atención al cliente:** tratamiento de datos personales para responder consultas, proporcionar asistencia y compartir información solicitada.
- **Comunicaciones comerciales y de marketing:** tratamiento de datos de contacto para el envío de boletines informativos (*newsletters*), material promocional y encuestas de satisfacción — siempre basándose en un consentimiento válido cuando sea legalmente exigido.
- **Seguimiento de sitios web y cookies:** recopilación de datos mediante cookies y tecnologías similares con el fin de analizar el uso del sitio web y personalizar el contenido.
- **Reclutamiento y gestión de recursos humanos:** tratamiento de datos personales de candidatos y empleados para procesos de selección, incorporación, cálculo de nóminas, evaluación del desempeño y demás procedimientos de Recursos Humanos.

- **Cumplimiento de obligaciones legales y regulatorias:** tratamiento de datos necesarios para cumplir obligaciones legales, incluyendo archivo, auditorías y notificaciones obligatorias a autoridades públicas.
- **Seguros y facturación:** intercambio de datos pertinentes con aseguradoras y entidades de facturación para gestionar siniestros y procesar pagos.
- **Operación y seguridad informática:** utilización de datos personales en registros del sistema, gestión de accesos, cifrado, monitorización y gestión de incidentes de seguridad.
- **Investigación y análisis estadístico:** uso de datos anonimizados o seudonimizados para investigación científica y fines estadísticos internos.
- **Gestión de derechos de los interesados:** tratamiento de datos personales para atender solicitudes de acceso, rectificación, supresión y demás derechos derivados del RGPD.
- **Gestión de proveedores y prestadores de servicios:** intercambio de datos personales con socios externos y proveedores en virtud de compromisos contractuales y garantías.
- **Transferencias transfronterizas de datos:** transmisión de datos personales a entidades situadas fuera del Espacio Económico Europeo (EEE), únicamente con garantías adecuadas y conforme a los mecanismos jurídicos aplicables.

4.5. Registro de datos personales

El Registro de Datos Personales constituye el inventario central de todas las actividades de tratamiento de datos personales realizadas dentro del Grupo FutureLife. Garantiza la transparencia, la responsabilidad y el cumplimiento del RGPD. Este registro documenta la gestión legal, segura y ética de los datos personales, incluidos aquellos que son sensibles o pertenecen a categorías especiales.

4.5.1. Alcance

En el Registro de Datos Personales se incluyen todas las categorías de datos tratados por el Grupo FutureLife, entre otras:

- Documentación clínica del paciente y su pareja.
- Datos personales genéticos, biométricos y de laboratorio.
- Información sobre salud reproductiva y tratamientos.
- Datos administrativos, financieros y de seguros.
- Información sobre empleados y proveedores.
- Datos tratados a través de terceros (por ejemplo, laboratorios, almacenes o proveedores de TI).

4.5.2. Responsabilidad

- El Data Protection Officer (DPO) es responsable de la gestión, control y actualización del Registro de Datos Personales.
- Las partes implicadas deben informar al DPO sobre cualquier actividad de tratamiento nueva o modificada.
- El DPO garantiza que el Registro de Datos Personales sea exacto, completo y actualizado, y que esté disponible para revisión por la autoridad competente en materia de protección de datos (Data Protection Authority, DPA) cuando se solicite.

4.5.3. Contenido

Para cada actividad de tratamiento se registrará la siguiente información:

- **Datos del responsable:** nombre, dirección y datos de contacto de la clínica.
- **Propósito del tratamiento:** prestación de atención clínica, diagnóstico, investigación (cuando sea relevante), facturación o actividades administrativas.
- **Categorías de interesados:** pacientes, parejas, donantes, niños nacidos como resultado del tratamiento, empleados y proveedores.
- **Categorías de datos personales:** datos identificativos, datos de contacto, historial clínico, información sobre salud reproductiva, datos genéticos, resultados de pruebas de laboratorio, datos de facturación y seguros.
- **Categorías especiales de datos personales:** datos explícitamente designados, en particular información sobre salud genética y reproductiva.
- **Destinatarios de los datos personales:** equipos internos, laboratorios, hospitales, proveedores de almacenamiento, aseguradoras y autoridades reguladoras.
- **Transferencias a terceros países:** información sobre posibles transferencias de datos personales fuera del EEE, incluyendo descripción de las garantías jurídicas y de seguridad implementadas (véase el apartado 4.8 Transferencias de datos).
- **Plazos de conservación:** períodos definidos conforme a requisitos médicos, legales y regulatorios (véase el apartado 4.9 Plazos de conservación).
- **Medidas de seguridad:** medidas adoptadas (por ejemplo, cifrado, seudonimización o control de acceso).

4.5.4. Conexión con el Registro de Incidentes

El Registro de Datos Personales está vinculado al proceso de gestión de violaciones de seguridad de datos personales. Para cada incidente registrado debe constar la actividad de tratamiento correspondiente, a fin de garantizar responsabilidad, trazabilidad y transparencia conforme a los requisitos del **RGPD**.

4.5.5. Revisiones y actualizaciones

El Registro de Datos Personales se revisa al menos una vez al año o siempre que se produzcan cambios significativos en las actividades de tratamiento de datos personales. Las actualizaciones del registro son obligatorias, especialmente en los siguientes casos:

- Se introducen nuevos procedimientos médicos, tecnologías o métodos diagnósticos.
- Se incorporan nuevos encargados del tratamiento o proveedores de servicios externos.
- Se producen cambios en los requisitos legales o regulatorios relativos a la protección de datos personales.

4.6. Gestión del consentimiento del paciente

Dada la naturaleza altamente sensible de los datos tratados sobre salud reproductiva y datos sanitarios, el Grupo FutureLife obtiene, registra y respeta los consentimientos de los pacientes:

- **Recopilación del consentimiento**
  - El consentimiento se obtiene en los casos previstos por la ley, especialmente para el tratamiento de datos pertenecientes a categorías especiales de datos personales (por ejemplo, datos sobre fertilidad, datos genéticos y médicos) y para cualquier uso secundario de los datos.

- El consentimiento se obtiene mediante un formulario de consentimiento del paciente que explica claramente el propósito del tratamiento, el alcance de los datos y los derechos del paciente.
- El consentimiento es siempre voluntario, específico, informado e inequívoco.

> **Gestión del consentimiento**

- Las preferencias y el estado del consentimiento se almacenan de forma segura.
- Solo el personal autorizado tiene acceso a la información sobre el consentimiento y la posibilidad de actualizarla.
- Cuando el tratamiento o la participación en investigación requiera un consentimiento prolongado, se ofrecerán regularmente oportunidades para confirmar o actualizar dicho consentimiento.

> **Revocación del consentimiento**

- El paciente puede revocar su consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento realizado antes de la revocación.
- La revocación del consentimiento no afecta la calidad ni el alcance de la atención prestada.
- Las solicitudes de revocación o modificación del consentimiento se gestionan sin demora indebida.

> **Registro y mantenimiento de evidencia**

- Se mantiene un registro completo sobre cuándo, cómo y para qué finalidad se otorgó el consentimiento (por ejemplo, registros electrónicos de auditoría o formularios firmados).
- Estos registros se conservan de forma segura durante el período establecido por la normativa aplicable.
- En caso de revocación del consentimiento, los registros se actualizan en consecuencia y los datos correspondientes se bloquean o se interrumpe su tratamiento.

