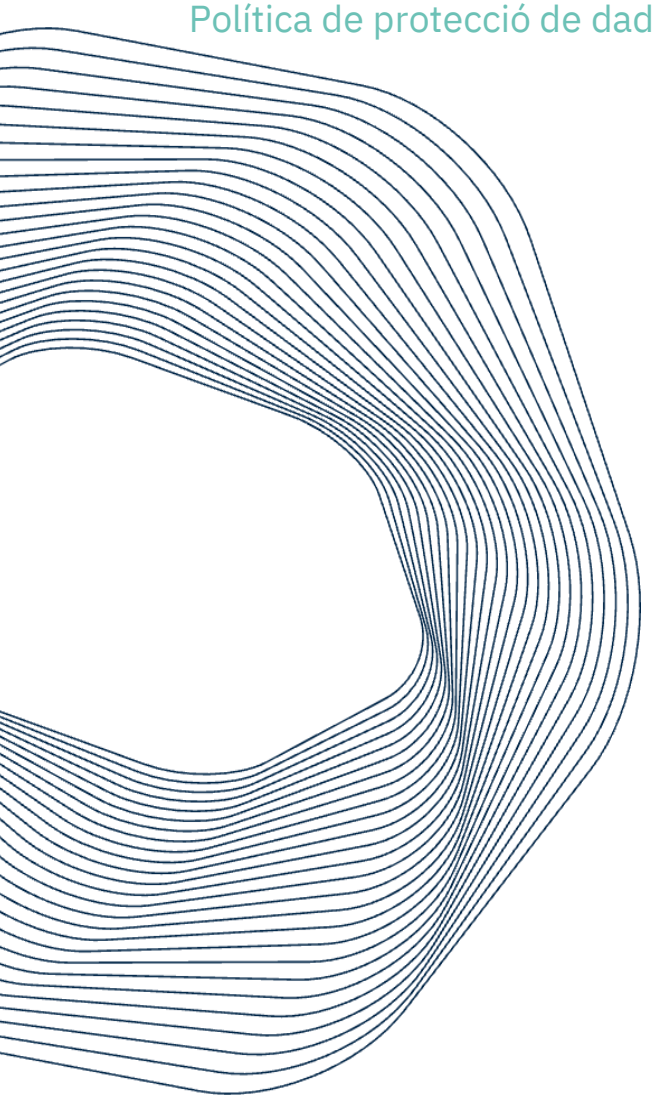
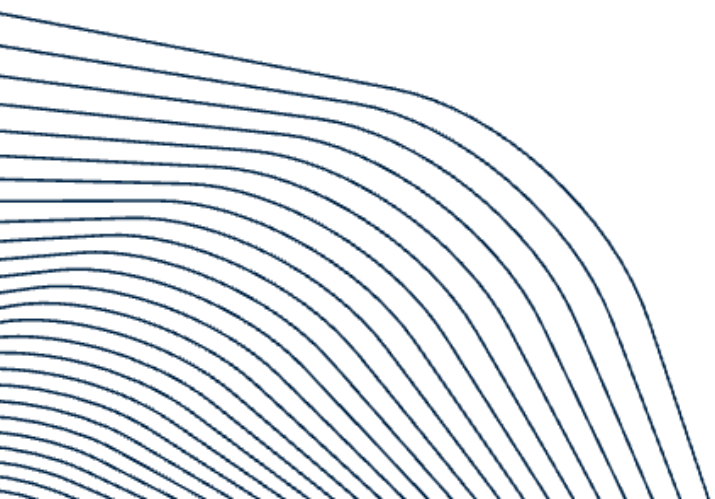
SISTEMA DE GESTIÓ DE PROTECCIÓ DE DADES PERSONALS

POLÍTICA DE PROTECCIÓ DE DADES PERSONALS

FUTURELIFE A.S.

Versió: 1.0
Data: 15-09-2025
Classificació: INTERNA





FutureLife

Política de protecció de dades personals

Títol del document:	Política de protecció de dades personals	FutureLife a.s.
Subtítol:	Sistema de Gestió de Dades Personals	Na príkopě 859/22
Persona de contacte 1:	Maroš Zuba	Nové Město, 110 00 Praga 1
Departament:	Digital	República Txeca
Persona de contacte 2:	Ilja David	
Departament:	Digital	
Document:	FL-DP-P1	
Data d'emissió:	15-09-2025	

Contingut del document:

La Política de protecció de dades personals descriu com el grup FutureLife processa les dades personals recollides dels sistemes interns, les plataformes digitals i altres fonts rellevants dins de l'organització. Aquesta política és obligatòria per a tota l'organització, incloent-hi tots els empleats, col·laboradors, filials i socis externs que gestionen dades personals. La política compleix el RGPD i altres lleis aplicables, així com els requisits de l'ISO/IEC 27701, que amplia la norma ISO/IEC 27001 incorporant mecanismes de control i directrius addicionals per a la gestió de dades personals i la informació sobre la protecció de dades personals.