4.7. Compartición de Datos Personales

FutureLife ha implementado medidas de protección para los casos en que sea necesario compartir datos personales con terceros o proveedores externos de servicios:

> **Aseguradoras y entidades de seguros mutuos (incluidas terceras partes en casos de seguro de responsabilidad civil):**

- Los datos personales pueden compartirse para verificar la cobertura del seguro y gestionar el pago de gastos sanitarios.
- Solo se comparten los datos estrictamente necesarios; no se facilitan datos médicos ni datos sanitarios sensibles, salvo que lo exija la ley.
- Si la aseguradora se encuentra fuera del EEE en un país sin un nivel equivalente de protección de datos:
  - Para la tramitación de reclamaciones puede ser necesario transferir datos personales.
  - La transferencia solo se realiza con el consentimiento informado y explícito del paciente.

- Se transfiere únicamente la cantidad mínima de datos necesaria.
- En caso de denegación del consentimiento, la aseguradora puede rechazar la cobertura, y el paciente asumiría los costes íntegros.

> **Sociedades filiales del Grupo FutureLife:**

- Pueden compartirse los datos personales mínimos necesarios entre clínicas del Grupo FutureLife para garantizar la continuidad y calidad de la atención.

> **Proveedores externos y prestadores de servicios:**

- Los datos personales pueden compartirse con socios que prestan servicios en áreas como atención sanitaria, diagnóstico, análisis de laboratorio, auditoría, seguridad, soporte de TI, asesoría jurídica y actividades administrativas.
- Los proveedores también pueden gestionar y mantener plataformas digitales o aplicaciones utilizadas por el Grupo FutureLife.
- Los datos se comparten únicamente en la medida necesaria para la prestación de los servicios contratados.

> **Representantes legales, asesores y autoridades reguladoras:**

- Los datos personales pueden compartirse para ejercer derechos del Grupo FutureLife, resolver reclamaciones, colaborar con autoridades o recibir asesoramiento jurídico.
- Los destinatarios pueden operar dentro o fuera del EEE; en caso de transferencia fuera del EEE se aplican garantías adecuadas, especialmente mediante Standard Contractual Clauses (SCCs).
- Todos los destinatarios de datos personales están obligados a proteger su confidencialidad, integridad y seguridad conforme al RGPD.

4.8. TRANSFERENCIAS DE DATOS PERSONALES

Según el Reglamento General de Protección de Datos (RGPD), los datos relativos a la atención sanitaria y a la salud reproductiva pueden fluir libremente dentro de la UE y el Espacio Económico Europeo (EEE), siempre que se traten bajo garantías adecuadas. Cualquier uso secundario de los datos —por ejemplo, con fines de investigación o registros sanitarios— requiere el consentimiento expreso del paciente y una protección sólida. El Espacio Europeo de Datos de Salud (EEDS), a partir de 2025, reforzará los derechos transfronterizos de los pacientes y establecerá nuevas normas para el uso secundario de datos sanitarios sensibles.

4.8.1. FLUJO DE DATOS PERSONALES Y CUMPLIMIENTO NORMATIVO

La transferencia de datos personales dentro de la UE/EEE no está sujeta a restricciones adicionales por motivos de protección de datos; por tanto, no se requieren las Standard Contractual Clauses (SCCs) ni evaluaciones de adecuación. No obstante, en cualquier transmisión de datos es imprescindible garantizar el pleno cumplimiento del RGPD y de las políticas internas de la organización:

> **Minimización de datos:** compartir únicamente la información estrictamente necesaria para el propósito definido.
> **Limitación de finalidad:** Los datos personales solo pueden tratarse con fines sanitarios claramente definidos y legítimos.

- **Integridad y confidencialidad:** Los datos deben protegerse contra accesos no autorizados, alteraciones, pérdidas o destrucciones.
- **Transparencia:** Los pacientes deben ser informados de manera clara cuando sus datos se compartan fuera de la UE/EEE.
- **Derechos del interesado:** Debe garantizarse el ejercicio de todos los derechos, incluidos el acceso, la rectificación, la limitación del tratamiento o la supresión.
- **Seguridad:** cifrado, control de accesos, registros de auditoría.

4.8.2. Uso Secundario de Datos Reproductivos

Cuando los datos se utilicen fuera del contexto de la atención directa, se aplican normas significativamente más estrictas. El uso secundario de datos reproductivos de pacientes (por ejemplo, investigación, mejora de la calidad, formación, registros, desarrollo de productos, marketing) requiere:

- **Consentimiento expreso:** Los datos solo se tratarán si el paciente ha otorgado su consentimiento explícito.
- **Garantías:** Seudonimización o anonimización.
- **Transparencia:** Los pacientes deben conocer qué investigación se apoya en sus datos personales y tener la posibilidad de revocar su consentimiento en cualquier momento.

4.8.3. Transferencias Internacionales de Datos Personales

La transferencia de datos sanitarios o relativos a la fertilidad fuera de la UE/EEE se realizará únicamente en conformidad con el RGPD. Si la Comisión Europea ha emitido una decisión de adecuación, los datos podrán transferirse a dichos países (por ejemplo, Suiza, Japón). Para otros destinos se aplican Standard Contractual Clauses (SCC) y se realizan evaluaciones de riesgos conforme a los requisitos derivados de la sentencia Schrems II. En situaciones excepcionales y específicas pueden aplicarse derogaciones, como el consentimiento expreso para una prueba de laboratorio puntual en el extranjero.

4.9. Plazos de Conservación

Los datos personales se conservan durante el tiempo estrictamente necesario para cumplir la finalidad para la que fueron recopilados, conforme al principio de limitación del plazo establecido por el RGPD. En algunos casos, los datos personales pueden tratarse incluso después de cumplida la finalidad original, por ejemplo, si el interesado se convierte en cliente.

Los plazos de conservación se establecen como sigue:

- **Documentación clínica:** Se conserva durante el período previsto por la normativa aplicable, normalmente 10 años desde la finalización del tratamiento o el alta, conforme a la legislación sanitaria.
- **Datos genéticos:** Según la normativa vigente, deben conservarse durante al menos 30 años desde la finalización del tratamiento o el alta.
- **Datos para fines legales y administrativos:** Tras el período inicial, pueden conservarse hasta 3 años, lo que corresponde al plazo legal de prescripción, para garantizar la protección jurídica y el cumplimiento normativo.
- **Datos para fines de investigación:** Pueden conservarse en forma anonimizada durante la duración del proyecto de investigación, normalmente entre 5 y 10 años, conforme a la normativa aplicable. Los datos pueden compartirse con instituciones de investigación acreditadas para fines legítimos.

- **Datos relacionados con consultas, reclamaciones o solicitudes de ejercicio de derechos:** Se conservan durante el tiempo necesario para gestionar la solicitud, normalmente entre 1 y 2 años, y pueden conservarse más tiempo si es necesario por motivos legales o regulatorios o para proteger intereses legítimos del responsable en caso de litigios.
- **Datos relacionados con relaciones contractuales:** Se conservan durante la vigencia del contrato y posteriormente durante 5 años tras su finalización, para la gestión de posibles reclamaciones o litigios.
- **Datos de suscripción a newsletters:** Se conservan hasta la revocación del consentimiento o la cancelación de la suscripción.

4.10. Eliminación de datos personales

La seguridad de los procedimientos de eliminación de datos personales en el marco del tratamiento se garantiza mediante medidas técnicas y organizativas adecuadas. El Grupo FutureLife implementa métodos documentados, verificables y seguros para la eliminación de datos personales, en conformidad con el Reglamento General de Protección de Datos (RGPD) y el Reglamento sobre Sustancias de Origen Humano (SoHO).

4.10.1. Derecho de Supresión

Los interesados tienen derecho a solicitar la supresión de sus datos personales sin demora indebida. Esto incluye situaciones en las que los datos personales ya no son necesarios para su finalidad original, se ha revocado el consentimiento o los datos se han tratado de forma ilícita.

4.10.2. Limitaciones en el Contexto de la Atención Sanitaria

El derecho de supresión en el ámbito sanitario está limitado por obligaciones legales de conservación y/o excepciones por motivos de salud pública o investigación. Según el RGPD, los datos relativos a la atención sanitaria y la fertilidad pertenecen a categorías especiales de datos (a veces denominados “datos sensibles”). Por ello, su tratamiento requiere consentimiento expreso u otra base jurídica, junto con garantías adicionales. El Reglamento de la UE sobre Sustancias de Origen Humano exige trazabilidad a largo plazo (códigos únicos no identificativos, como el Código Europeo Único) para materiales reproductivos como gametos y embriones, normalmente hasta 30 años. Por tanto, las clínicas pueden no estar en condiciones de eliminar determinados registros sanitarios incluso a petición del interesado.

4.10.3. TÉCNICAS DE ELIMINACIÓN SEGURA

Todas las actividades relacionadas con la eliminación de datos personales deben registrarse y ser verificables.

- **Datos digitales**
  - **Eliminación criptográfica:** destrucción de claves de cifrado para hacer los datos ilegibles.
  - **Sobrescritura (data wiping):** uso de herramientas certificadas para sobrescribir el almacenamiento con patrones aleatorios.
  - **Herramientas certificadas de borrado:** utilización de software aprobado en la UE para la eliminación segura de datos.
- **Copias de seguridad y archivos**
  - **Planes de retención:** garantizan la eliminación automática o sobrescritura de datos respaldados una vez expirado el plazo de conservación.
  - **Segregación de funciones:** solo personal autorizado puede eliminar datos sensibles.
  - **Registro inmutable:** asegura la trazabilidad de las eliminaciones incluso en copias de seguridad.
- **Soporte físico y papel:** trituración, desfibrado o incineración, o bien trituración mecánica para la destrucción física del soporte.

4.10.4. DOCUMENTACIÓN Y AUDITORÍAS

Todos los procedimientos de eliminación de datos personales deben documentarse. Esto incluye la definición de plazos de conservación, desencadenantes de eliminación y las excepciones. Se requieren auditorías periódicas para verificar el cumplimiento del RGPD y de las obligaciones relacionadas con las sustancias de origen humano. Todas las operaciones de eliminación deben mantener trazabilidad mediante registros de auditoría.

4.11. NOTIFICACIÓN A LAS AUTORIDADES DE PROTECCIÓN DE DATOS

En caso de violación de la seguridad de los datos personales, la autoridad de control competente debe ser informada sin demora indebida y, cuando sea posible, en un plazo máximo de 72 horas desde que el responsable tenga conocimiento del incidente. Todas las entidades del Grupo FutureLife deben cumplir los procedimientos internos de notificación de incidentes. La documentación relativa a la violación de seguridad y al proceso de notificación debe conservarse para fines de auditoría y demostración de cumplimiento.

El Data Protection Officer (DPO) es responsable de:

- Coordinar todo el proceso de notificación a la autoridad de control.
- Mantener y actualizar el Registro de Datos Personales, asegurando que los registros de actividades de tratamiento sean precisos, completos y actualizados.
- Preparar el informe sobre la violación de seguridad, que debe incluir:
  - Naturaleza y alcance de la violación.
  - Categorías y número de interesados y registros afectados.
  - Datos de contacto para acciones posteriores y comunicación adicional.
  - Consecuencias probables de la violación y medidas correctivas adoptadas o previstas.

El Local Security Officer debe:

- Garantizar la escalada oportuna del incidente desde las entidades locales al DPO.

El Jefe del Departamento Jurídico debe:

- Revisar las implicaciones legales de la violación y apoyar la comunicación con las autoridades competentes.

4.12. GESTIÓN DE RIESGOS DE TERCEROS

El Grupo FutureLife garantiza que todos los proveedores de servicios y terceros que traten datos personales en nombre de las sociedades del Grupo cumplan estrictos requisitos de protección de datos y seguridad de la información, en conformidad con las políticas internas y la normativa de FutureLife. El Grupo mantiene un Vendor Risk Register y se rige por el Supplier Cybersecurity Standard (FL-CS-S2).

4.12.1. EVALUACIÓN PREVIA AL INICIO DE LA COLABORACIÓN

- Todas las terceras partes deben completar un cuestionario sobre protección de datos y seguridad de la información.
- Se realiza una evaluación de riesgos para valorar prácticas de tratamiento de datos, certificaciones (por ejemplo, ISO 27001) y cumplimiento normativo interno.
- Los Acuerdos de Tratamiento de Datos (DPA) deben firmarse antes de compartir cualquier dato personal.

4.12.2. MONITORIZACIÓN

- Se realizan auditorías o evaluaciones anuales para proveedores de alto riesgo.
- Se revisa el historial de violaciones de seguridad, la capacidad de respuesta ante incidentes y el uso de subcontratistas.
- Las terceras partes deben informar al Grupo FutureLife sobre cualquier violación de seguridad de datos personales o cambios significativos en las actividades de tratamiento.

4.13. MAPAS Y ESQUEMAS PARA EL TRATAMIENTO DE DATOS PERSONALES

Para garantizar la claridad y el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la normativa relacionada, es necesario crear y mantener diagramas visuales y flujos de actividades de tratamiento de datos personales. Estos diagramas deben mostrar:

- El flujo de datos personales a través de sistemas y departamentos.
- Los puntos de recopilación, almacenamiento y transmisión de datos personales.
- Las interfaces con encargados externos del tratamiento (terceros).
- La ubicación de los repositorios de datos personales (incluidos servicios en la nube y transferencias transfronterizas).

Estos mapas de datos deben utilizarse para los siguientes fines:

- Identificación de riesgos y deficiencias en la protección de datos personales.
- Apoyo en la realización de evaluaciones de impacto en la protección de datos (Data Protection Impact Assessment, DPIA).
- Facilitación de auditorías internas y programas de formación.

Todos los diagramas deben ser revisados por el Data Protection Officer (DPO) al menos cada dos años o cuando se produzcan cambios significativos en las actividades de tratamiento.

4.14. Evaluación de Impacto en la Protección de Datos (EIPD)

La Evaluación de Impacto en la Protección de Datos (Data Protection Impact Assessment, DPIA) debe realizarse antes de iniciar cualquier actividad de tratamiento que probablemente implique un alto riesgo para los derechos y libertades de las personas físicas. Esto incluye, entre otros:

- Tratamiento a gran escala de categorías especiales de datos personales.
- Monitorización sistemática de espacios accesibles al público.
- Uso de nuevas tecnologías o técnicas de perfilado.

Cada evaluación de impacto debe incluir:

- Descripción del tratamiento y su finalidad.
- Evaluación de la necesidad y proporcionalidad del tratamiento en relación con los fines.
- Identificación de riesgos para los derechos y libertades de los interesados.
- Medidas para mitigar los riesgos identificados.

El DPO debe documentar y conservar las Evaluaciones de Impacto en la Protección de Datos. En los casos en que lo exija el RGPD, es necesario iniciar una consulta con la autoridad de control antes de comenzar el tratamiento.