Creat per:	**Verificat per:**	**Aprovat per:**
Ilja David	Maroš Zuba	Ignacio Couto
Director/a de Ciberseguretat	Cap del Departament Legal	CTO
Digital	Digital	Digital
FutureLife a.s.	FutureLife a.s.	FutureLife a.s.

Paraules clau:

Política de Protecció de Dades Personals, tecnologia de la informació, tecnologies operatives, protecció, RGPD

Confidencialitat del document:

☐ PÚBLIC. Dades d'accés públic relacionades amb les activitats diàries de l'organització o processos de domini públic.

☒ INTERN. Dades confidencials sobre el funcionament normal del negoci o els processos interns de l'organització.

☐ CONFIDENCIAL. Dades relacionades amb activitats comercials estratègiques, contractes, informació financera, dades personals i dades sobre l'estat de salut.

SEGUIMENT DE CANVIS

Versió	Data	Motiu del canvi	Creat per	Verificat per	Aprovat per
1.0	15.09.2025	Primera edició	Ilja David	Maroš Zuba	Ignacio Couto

CONTINGUT

1. INFORMACIÓ INTRODUCTÒRIA

1.1. PROPÒSIT

Aquesta Política de protecció de dades personals (d'ara endavant, la «Política») estableix un marc únic per garantir la protecció de les dades personals dins de FutureLife a.s. i totes les seves empreses afiliades que pertanyen al mateix grup empresarial (d'ara endavant, el «Grup FutureLife»). El seu objectiu és definir els principis, rols i responsabilitats relacionats amb el tractament de dades personals d'acord amb la normativa aplicable, inclòs el RGPD (Reglament general de protecció de dades) i altres disposicions nacionals rellevants.

1.2. ÀMBIT

Aquesta Política s'aplica a tots els processos, tecnologies i entitats del Grup FutureLife que duen a terme activitats de tractament de dades personals, i garanteix un enfocament uniforme en la protecció de dades personals, la seguretat de la informació i l'exercici dels drets dels interessats.

1.3. DOCUMENTS RELACIONATS

Aquesta secció enumera els documents interns relacionats que donen suport i complementen la Política de protecció de dades personals:

- **FL-CS-P1 – Política de ciberseguretat (Cybersecurity Policy):** marc normatiu per a la gestió de la ciberseguretat dins de l'organització.
- **FL-CS-S1 – Ciberseguretat de l'usuari final (End User Cybersecurity):** estàndard de comportament segur i responsabilitat dels usuaris finals dins de l'organització.
- **FL-CS-S2 – Ciberseguretat de proveïdors Supplier Cybersecurity):** estàndard per avaluar i gestionar els riscos de ciberseguretat relacionats amb proveïdors externs.
- **FL-CS-S6 – Pla de continuïtat empresarial (Business Continuity Plan):** estàndard per garantir la resiliència operativa i la recuperació de les interrupcions.
- **FL-CS-OP2 – Pla de Resposta a Incidents Ciberseguretat (Cybersecurity Response Plan):** procediment per detectar, respondre i recuperar-se d'incidents de ciberseguretat.
- **FL-CS-OP3 – Cicle de vida de desenvolupament de sistemes segurs (Secure System Development Lifecycle):** procediment per integrar les mesures de seguretat al llarg de tot el procés de desenvolupament del sistema.
- **FL-CS-OP7 – Comunicació d'incidents (Incident Communication):** procediment per a la comunicació interna i externa durant incidents de ciberseguretat.
- **FL-CS-OP09 – Requisits de seguretat de sistemes nous (New System Security Requirements):** especificació dels requisits de seguretat per al disseny i la implementació de sistemes nous.
- **FL-CS-S7 – Estàndard de seguretat de la IA (AI Security Standard):** estàndard per a l'ús segur de les eines d'IA, incloent-hi la protecció de les dades personals i organitzatives, així com de la infraestructura associada.
- **FL-CS-S4 – Auditoria interna (Internal Audit):** defineix els requisits i les responsabilitats per a l'auditoria interna com a part del Sistema de Gestió de Ciberseguretat.