4.15. Formación y Concienciación de Empleados

Todo el personal con acceso a datos personales, incluidos datos de salud y de salud reproductiva y fertilidad, recibe formación anual obligatoria sobre el RGPD, el Espacio Europeo de Datos de Salud (EEDS) y ciberseguridad, con módulos dedicados para técnicos de laboratorio (manejo seguro de datos de donantes y embrionarios), clínicos (principios de gestión de la confidencialidad y el consentimiento) y personal informático (seguridad de sistemas de información y controles de acceso). Para fomentar la concienciación, las clínicas realizan simulaciones de phishing y campañas de higiene cibernética, y se supervisa el progreso y la finalización de la formación para garantizar el cumplimiento y la privacidad continuos (incluyendo categorías especiales de datos personales relacionados con la fertilidad y los donantes).

4.16. Revisión y Gestión de la Política de Protección de Datos Personales

La Política de Protección de Datos Personales del Grupo FutureLife debe revisarse al menos una vez al año o inmediatamente tras cualquier cambio significativo en los requisitos regulatorios. El proceso de revisión lo coordina el DPO en colaboración con el Head of Legal, el Cybersecurity Manager y el Chief Transformation Officer.

La dirección de las clínicas y los asesores legales locales son responsables de verificar la aplicabilidad de la política a nivel de filiales y garantizar el cumplimiento de la normativa local. Todas las actualizaciones deben documentarse en la tabla de control de versiones y comunicarse a las partes interesadas. El resumen de cambios debe incluirse en el aviso de actualización de la Política.

4.17. Disponibilidad de la Política

El Grupo FutureLife se compromete a garantizar que esta Política de Protección de Datos Personales sea accesible para todas las personas físicas. Las solicitudes para obtenerla en formatos alternativos pueden dirigirse al DPO.

Medidas de accesibilidad:

- La Política está disponible en todas las ubicaciones donde opera el Grupo FutureLife.
- Los formatos accesibles (por ejemplo, letra grande, archivos PDF compatibles con lectores de pantalla) están disponibles previa solicitud.
- Las clínicas exhiben copias impresas en las recepciones y proporcionan acceso digital a través de sitios web y/o portales para pacientes.
- El personal está capacitado para ayudar a los pacientes a comprender la Política y ejercer sus derechos.

4.18. Actualización de la Política de Protección de Datos Personales

El Grupo FutureLife se reserva el derecho de modificar, actualizar o sustituir esta Política de Protección de Datos Personales en cualquier momento y a su discreción. La continuación del uso de los servicios tras cualquier modificación se considerará como aceptación de la versión actualizada de esta Política.

Se recomienda a los interesados (usuarios) revisar periódicamente esta Política para mantenerse informados sobre posibles cambios. Si el interesado no está de acuerdo con este documento, en todo o en parte, o con cualquier modificación posterior, deberá dejar de utilizar los servicios de inmediato.

4.19. Anexo de Privacidad de Datos (DPA)

El Data Privacy Annex (DPA) es una parte obligatoria del marco de protección de datos del Grupo FutureLife. Actúa como documento formal que define los requisitos específicos de privacidad y protección de datos aplicables a cada aplicación, sistema o servicio que trata datos personales, garantizando transparencia, responsabilidad y coherencia en la gestión de datos personales dentro del Grupo FutureLife.

El objetivo del DPA es asegurar que todas las actividades de tratamiento estén claramente definidas y se realicen en conformidad con la normativa aplicable en materia de protección de datos (como el RGPD) y con los estándares internos del Grupo FutureLife. El DPA debe incluir detalles sobre:

- Categorías de datos personales tratados.
- Base jurídica para el tratamiento.
- Plazo de conservación de los datos personales.
- Medidas de seguridad implementadas.
- Roles y responsabilidades de las partes implicadas.
- Cualquier transferencia de datos personales fuera de la UE/EEE, si es relevante para la actividad de tratamiento.

4.20. Violación de Seguridad de Datos – Notificación a Personas Físicas

Además de la notificación a las autoridades de control, el Grupo FutureLife se compromete a informar sin demora indebida a las personas afectadas (interesados) en caso de violación de la seguridad de datos personales, cuando sea probable que dicha violación implique un alto riesgo para sus derechos y libertades.

4.20.1. Condiciones para la notificación

- La violación de seguridad afecta a categorías especiales de datos personales, especialmente datos de salud, fertilidad o datos genéticos.
- La violación puede dar lugar a robo de identidad, discriminación, daño reputacional u otras consecuencias graves para el interesado.

4.20.2. Métodos y Plazos para Informar a los Interesados

- Las personas afectadas serán informadas sin demora indebida y, cuando sea posible, en un plazo máximo de 72 horas desde la confirmación de la violación, mediante correo electrónico, teléfono o portal seguro para pacientes.
- La notificación incluirá una descripción de la naturaleza de la violación, las consecuencias probables, las medidas adoptadas o previstas para mitigar sus efectos y los datos de contacto para obtener más información.
- Cuando no sea posible la comunicación directa con los interesados, se publicarán avisos en el sitio web de la clínica o a través de otros canales adecuados.

4.21. Uso de Inteligencia Artificial y Toma de Decisiones Automatizada

El Grupo FutureLife puede utilizar herramientas de Inteligencia Artificial (IA) y procesos de toma de decisiones automatizadas para apoyar los procesos clínicos y operativos. Estas herramientas se emplean para mejorar la precisión, eficiencia y calidad de la atención prestada. No se adoptan decisiones con impacto legal o médico significativo exclusivamente mediante tratamiento automatizado: todas dichas decisiones están sujetas a supervisión humana y revisión clínica.

Cada sistema que utilice datos personales e incorpore modelos de IA debe cumplir con:

- Desarrollo interno o externo de IA:
  - **FL-CS-OP09 New System Security Requirements.**
  - **FL-CS-S7 AI Security Standard.**
  - Evaluación específica del impacto en el negocio (Business Impact Assessment, BIA).
- Sistemas adquiridos e implementados interna o externamente:
  - **FL-CS-OP-03 Secure System Development Lifecycle.**

Ejemplos de herramientas y procesos automatizados:

- Clasificación y selección de embriones.
- Algoritmos de emparejamiento de donantes y receptores.
- Análisis genético de riesgos.
- Modelos predictivos de resultados de tratamiento.
- Clasificación automatizada y planificación de citas.

Derechos de los pacientes:

- Ser informados sobre el uso de IA en su atención.
- Expresar su opinión sobre dicho tratamiento.
- Solicitar la intervención humana en la decisión.
- Impugnar decisiones adoptadas exclusivamente mediante tratamiento automatizado.

Cuando sea relevante, se realizará una EIPD para evaluar los riesgos asociados al tratamiento de datos personales y garantizar el cumplimiento del RGPD, especialmente del artículo 22 y disposiciones relacionadas.

4.22. Protección de Datos de Donantes y Niños Concebidos mediante Donación

El Grupo FutureLife cumple con el marco regulatorio de la UE sobre Sustancias de Origen Humano (Substances of Human Origin, SoHO) para garantizar los más altos estándares de seguridad, trazabilidad y protección de datos personales en el tratamiento de información relativa a donantes y niños concebidos mediante donación. Estas normas están diseñadas para asegurar la trazabilidad a largo plazo y la protección de la salud pública, preservando al mismo tiempo la anonimidad de los donantes, la confidencialidad de los pacientes y la privacidad de los niños concebidos mediante donación.

4.22.1. Codificación única y trazabilidad

Todo material procedente de donantes se identifica con un código único no identificativo (por ejemplo, el Código Europeo Único – Single European Code), que permite la trazabilidad completa desde la donación hasta el uso clínico, manteniendo la anonimidad tanto del donante como del paciente. Cualquier dato directamente identificativo se conserva de forma separada y segura, con acceso restringido únicamente a personal autorizado y solo para fines permitidos por la normativa. La separación entre código e identidad garantiza el cumplimiento regulatorio, facilita el seguimiento de calidad y seguridad y protege la confidencialidad de donantes y receptores.