1.4. TERMES

TÈRME	EXPLICACIÓ
Responsable del tractament de dades	Persona física o jurídica que determina els finalitats i els mitjans del tractament de dades personals.
Responsable del tractament de dades personals	Entitat que tracta dades personals en nom del responsable del tractament.
Categories especials de dades personals	Informació confidencial que, si es revelés, podria causar danys, discriminació o pèrdues a persones o organitzacions, o posar en perill la seguretat nacional. Exemples: informació personal de salut (PHI), dades financeres, informació personal identificable (PII), secrets comercials i dades potencialment sensibles.
Categories especials de dades	Dades personals sensibles, com ara dades de salut, dades genètiques, dades biomètriques o informació sobre l'origen racial o ètnic.
Consentiment	Expressió lliure, específica, informada i inequívoca de la voluntat de l'interessat.
Cookies	Fitxers de text petits que es descarreguen i s'emmagatzemen al dispositiu de l'usuari i que contenen una quantitat limitada d'informació.
Anonimització	Procés d'eliminació o modificació irreversible dels identificadors personals perquè no sigui possible identificar l'individu.
Responsables conjunts	Dues o més entitats que determinen conjuntament els fins i els mitjans del tractament de dades personals.
Dades personals	Qualsevol informació relativa a una persona física identificada o identificable.
Dades de salut personal	Informació mèdica confidencial que identifica una persona i es refereix a la seva salut física o mental, passada, present o futura, a la prestació d'atenció sanitària o al pagament de serveis sanitaris.
Ús principal de les dades de salut	Ús de la informació recollida directament durant la prestació d'atenció sanitària a la persona.
Ús secundari de les dades de salut	Informació recollida durant l'atenció que s'utilitza per a finalitats diferents de l'atenció directa (p. ex., recerca, salut pública, planificació de serveis, millora de la qualitat, desenvolupament de polítiques).

1.5. ABREVIATURES

ABREVIATURA	EXPLICACIÓ
IA	Intel·ligència Artificial (Artificial Intelligence, AI)
CRA	Llei de Resiliència Cibernètica (Cyber Resilience Act)
DPA	Annex de privacitat de dades (Data Privacy Annexe)
EIPD	Avaluació d'impacte en la protecció de dades (Data Protection Impact Assessment, DPIA)
DPO	Responsable de Protecció de Dades (Data Protection Officer)
EEE	Espai Econòmic Europeu (European Economic Area, EEA)
EEHRXF	Format Europeu d'Intercanvi de l'Historial de Salut Electrònic (European Electronic Health Record Exchange Format)
EEDS	Espai Europeu de Dades de Salut (European Health Data Space, EHDS)
HCE	Historials clínics electrònics (Electronic Health Record, EHR)
RGPD	Reglament general de protecció de dades (General Data Protection Regulation, GDPR)
HDAB	Òrgan d'Accés a les Dades de Salut (Health Data Access Body)
NIS2	Directiva de seguretat de les xarxes i sistemes de la informació (Network and Information Security Directive 2)
PDE	Producte amb elements digitals (Product with Digital Elements)
PHI	Informació personal de salut i categories especials de dades personals (Personal Health Information & Sensitive Data)
PII	Informació Personalment Identificable (Personally Identifiable Information)
RACI	Matriu d'assignació de responsabilitats (Responsibility Assignment Matrix)

SAE	Esdeveniments adversos greus (Serious Adverse Events)
SAR	Reaccions adverses greus (Serious Adverse Reactions)
SCCs	Clàusules contractuals estàndard (Standard Contractual Clauses)
SoHO	Reglament sobre substàncies d'origen humà (Substances of Human Origins Regulation)

2. POLÍTICA DE PROTECCIÓ DE DADES PERSONALS

FutureLife Group fa tot el possible per respectar la privacitat i garantir la seguretat de les dades personals que processa, d'acord amb el Reglament general de protecció de dades (RGPD), la Directiva NIS2, l'Espai Europeu de Dades de Salut (EHDS), el Reglament de la UE sobre substàncies d'origen humà (Reglament SoHO de la UE), el Pla d'Acció de Ciberseguretat de la UE fins al 2025, la Llei d'Intel·ligència Artificial de la UE (Llei d'IA), la Llei de Resiliència Cibernètica (CRA) i les normatives nacionals aplicables de protecció de dades.

Aquesta Política de protecció de dades personals conté informació important sobre les dades personals, els mètodes de recollida, ús i protecció d'aquestes, i per tant, s'ha de revisar amb atenció.

2.1. IDENTIFICACIÓ DEL RESPONSABLE DEL TRACTAMENT DE DADES

Les dades personals són tractades, segons les circumstàncies de cada cas, pel FutureLife Group i/o les seves filials corresponents com a responsables del tractament per a les finalitats descrites en aquesta Política de protecció de dades personals.

2.2. FUTURELIFE COM A RESPONSABLE DEL TRACTAMENT

Les dades personals són recollides i tractades pel FutureLife Group com a responsable del tractament en el context de les seves activitats organitzatives, per exemple, en subscriure-s'hi a butlletins informatius o en enviar una sol·licitud d'informació a través de formularis de contacte. Les dades d'identificació del FutureLife Group, com a responsable del tractament, són les següents:

2.2.1. FILIALS DEL GRUP FUTURELIFE COM A RESPONSABLES DEL TRACTAMENT DE DADES

FutureLife Group és responsable del tractament de les dades personals en l'àmbit de les seves pròpies activitats operatives, incloent-hi la prestació de serveis sanitaris, el manteniment dels historials mèdics dels pacients i altres activitats empresarials autoritzades.
La filial que gestiona un centre mèdic o una clínica i que determina els fins i els mitjans del tractament de dades personals per a les finalitats esmentades es considerarà responsable d'aquestes dades personals. Es pot obtenir una llista completa de les filials del FutureLife Group i de les seves clíniques sanitàries afiliades a petició.

La documentació mèdica és processada exclusivament per la clínica corresponent del FutureLife Group que presta els serveis sanitaris. El FutureLife Group no té accés, en cap cas, a informació sanitària personalment identificable.

2.2.2. FUTURELIFE I LES SEVES FILIALS COM A CORRESPONSABLES DEL TRACTAMENT DE DADES

Segons la naturalesa de les activitats específiques, el FutureLife Group, juntament amb les seves filials, pot actuar com a corresponsable del tractament de les dades personals dels usuaris, en particular amb finalitats de màrqueting, per a l'enviament de comunicacions comercials relacionades amb el FutureLife Group, la realització d'enquestes de mercat i de satisfacció, i l'exercici d'altres funcions operatives i organitzatives a nivell de Grup.

2.3. GESTIÓ D'INCIDENTS DE SEGURETAT AL GRUP FUTURELIFE

Els incidents relacionats amb la protecció de dades personals es gestionen d'acord amb **el Pla de Resposta a Incidents de Ciberseguretat** del FutureLife Group **(FL-CS-OP2)**.

Aquest pla estableix els procediments per a la identificació, l'avaluació, la notificació i la resolució oportuna dels incidents de seguretat que puguin donar lloc a una violació de la seguretat de les dades personals.

L'objectiu d'aquests procediments és minimitzar l'impacte sobre els interessats, garantir que es prenguin les mesures correctores adequades i complir les obligacions legals, inclosa l'obligació de notificar a l'autoritat de control competent i als interessats afectats.

3. ROLS I RESPONSABILITATS

Aquesta secció defineix els rols clau dins del Grup FutureLife i les responsabilitats per a la protecció de les dades personals.

Per a una descripció detallada de l'assignació de rols i responsabilitats d'acord amb aquesta Política de protecció de dades personals, s'inclou una matriu RACI a l'Annex B.

3.1. RESPONSABLE DE PROTECCIÓ DE DADES (DATA PROTECTION OFFICER, DPO)

Pel que fa a la protecció de dades personals, el **DPO** ha de:

- Supervisar el compliment dels principis i requisits del RGPD i d'altres normatives aplicables en matèria de protecció de dades.
- Actuar com a punt de contacte amb l'autoritat de control competent.
- Proporcionar directrius metodològiques i formació sobre la protecció de dades personals.
- Realitzar auditories i avaluacions internes relacionades amb el tractament de dades personals.
- Assessorar en la realització d'Avaluacions d'Impacte en la Protecció de Dades (AIPD).
- Revisar i actualitzar el Registre d'Activitats de Tractament.
- Revisar i actualitzar la documentació relativa a les activitats de tractament, incloent-hi mapes de processos i diagrames associats.
- Mantenir i conservar registres de les activitats de tractament de dades personals.