4.22.2. Eventos y Reacciones Adversas Graves

Se mantienen procedimientos formales para la identificación, documentación y notificación de Serious Adverse Events (SAE) y Serious Adverse Reactions (SAR), en conformidad con la normativa de la UE y los requisitos regulatorios nacionales. Todos los incidentes se registran, investigan y, cuando lo exige la ley, se notifican a las autoridades competentes dentro de los plazos establecidos. Los pacientes y donantes son informados sin demora cuando el evento o reacción sea relevante para su atención, seguridad o tratamiento en curso.

4.22.3. Derecho a la Limitación del Tratamiento y Acceso a los Datos Personales

Según el RGPD, los pacientes y donantes tienen derecho a limitar el tratamiento de sus datos personales y reproductivos. Dado que los datos sobre fertilidad y reproducción constituyen categorías especiales de datos personales, las personas físicas (interesados) gozan de derechos ampliados, especialmente en lo relativo al consentimiento expreso para su tratamiento y la posibilidad de revocarlo en cualquier momento.

Medidas técnicas y organizativas implementadas por la clínica para garantizar la limitación del tratamiento y el acceso incluyen:

- **Control de acceso basado en roles (Role-Based Access Control - RBAC):** Garantiza que solo las personas autorizadas puedan consultar los registros sensibles.
- **Separación de registros entre donantes y receptores:** Evita la vinculación no deseada o no autorizada de datos.
- **Registro completo de accesos:** Permite monitorizar y auditar todos los accesos a datos de reproducción.

4.22.4. Anonimato del Donante vs. Derechos de Pacientes y Niños

En algunos Estados miembros de la UE, la normativa nacional otorga a los niños concebidos mediante donación el derecho a acceder a datos identificativos del donante al alcanzar la mayoría de edad. En tales casos, cuando sea legalmente posible, el Grupo FutureLife cumple con las obligaciones legales, manteniendo los más altos estándares de seguridad y minimización de datos personales.

4.22.5. Minimización del riesgo genético

La minimización del riesgo genético constituye una obligación esencial conforme al Reglamento de la UE sobre Sustancias de Origen Humano (que establece requisitos de calidad y seguridad), al RGPD (que regula el tratamiento de datos genéticos) y a la normativa nacional en materia sanitaria. El objetivo es reducir la probabilidad de transmisión de enfermedades hereditarias o anomalías genéticas desde gametos donados (espermatozoides/óvulos) o embriones al receptor y a sus futuros hijos.

Elementos clave para la minimización del riesgo genético:

- **Salud e antecedentes familiares**
  - Los donantes rellenan cuestionarios detallados sobre su historial de salud familiar (normalmente de 2-3 generaciones).
  - En particular, se monitorizan enfermedades del sistema cardiovascular, síndromes tumorales, enfermedades neurológicas, trastornos metabólicos y defectos congénitos del desarrollo.
- **Examen físico**
  - Examen clínico para descartar factores de riesgo evidentes (por ejemplo, anomalías del desarrollo).
- **Pruebas de laboratorio**
  - El cribado estándar para enfermedades infecciosas (VIH, VHB, VHC, sífilis, CMV).
  - Cribado de portadores de enfermedades genéticas (por ejemplo, fibrosis quística, talasemia, enfermedad de Tay-Sachs, SMA).
  - Análisis cromosómico (cariotipado), si es necesario.
- **Asesoramiento genético**
  - Si se identifican factores de riesgo, se ofrece a los donantes y, si procede, a futuros padres, asesoramiento genético profesional.
  - El asesoramiento ayuda a evaluar los riesgos residuales e informa la elegibilidad de los donantes a la hora de tomar decisiones.
- **Criterios de exclusión de donantes**
  - Los donantes con enfermedades hereditarias conocidas o con alto riesgo de portar enfermedades genéticas graves quedan excluidos del programa de donación.
  - En algunas jurisdicciones, la ley puede permitir excepciones basadas en el consentimiento informado explícito del destinatario, pero estos casos son excepcionales.
- **Historia clínica y familiar:**
  - Los donantes completan cuestionarios detallados sobre antecedentes familiares (normalmente de 2–3 generaciones).

- Se evalúan enfermedades cardiovasculares, síndromes tumorales, trastornos neurológicos, enfermedades metabólicas y malformaciones congénitas.

> **Examen físico:**

- Evaluación clínica para descartar factores de riesgo evidentes (p. ej., anomalías del desarrollo).

> **Pruebas de laboratorio:**

- Cribado estándar de enfermedades infecciosas (VIH, VHB, VHC, sífilis, CMV).
- Cribado de portadores de enfermedades genéticas (p. ej., fibrosis quística, talasemia, enfermedad de Tay-Sachs, SMA).
- Análisis cromosómico (cariotipo), cuando se requiera.

> **Asesoramiento genético:**

- Si se identifican factores de riesgo, se ofrece asesoramiento especializado a donantes y, en su caso, a futuros padres.
- El asesoramiento ayuda a evaluar los riesgos residuales y a tomar decisiones sobre la idoneidad del donante.

> **Criterios de exclusión del donante:**

- Donantes con enfermedades hereditarias conocidas o alto riesgo de ser portadores de patologías genéticas graves son excluidos del programa.
- En algunas jurisdicciones, la normativa puede permitir excepciones basadas en el consentimiento informado del receptor, aunque estos casos son excepcionales.

4.23. Datos de Menores y Consentimiento Parental

Los servicios y actividades comerciales del Grupo FutureLife no están dirigidos a menores y no se recopilan ni tratan intencionadamente datos personales de menores. Los servicios del Grupo FutureLife están destinados exclusivamente a personas mayores de edad.

En los casos en que determinados servicios se dirijan expresamente a menores, será obligatorio obtener el consentimiento de los padres o tutores legales para la recopilación y tratamiento de sus datos personales, conforme a la normativa aplicable. Si el interesado es menor, debe obtenerse el consentimiento previo antes de proporcionar cualquier dato personal a una empresa del Grupo FutureLife.

4.23.1. Verificación de Edad y Documentación

Las clínicas deben verificar la edad del interesado mediante documentos oficiales antes de iniciar cualquier recopilación de datos personales o prestación de tratamiento.

Todos los formularios de consentimiento deben estar debidamente firmados, fechados y almacenados de forma segura. Los registros electrónicos de auditoría sobre la concesión y revocación del consentimiento se mantienen durante el período exigido por la normativa y las políticas internas.

4.23.2. Procedimientos para la Preservación de la Fertilidad en Menores

En determinados casos excepcionales, es posible y necesario tratar a menores. Estos casos suelen incluir la preservación de la fertilidad en niños con enfermedades graves, como patologías oncológicas.

A) Criopreservación del tejido ovárico

La criopreservación de tejido ovárico es el método principal para preservar la fertilidad en niñas prepuberales. Este procedimiento consiste en la extracción quirúrgica de tejido ovárico que contiene ovocitos inmaduros, los cuales se congelan para su uso posterior. Más adelante, si la paciente desea tener hijos, el tejido conservado puede ser reimplantado en su cuerpo; los ovocitos inmaduros también pueden madurarse en condiciones de laboratorio y utilizarse posteriormente, especialmente en procedimientos de reproducción asistida.

B) Estimulación de los ovarios y obtención de óvulos maduros

En adolescentes que ya han pasado la pubertad y han desarrollado ovocitos maduros, es posible realizar una estimulación ovárica controlada y la posterior extracción de ovocitos maduros. Los ovarios se estimulan mediante tratamiento hormonal y los ovocitos obtenidos se almacenan mediante criopreservación.