3.2. DIRECTOR/A DE TRANSFORMACIÓ (CHIEF TRANSFORMATION OFFICER ,CTO)

Pel que fa a la protecció de dades personals, el **CTO** ha de:

- Aprovar i supervisar la implementació de la Política de protecció de dades personals.
- Dirigir les iniciatives estratègiques relacionades amb la protecció de dades a tota l'organització.
- Assegurar que els procediments de protecció de dades estiguin alineats amb els objectius de transformació empresarial.
- Promoure la coordinació interdisciplinària en matèria de protecció de la privacitat.
- Garantir la implementació i execució de programes de formació i conscienciació sobre la protecció de dades personals.
- Donar suport a l'aplicació de les mesures disciplinàries adequades en casos de no compliment.

3.3. CAP DE L'ÀREA JURÍDICA (HEAD OF LEGAL)

Pel que fa a la protecció de dades personals, el Cap de l'Àrea Jurídica assumeix el paper de Delegat de Protecció de Dades del Grup (DPO del Grup) i ha de:

- Implementar i mantenir mesures tècniques de seguretat per a la protecció de dades personals.
- Gestionar incidents de ciberseguretat i vulneracions de la seguretat de les dades personals.
- Donar suport als processos de conservació i supressió de dades.
- Col·laborar amb el DPO local per garantir el compliment normatiu a nivell de sistema.
- Realitzar proves de seguretat, proves de penetració i anàlisis periòdiques de riscos.
- Proporcionar formació sobre ciberseguretat i el tractament segur de dades personals.

- Col·laborar amb proveïdors externs per garantir la seguretat dels sistemes i dels fluxos de dades.
- Assegurar el xifratge, el control d'accés i altres mesures tècniques per protegir les dades personals.

3.4. Responsable de Seguretat Local

Pel que fa a la protecció de dades personals, el **Responsable de Seguretat Local** ha de:

- Assegurar el compliment local de la Política de protecció de dades personals i del RGPD.
- Supervisar la manipulació segura de la documentació mèdica i d'altres categories especials de dades personals.
- Formar el personal de la clínica en els procediments de protecció de dades.
- Informar els incidents relacionats amb les dades personals a la unitat de gestió central.
- També assumeix el paper de DPD local, si així ho determina la direcció.
- Coordinar-se amb el DPO i el director/a de TI en la gestió de riscos a nivell de clínica.

3.5. Director/a de Ciberseguretat

Pel que fa a la protecció de dades personals, el/la **responsable de ciberseguretat** ha de:

- Dissenyar, implementar i mantenir mesures de seguretat per a la protecció de dades personals.
- Monitorar les ciberamenaces i vulnerabilitats que puguin comprometre les dades personals.
- Coordinar la resposta als incidents de seguretat i a les violacions de dades personals en col·laboració amb el Delegat de Protecció de Dades local i el Cap de l'Àrea Jurídica.

3.6. Responsable del negoci (BO)

Pel que fa a la protecció de dades personals, el **Responsable del negoci** (BO) ha de:

- Assegurar que les activitats de tractament de dades personals en el seu àmbit compleixin la Política de protecció de dades personals i la normativa aplicable (p. ex., RGPD).
- Col·laborar amb el DPO en la identificació i mitigació dels riscos relacionats amb la protecció de dades personals.
- Assegurar que els proveïdors i sistemes utilitzats a la seva àrea compleixin els requisits de protecció de dades i de seguretat de la informació.

Ser responsable de l'ús legítim de les dades personals en les aplicacions i serveis sota la seva gestió.

3.7. Propietari funcional (FO)

Pel que fa a la protecció de dades personals, un **Propietari Funcional** (FO) ha de:

- Garantir el compliment operatiu dels requisits de protecció de dades dins del seu àmbit funcional.
- Dirigir l'Avaluació d'Impacte en la Protecció de Dades (DPIA) en col·laboració amb el Responsable de l'Àrea de Negoci i el Delegat de Protecció de Dades (DPO).
- Assegurar que els procediments de tractament de dades personals estiguin documentats i que compleixin les normes internes de protecció de dades.
- Donar suport a l'execució d'auditories, revisions i actualitzacions dels sistemes i aplicacions que processen dades personals.

- Iniciar i supervisar la preparació de l'avaluació d'impacte en la protecció de dades (AIPD) per a noves activitats de tractament o per a aquelles que hagin experimentat canvis significatius.

Coordina amb l'àrea de TI i el departament jurídic la implementació de mesures tècniques i organitzatives per a la protecció de dades personals.