4.23.3. Aspectos médicos y legales

- **Necesidad médica:** Los procedimientos se realizan generalmente cuando el estado de salud del menor o su tratamiento puede conducir a infertilidad.
- **Consentimiento:** Se requiere siempre el consentimiento tanto del paciente (si tiene suficiente madurez para comprender la naturaleza del procedimiento) como de sus padres/tutores legales; el consentimiento debe ser informado y conforme a la normativa aplicable.
- **Investigación:** Se lleva a cabo investigación continua para encontrar nuevas opciones de preservación de la fertilidad en niños que aún no han alcanzado la pubertad.

4.23.4. Derecho a Revocar el Consentimiento

Los padres o tutores legales pueden revocar su consentimiento en cualquier momento. Tras la revocación, el tratamiento de los datos personales del menor se limitará o finalizará, salvo que la normativa aplicable exija continuar con el tratamiento.

4.23.5. Cumplimiento de la normativa nacional

El Grupo FutureLife debe garantizar el cumplimiento de la normativa nacional en cada país donde opera, especialmente en lo relativo a la edad mínima para recibir tratamiento médico y la elegibilidad para tratamientos de fertilidad.

5. CUMPLIMIENTO CON OTRAS NORMATIVAS

5.1. REGLAMENTO DE CIBERRESILIENCIA (CRA)

El Reglamento de Ciberresiliencia (Cyber Resilience Act, CRA), que entró en vigor en 2024 y cuyas obligaciones principales serán plenamente aplicables a partir de diciembre de 2027, establece requisitos de ciberseguridad para los Productos con Elementos Digitales (Products with Digital Elements, PDE), incluyendo hardware y software comercializados en la Unión Europea. Los fabricantes, importadores y distribuidores de estos productos tendrán obligaciones en materia de ciberseguridad, incluyendo la realización de evaluaciones de riesgos y la documentación de los esfuerzos de cumplimiento.

El Grupo FutureLife debe prepararse para cumplir con los requisitos del CRA mediante:

- Identificación de todos los productos con elementos digitales (PDE), como sistemas de Historias Clínicas Electrónicas (Electronic Health Records, EHR) y herramientas basadas en inteligencia artificial.
- Garantizar el principio de security by design (seguridad desde el diseño).
- Implementación de procedimientos formalizados para la gestión de vulnerabilidades (vulnerability handling).
- Coordinación del proceso de certificación CRA a través del Gerente de Ciberseguridad.

5.2. ESPACIO EUROPEO DE DATOS DE SALUD (EEDS)

El Grupo FutureLife debe comprometerse a implementar el Espacio Europeo de Datos de Salud (European Health Data Space, EHDS), un marco regulatorio que entrará en vigor en 2025 y cuyo objetivo es facilitar el acceso seguro y eficiente, el intercambio y el uso de datos sanitarios, incluyendo datos sobre salud reproductiva, en todos los Estados miembros de la UE.

5.2.1. USO PRIMARIO DE DATOS SANITARIOS

FutureLife garantizará el cumplimiento de las normas del EEDS relativas al tratamiento de datos personales de salud para la atención directa al paciente, aplicando los siguientes principios:

- **Interoperabilidad:** Los sistemas deben actualizarse para soportar los estándares técnicos del EEDS en formatos de datos, protocolos de comunicación/intercambio y coherencia semántica.
- **Derechos de acceso:** Los pacientes deben poder acceder a sus datos sanitarios de forma segura y fácil, incluso a través de fronteras, incluyendo registros relacionados con reproducción y fertilidad.
- **Portabilidad de datos:** Deben desarrollarse mecanismos que permitan a los pacientes transferir sus datos sanitarios entre clínicas FutureLife y otros proveedores autorizados dentro de la UE, conforme al derecho de portabilidad previsto en el RGPD.

5.2.2. USO SECUNDARIO DE DATOS SANITARIOS

FutureLife apoya el uso secundario ético y legal de datos sanitarios para investigación, innovación y salud pública en el marco del EEDS, bajo las siguientes condiciones:

- **Consentimiento expreso:** El uso secundario de datos sobre fertilidad y datos genéticos requiere consentimiento informado, documentado y explícito del interesado, salvo que exista otra base legal conforme al RGPD y al EEDS.

- **Minimización y seudonimización:** Solo se utiliza el mínimo de datos necesario y los identificadores se eliminan o seudonimizan para garantizar la protección de datos personales.
- **Transparencia:** Los pacientes deben ser informados claramente sobre la naturaleza, finalidad y destinatarios del uso secundario de sus datos, y deben poder revocar su consentimiento en cualquier momento. Se ofrecerán mecanismos claros y reversibles de opt-out, cuando lo permita la normativa aplicable.

5.2.3. Formato Europeo para el Intercambio de Historias Clínicas Electrónicas (EEHRXF)

El Grupo FutureLife está implementando activamente el Formato Europeo de Intercambio de Historias Electrónicas de Salud (EEHRXF). La EEHRXF es la base técnica del EEDS, que garantiza el uso principal de los datos de salud para la atención directa al paciente y garantiza la interoperabilidad entre los Estados miembros. Es un estándar que permite el intercambio de datos transfronterizo controlado por pacientes dentro del EEDS. Cubre la estructuración e intercambio de categorías clave de datos electrónicos de salud, como resúmenes de pacientes, recetas electrónicas, resultados de laboratorio, imágenes e informes médicos, informes de altas hospitalarias y datos de enfermedades raras.

5.2.4. Mecanismo de portabilidad de datos

FutureLife permitirá a los pacientes recibir y transferir sus datos sanitarios personales en un formato estructurado, de uso común y legible por máquina, conforme al derecho de portabilidad del RGPD.

Mecanismos de portabilidad:

- Los pacientes podrán solicitar sus datos mediante portales seguros o mediante solicitud escrita al DPO.
- Los datos se proporcionarán en formatos compatibles con el EEDS, como HL7 FHIR, CDA o EEHRXF XML.
- Las transferencias a otros proveedores se realizarán mediante interfaces API seguras o protocolos cifrados para la transmisión de archivos.

5.2.5. Centros Nacionales EEDS

FutureLife reconoce que cada Estado miembro debe establecer un centro nacional del EEDS para coordinar el intercambio de datos sanitarios. FutureLife se compromete a:

- Colaborar con los centros nacionales del EEDS en los países donde opera.
- Registrar conjuntos de datos elegibles en los centros nacionales para uso secundario, cuando se requiera consentimiento del paciente y aprobación regulatoria.
- Participar en programas piloto y procesos de onboarding técnico dirigidos por autoridades nacionales para probar y validar sistemas compatibles con el EEDS.

5.2.6. Intercambio Transfronterizo de Datos

- Los datos sanitarios transfronterizos solo podrán reutilizarse con fines de investigación en entornos seguros aprobados por el organismo de acceso a los datos sanitarios (Health Data Access Body, HDAB) nacional.
- Las instituciones sanitarias deben catalogar los conjuntos de datos e indicar al HDAB todos los derechos de propiedad intelectual y secretos comerciales aplicables.

- El uso secundario de datos personales para marketing o cualquier perfilado discriminatorio está estrictamente prohibido.

5.2.7. Implementación de la ciberseguridad en el EEDS

El objetivo del Espacio Europeo de Datos de Salud es permitir el intercambio transfronterizo y el uso secundario de datos sanitarios para fines de investigación, lo que implica la participación de un mayor número de entidades y un volumen más amplio de datos, aumentando así los puntos de entrada potenciales para actores malintencionados. Dada la sensibilidad de los datos sobre salud reproductiva, la implementación segura del EEDS dentro del Grupo FutureLife requiere un marco de ciberseguridad adaptativo y robusto.

Además del cumplimiento de los documentos internos, se aplicarán las siguientes medidas organizativas:

- **Prevención de violaciones de seguridad de datos personales:** Alinear los procedimientos con el **Plan de Respuesta a Incidentes de Ciberseguridad (FL-CS-OP2)** y garantizar la detección, notificación y mitigación oportunas de incidentes que afecten a la seguridad de los datos relacionados con el EEDS.
- **Implementación de sistemas HCE certificados:** Antes de su uso en intercambios transfronterizos, asegurar que todos los sistemas de Historias Clínicas Electrónicas **(Electronic Health Records, EHR)** utilizados en las clínicas estén certificados conforme al EEDS en términos de interoperabilidad, seguridad y protección de la privacidad.
- **Intercambio seguro de datos:** Utilizar canales de comunicación cifrados y API seguras para compartir datos con los centros nacionales del EEDS y la infraestructura **HealthData@EU** (nodo central que agrupa conjuntos de datos sanitarios de toda Europa).
- **Colaboración con centros nacionales del EEDS:** Cooperar activamente con las autoridades nacionales de acceso a datos sanitarios (**Health Data Access Body, HDAB**) para garantizar una integración segura y el cumplimiento de los requisitos legales.

5.2.8. Gestión y Cumplimiento Normativo

- Se establecerá la función de Coordinador del EEDS (dentro del equipo del DPO) para supervisar la implementación, colaborar con los centros nacionales del EEDS y garantizar la preparación para el cumplimiento progresivo de los requisitos.
- El Head of Legal supervisará periódicamente la evolución normativa y garantizará el cumplimiento de las disposiciones del RGPD, SoHO y EEDS.
- Todas las actividades de tratamiento relacionadas con el EEDS se documentarán en el Registro de Datos Personales y estarán sujetas a auditoría.

ANEXO A – CATEGORÍAS DE DATOS PERSONALES Y FINES DEL TRATAMIENTO

A continuación se indican las categorías de datos personales recopilados, los fines para los que se utilizan y el período durante el cual se conservan.

Tabla 1: Categorías de datos personales y fines del tratamiento

Propósito del tratamiento de datos personales	Categorías de datos personales	Base legal para el tratamiento	Responsable / Responsables conjuntos
1. Gestión de solicitudes de información, reclamaciones o sugerencias			
Las solicitudes se tratan para responder a consultas, resolver preocupaciones y atender las peticiones recibidas.	Datos de contacto: nombre, dirección de correo electrónico, número de teléfono. Datos de contenido: información incluida en la solicitud o comunicación.	Consentimiento del interesado (art. 6.1.a RGPD). Interés legítimo del responsable en el control de calidad, resolución de disputas y mejora de los servicios (art. 6.1.f RGPD).	Grupo FutureLife, junto con la clínica correspondiente del grupo a la que se dirige la solicitud.
2. Prestación de servicios sanitarios			
Los datos personales se tratan para garantizar la correcta prestación de servicios sanitarios, incluyendo la gestión de historiales clínicos y el tratamiento de datos y documentos generados en relación con la atención médica.	Datos de contacto: nombre, correo electrónico, número de teléfono, dirección postal. Datos identificativos: número de documento de identidad, número de pasaporte, sexo/género, fecha de nacimiento. Datos de imagen: fotografías, escaneos u otros documentos gráficos. Datos sanitarios y datos sobre salud reproductiva (categorías especiales de datos personales): historial clínico, informes médicos, resultados diagnósticos, información sobre tratamientos, muestras biológicas, pruebas de laboratorio, datos relacionados con la fertilidad, y otra información sanitaria relevante.	Ejecución de un contrato con el interesado (art. 6.1.b RGPD). Cumplimiento de obligaciones legales del responsable (art. 6.1.c RGPD).	Clínica FutureLife correspondiente que presta los servicios sanitarios y actúa como responsable del tratamiento (o responsable conjunto junto con el Grupo FutureLife, cuando así se determine).

Propósito del tratamiento de datos personales	Categorías de datos personales	Base legal para el tratamiento	Responsable / Responsables conjuntos
3. Gestión de Registros de Pacientes			
Los datos personales se tratan con el fin de conservar los registros médicos de los pacientes y garantizar una gestión administrativa y organizativa adecuada de los centros de salud.	- Datos de contacto: nombre, dirección de correo electrónico, número de teléfono, dirección postal, etc. – Datos de salud: historial médico, diagnósticos, tratamientos, alergias, medicamentos, signos vitales y otra información sanitaria relevante del paciente y su pareja. – Datos de identificación: número de identificación personal, número de paciente, número de pasaporte, sexo/género, fecha de nacimiento. - Datos administrativos: detalles de citas, datos de facturación, datos de seguros, formularios de consentimiento y registros de comunicación.	Ejecución de un contrato con el interesado (artículo 6(1)(b) RGPD). Cumplimiento de las obligaciones legales del responsable (artículo 6(1)(c) del RGPD). Para categorías especiales de datos personales, el tratamiento se basa en la prestación de servicios sanitarios conforme a la legislación de la UE o de los Estados miembros (artículo 9(2)(h) del RGPD).	Clínicas del Grupo FutureLife.
4. Gestión de la Relación con Donantes			
Los datos personales se tratan con el fin de crear perfiles de donantes y gestionar la relación contractual entre el donante y la clínica. Esto incluye la prestación de la atención sanitaria necesaria y el pago de una compensación acordada.	– Datos de contacto: nombre, correo electrónico, número de teléfono, dirección postal. – Datos de identificación: número de documento de identidad, número de pasaporte, sexo/género, fecha de nacimiento. – Datos de salud y genética (categorías especiales de datos personales): antecedentes de salud y familiares, resultados de pruebas, información de fertilidad, pruebas genéticas y otra información sanitaria relevante. – Datos administrativos y financieros: datos sobre la relación contractual, programación de visitas, datos de remuneración/compensación, datos de pagos y contabilidad, formularios de consentimiento y registros de comunicación.	Ejecución de un contrato con el interesado (artículo 6(1)(b) RGPD). Cumplimiento de las obligaciones legales del responsable del tratamiento (artículo 6(1)(c) del RGPD). Para categorías especiales de datos personales, el tratamiento se basa en la prestación de servicios sanitarios conforme a la legislación de la UE o de los Estados miembros (artículo 9(2)(h) del RGPD).	Clínicas del Grupo FutureLife.

Propósito del tratamiento de datos personales	Categorías de datos personales	Base legal para el tratamiento	Responsable / Responsables conjuntos
5. Derivación de Pacientes			
Los datos personales se tratan y envían a la clínica recomendada para garantizar que el tratamiento necesario pueda prestarse en un centro asistencial alternativo a petición del paciente.	– Datos de contacto: nombre, dirección de correo electrónico, número de teléfono, dirección postal. – Datos de identificación: número de documento de identidad, número de pasaporte, sexo/género, fecha de nacimiento.	Consentimiento del interesado para la transferencia de datos personales a otras clínicas del Grupo FutureLife (artículo 6(1)(a) del RGPD).	Clínicas del Grupo FutureLife.
6. Propósitos internos administrativos y gerenciales			
Los datos personales se tratan con el fin de garantizar una gestión administrativa y organizativa adecuada de las clínicas, así como para fines estadísticos internos.	– Datos de contacto: nombre, correo electrónico, número de teléfono. - Datos administrativos: detalles de reuniones, datos de facturación, datos de seguros y registros de comunicación. –Datos estadísticos internos.	El interés legítimo del responsable del tratamiento en la gestión y control de las actividades organizativas y las relaciones comerciales (artículo 6(1)(f) del RGPD).	El Grupo FutureLife junto con la clínica correspondiente del grupo implicado en la actividad de tratamiento (corresponsables del tratamiento).
7. Fines de la encuesta			
Los datos personales se tratan con el fin de enviar encuestas de calidad y satisfacción relacionadas con los servicios prestados y la atención proporcionada.	– Datos de contacto: nombre, correo electrónico, número de teléfono. –Datos estadísticos internos.	Interés legítimo en el control de calidad, la adaptación de actividades y el desarrollo de productos y servicios mejorados (Art. 6 (1) (f) RGPD).	El Grupo FutureLife junto con la clínica correspondiente del grupo al que se dirige la solicitud.