3.8. Departament de Recursos Humans (HR Departament)

Pel que fa a la protecció de dades personals, el Departament de Recursos Humans ha de:

- Garantir el tractament lícit de les dades personals dels empleats.
- Gestionar la protecció de dades durant els processos de selecció, incorporació i finalització de la relació laboral.
- Garantir la confidencialitat i l'emmagatzematge segur dels expedients del personal.

3.9. Tots els empleats

Pel que fa a la protecció de dades personals, tots els empleats han de:

- Complir la Política i els procediments relatius a la protecció de dades personals.
- Participar en la formació obligatòria sobre protecció de dades i ciberseguretat.
- Notificar sense demora qualsevol sospita de violació o mal ús de dades personals.
- Processar les dades personals de manera responsable i d'acord amb els principis de seguretat.

3.10. Proveïdors externs i tercers

Pel que fa a la protecció de dades personals, tots els proveïdors externs i tercers han de:

- Tractar les dades personals exclusivament d'acord amb les instruccions de FutureLife.
- Complir totes les obligacions contractuals relatives a la protecció de dades.
- Implementar i mantenir mesures tècniques i organitzatives adequades.
- Signar i complir els acords de confidencialitat i els acords de tractament de dades (DPAs).
- Cooperar en la realització d'auditories, controls i avaluacions de compliment.

4. GESTIÓ DE DADES PERSONALS

Alguns serveis es poden utilitzar sense proporcionar dades personals. No obstant això, per accedir a funcions com el registre, les subscripcions al butlletí o la comunicació personalitzada, és essencial proporcionar dades personals.

Es poden recollir dades personals:

- Directament, per exemple, mitjançant formularis, trucades o correus electrònics.
- Indirectament, mitjançant galetes i altres tecnologies de seguiment.

Els camps obligatoris estan marcats amb un asterisc (*); sense emplenar-los, no és possible prestar el servei. La informació detallada sobre les categories de dades personals, les finalitats del tractament i els períodes de conservació està disponible a **l'Annex A: Categories de dades personals i finalitats del tractament.**

4.1. SEGURETAT

La seguretat i confidencialitat de les dades personals al FutureLife Group s'assegura mitjançant un conjunt de mesures tècniques i organitzatives que es detallen a la **Política de Ciberseguretat (FL-CS-P1)**. Aquestes mesures s'han implementat per prevenir la pèrdua, l'ús indegut, l'accés no autoritzat o qualsevol altra tractament il·lícit de dades personals, d'acord amb el RGPD i la normativa nacional de protecció de dades aplicable.

El titular de les dades també és responsable de protegir la seva informació personal i ha d'anar amb compte quan comparteixi contingut. FutureLife Group no supervisa el contingut o la informació que el titular de les dades decideix compartir amb tercers i no es fa responsable de les conseqüències d'aquesta compartició.

4.2. COOKIES

Gran part de la informació esmentada en aquesta Política de protecció de dades personals es recull mitjançant galetes. Les galetes són petits fitxers de text que contenen una quantitat limitada d'informació i que es descarreguen al dispositiu de l'usuari —per exemple, ordinador, telèfon intel·ligent o tauleta— quan es visita un lloc web.

Les galetes s'utilitzen principalment per recordar la configuració del compte, l'idioma i el país preferits, així com per analitzar el comportament de l'usuari al lloc web i mostrar publicitat personalitzada tant en el lloc web com en llocs web de tercers.

Quan ho exigeixi la normativa, es demanarà el consentiment de l'usuari per a l'ús de les galetes. Per a més informació sobre com s'utilitzen les galetes i com gestionar-les o desactivar-les, consulteu **la** nostra **Política de cookies**.

4.3. DRETS DE L'USUARI EN RELACIÓ AMB LA PROTECCIÓ DE LES DADES PERSONALS

Les persones interessades les dades personals de les quals es tracten poden exercir els seus drets en qualsevol moment d'acord amb la normativa aplicable, incloent-hi els drets d'accés, rectificació, limitació del tractament, supressió, oposició i portabilitat de les dades personals.