PROPÓSITO DEL TRATAMIENTO DE DATOS PERSONALES	CATEGORÍAS DE DATOS PERSONALES	BASE LEGAL PARA EL TRATAMIENTO	RESPONSABLE / RESPONSABLES CONJUNTOS
8. Fines de marketing. Envío de mensajes comerciales y boletines.			
Los datos personales se tratan con el fin de gestionar suscripciones a servicios de notificación y comunicación (por ejemplo, boletines) y proporcionar información sobre servicios u ofertas especiales.	– Datos de contacto: nombre, correo electrónico, número de teléfono.	El consentimiento del sujeto proporcionado mediante suscripción (artículo 6(1)(a) RGPD). En el caso de una relación contractual existente, el interés legítimo del responsable del tratamiento en enviar información sobre productos y servicios similares (artículo 6(1)(f) del RGPD).	El Grupo FutureLife, junto con la clínica correspondiente del grupo a la que se refiere el envío de comunicaciones comerciales.
9. Investigación científica y de investigación			
Los datos personales se tratan con fines científicos y de investigación para profundizar el conocimiento sobre las condiciones de fertilidad y salud reproductiva, mejorar los métodos de tratamiento de reproducción asistida y apoyar la formación profesional en este ámbito.	- Datos médicos y de salud: historial médico, resultados diagnósticos, información sobre tratamientos, signos vitales, datos de salud mental/conductual, datos de salud reproductiva, etc.	Interés legítimo en realizar actividades de investigación científica en el ámbito de la fertilidad y la salud reproductiva (artículo 6(1)(f) del RGPD). Si los datos no están anonimizados, se requiere el consentimiento explícito de los interesados (artículo 6(1)(a) RGPD).	El Grupo FutureLife junto con la clínica correspondiente del Grupo al que se refiere la investigación.

Propósito del tratamiento de datos personales	Categorías de datos personales	Base legal para el tratamiento	Responsable / Responsables conjuntos
10. Mantenimiento y análisis de sitios web			
Los datos personales se tratan con el propósito de garantizar y optimizar el rendimiento del sistema, evaluar la seguridad y la estabilidad, y proporcionar publicidad personalizada basada en el comportamiento del usuario. Esto se consigue mediante el uso de tecnología de cookies. Para información más detallada, consulte la Política de Cookies.	- La dirección IP del dispositivo conectado a Internet. – Fecha y hora de acceso. - La URL del referente, el tipo de navegador y el sistema operativo. - El nombre del proveedor de acceso.	Para cookies que no son necesarias: consentimiento proporcionado mediante la configuración/preferencias de cookies (artículo 6 (1)(a) RGPD). Para cookies técnicas y necesarias: interés legítimo en garantizar la seguridad, estabilidad y usabilidad del sitio web (artículo 6 (1)(f) RGPD).	Grupo FutureLife.
11. Cumplimiento de las obligaciones legales			
Los datos personales se tratan con el fin de cumplir con obligaciones legales, incluidas aquellas relacionadas con la protección de datos personales, obligaciones fiscales y contables, sanitarias y otras normativas legales aplicables. Los datos también pueden estar disponibles para las autoridades policiales, tribunales, administración u otras autoridades públicas si la ley lo requiere.	– Datos de contacto: nombre, correo electrónico, número de teléfono. - Datos de contenido: información contenida en documentos y comunicaciones relacionadas con el cumplimiento de requisitos legales o regulatorios.	Cumplimiento de obligaciones legales (artículo (1)(c) RGPD).	El Grupo FutureLife, junto con la clínica correspondiente del grupo al que se refiere la obligación y el tratamiento de datos personales.

ANEXO B – MATRIZ RACI

Esta matriz RACI describe los roles y responsabilidades relacionados con el cumplimiento de la Política de Protección de Datos Personales entre las partes interesadas clave. A continuación se incluye la leyenda que explica el significado de cada designación utilizada en la matriz RACI:

- **R (Responsible):** Persona que debe ejecutar la tarea o actividad de forma directa.
- **A (Accountable):** Persona que debe asumir la responsabilidad final de la correcta y completa realización de la tarea.
- **C (Consulted):** Persona que debe ser consultada información, opiniones o conocimientos especializados antes de completar la tarea.
- **I (Informed):** Persona que debe mantenerse informada sobre el progreso y las decisiones tomadas, pero no participa activamente en la ejecución de la tarea.

Tabla 2: Matriz RACI

Actividad / Rol	DPO	CTO	Jefe del Departamento Jurídico	Local Security Officer	Departamento de Recursos Humanos	Empleados	Proveedores	Gerente de Ciberseguridad	Business Owner	Functional Owner
Supervisar el cumplimiento del RGPD	R	A	A	C	I	I	I	C	A	C
Punto de contacto con las autoridades de control	R	I	I	I	I	I	I	I	I	I
Formación y consultoría en el ámbito de la protección de datos personales	R	C	C	C	C	I	I	C	I	C
Auditorías y evaluaciones internas	R	A	C	C	I	I	C	C	C	C
Evaluación del Impacto en la Protección de Datos (EIPD)	A	I	C	C	I	I	C	C	R	R
Registros de las actividades de tratamiento	R	I	C	C	I	I	C	I	C	R

Aprobación de la Política y supervisión posterior	I	A	R	I	I	I	I	C	C	I
Salvaguardas técnicas para los datos personales	C	I	R	C	I	I	R	A	C	C
Respuesta a incidentes y violaciones de seguridad de datos personales	C	I	R	C	C	I	C	A	I	I
Cumplimiento local del RGPD	I	I	C	R	I	I	I	C	R	R
Tratamiento de datos personales de empleados	I	I	I	I	R	I	I	I	R	R
Formación del personal	C	I	C	R	R	R	I	C	I	C
Manejo responsable de datos personales	I	I	I	I	I	R	R	C	R	R
Tratamiento contractual de datos personales	I	I	I	I	I	I	R	C	R	C
Pruebas de penetración y análisis de riesgos	I	C	C	I	I	I	I	R	C	C
Cifrado y control de acceso	I	I	C	I	I	I	I	R	C	C

FutureLife

Política de Protección de Datos Personales

ACERCA DE FUTURELIFE

Desde la fundación del Grupo FutureLife en 2014, hemos continuado creciendo cada año. Hoy contamos con más de 50 clínicas en 16 países europeos, operadas por más de 1.500 miembros cualificados del equipo y 600 médicos. Nuestras clínicas ofrecen tratamientos integrales contra la infertilidad, incluyendo pruebas genéticas, inmunológicas y otros análisis complementarios.

Nuestro principal objetivo es proporcionar atención de calidad y tratamientos eficaces para crear niños sanos y familias felices. Invertimos continuamente en nuestras clínicas, en investigación y en formación. Esto nos permite ofrecer a nuestros equipos conocimientos especializados, estabilidad financiera, buenas condiciones laborales y una remuneración competitiva.