La gestió i el tractament de les sol·licituds per a l'exercici dels drets corresponen a les funcions següents:

- **Responsable de Protecció de Dades (RPD):** Responsable de l'administració i la verificació de totes les sol·licituds d'exercici de drets.
- **Cap del Departament Legal:** Assegura el compliment normatiu i proporciona suport en casos complexos.
- **Responsable de Seguretat Local:** coordina la implementació local de les mesures de seguretat i la preparació d'informes relacionats amb les sol·licituds.
- **Departament de Recursos Humans:** Gestiona les sol·licituds relatives a les dades personals dels empleats.
- **Responsable de negoci (BO):** responsable de la gestió adequada de les sol·licituds relacionades amb els sistemes sota el seu control.
- **Propietari funcional (FO):** dona suport a l'execució tècnica, incloent-hi la restricció de dades quan sigui possible.

En rebre una sol·licitud vàlida:

- El tractament de les dades personals objecte de la sol·licitud s'ha de suspendre immediatament.
- Les dades personals s'han de bloquejar durant el procés de verificació.
- Si el titular de les dades presenta una objecció, les dades personals ja no es podran tractar, tret que el responsable del tractament demostri motius legítims imperiosos per continuar el tractament.

Les sol·licituds s'han d'enviar per correu electrònic a **dpo@futurelifegroup.com** amb l'assumpte "Subjecta/at a la protecció de dades personals" i indicant clarament el dret que es vol exercir.

Les persones interessades també tenen dret a presentar una reclamació davant l'autoritat de supervisió competent si consideren que les seves dades personals s'estan tractant en violació de la normativa aplicable.

4.4. TIPUS I ACTIVITATS DE TRACTAMENT DE DADES PERSONALS

La llista següent indica els principals tipus i activitats de tractament de dades personals que duu a terme el FutureLife Group. Totes aquestes activitats es duen a terme d'acord amb el RGPD i la normativa nacional de protecció de dades aplicable:

- **Gestió de dades de pacients:** recollida, emmagatzematge i tractament de dades personals i dades de salut amb la finalitat de prestar serveis sanitaris, mantenir registres mèdics i complir les obligacions legals.
- **Programació de visites:** tractament de dades de contacte i d'identificació per gestionar reserves, programar visites i garantir la comunicació amb els pacients.
- **Comunicació i atenció al client:** tractament de dades personals per respondre consultes, oferir assistència i compartir la informació sol·licitada.
- *Com***unicacions comercials i de màrqueting:** tractament de les dades de contacte per a l'enviament de butlletins informatius (*newsletters*), material promocional i enquestes de satisfacció — sempre basat en el consentiment vàlid quan sigui legalment requerit.
- **Seguiment del lloc web i galetes:** recollida de dades mitjançant galetes i tecnologies similars amb la finalitat d'analitzar l'ús del lloc web i personalitzar el contingut.
- **Reclutament i gestió de recursos humans:** tractament de dades personals de candidats i empleats per a processos de selecció, incorporació, càlcul de nòmines, avaluació de rendiment i altres procediments de recursos humans.

- **Compliment d'obligacions legals i reguladores:** tractament de dades necessàries per complir amb les obligacions legals, incloent-hi l'arxivament, les auditories i les notificacions obligatòries a les autoritats públiques.
- **Assegurances i facturació:** intercanvi de dades rellevants amb asseguradores i entitats de facturació per gestionar reclamacions i processar pagaments.
- **Operació i seguretat de TI:** ús de dades personals en registres del sistema, gestió d'accés, xifratge, monitoratge i gestió d'incidents de seguretat.
- **Recerca i anàlisi estadística:** ús de dades anonimitzades o pseudonimitzades per a la recerca científica i per a finalitats estadístiques internes.
- **Gestió dels drets de les persones interessades:** tractament de dades personals per respondre a sol·licituds d'accés, rectificació, supressió i altres drets en virtut del RGPD.
- **Gestió de proveïdors i prestadors de serveis:** intercanvi de dades personals amb socis i proveïdors externs en virtut d'obligacions i garanties contractuals.
- **Transferències internacionals de dades:** transmissió de dades personals a entitats situades fora de l'Espai Econòmic Europeu (EEE), només amb garanties adequades i d'acord amb els mecanismes legals aplicables.

4.5. REGISTRE DE DADES PERSONALS

El Registre de Dades Personals és l'inventari central de totes les activitats de tractament de dades personals realitzades dins del FutureLife Group. Assegura la transparència, la responsabilitat i el compliment del RGPD. Aquest registre documenta la gestió legal, segura i ètica de les dades personals, incloses les dades sensibles o les que pertanyen a categories especials.

4.5.1. ABAST

El Registre de Dades Personals inclou totes les categories de dades tractades pel FutureLife Group, incloent-hi:

- Documentació clínica del pacient i de la seva parella.
- Dades personals genètiques, biomètriques i de laboratori.
- Informació sobre salut reproductiva i tractaments.
- Dades administratives, financeres i d'assegurances.
- Informació sobre empleats i proveïdors.
- Dades processades a través de tercers (p. ex. laboratoris, magatzems o proveïdors de TI).

4.5.2. RESPONSABILITAT

- El Responsable de Protecció de Dades (DPO) és responsable de gestionar, controlar i actualitzar el Registre de Dades Personals.
- Les parts implicades han d'informar el DPO de qualsevol nova o modificada activitat de tractament.
- El DPO garanteix que el Registre de Dades Personals sigui exacte, complet i actualitzat, i que estigui disponible per a la seva revisió per part de l'autoritat de protecció de dades competent (APD) a petició.

4.5.3. CONTINGUT

S'haurà de registrar la informació següent per a cada activitat de tractament:

- **Detalls del responsable del tractament:** nom, adreça i dades de contacte de la clínica.
- **Finalitat del tractament:** prestació d'atenció clínica, diagnòstic, recerca (si s'escau), facturació o activitats administratives.
- **Categories de persones interessades:** pacients, socis, donants, fills nascuts com a resultat del tractament, empleats i proveïdors.
- **Categories de dades personals:** dades d'identificació, dades de contacte, historial mèdic, informació sobre salut reproductiva, dades genètiques, resultats d'analítiques de laboratori, dades de facturació i assegurança.
- **Categories especials de dades personals:** dades explícitament designades, en particular informació sobre la salut genètica i reproductiva.
- **Destinataris de les dades personals:** equips interns, laboratoris, hospitals, proveïdors d'emmagatzematge, asseguradores i autoritats reguladores.
- **Transferències a tercers països:** informació sobre possibles transferències de dades personals fora de l'EEE, inclosa una descripció de les garanties legals i de seguretat implementades (vegeu la secció 4.8 Transferències de dades).
- **Plaços de conservació:** períodes definits d'acord amb els requisits mèdics, legals i normatius (vegeu la secció 4.9 Plaços de conservació).
- **Mesures de seguretat:** mesures adoptades (p. ex. xifratge, pseudonimització o control d'accés).

4.5.4. Enllaç al Registre d'Incidents

El Registre de Dades Personals està vinculat al procés de gestió de violacions de la seguretat de les dades personals. Per a cada incident registrat, s'ha de registrar l'activitat de tractament corresponent per garantir la responsabilitat, la traçabilitat i la transparència d'acord amb els requisits del **RGPD**.

4.5.5. Revisions i actualitzacions

El Registre de Dades Personals es revisa com a mínim un cop l'any o sempre que hi hagi canvis significatius en les activitats de tractament de dades personals. Les actualitzacions del registre són obligatòries, especialment en els casos següents:

- S'introdueixen nous procediments mèdics, tecnologies o mètodes de diagnòstic.
- S'incorporen nous processadors de dades o proveïdors de serveis externs.
- Es produeixen canvis en els requisits legals o normatius relatius a la protecció de dades personals.

4.6. Gestió del consentiment del pacient

Donada la naturalesa altament sensible de les dades de salut reproductiva i de l'assistència sanitària processades, el FutureLife Group obté, registra i respecta el consentiment del pacient:

- **Recollida del consentiment**
  - El consentiment s'obté en els casos que preveu la llei, especialment per al tractament de dades de categories especials de dades personals (p. ex., dades de fertilitat, dades genètiques i mèdiques) i per a qualsevol ús secundari de les dades.
  - El consentiment s'obté mitjançant un formulari de consentiment del pacient que explica clarament l'objectiu del tractament, l'abast de les dades i els drets del pacient.

- El consentiment és sempre voluntari, específic, informat i inequívoc.

> **Gestió del consentiment**

- Les preferències i l'estat del consentiment s'emmagatzemen de manera segura.
- Només el personal autoritzat té accés a la informació del consentiment i la capacitat d'actualitzar-la.
- Quan el tractament o la participació en una investigació requereix un consentiment prolongat, s'oferiran oportunitats periòdiques per confirmar o actualitzar el consentiment.

> **Retirada del consentiment**

- El pacient pot retirar el seu consentiment en qualsevol moment, sense afectar la licitud del tractament realitzat abans de la retirada.
- La retirada del consentiment no afecta la qualitat ni l'abast de l'atenció prestada.
- Les sol·licituds de retirar o modificar el consentiment es tramiten sense dilació indeguda.

> **Registre i conservació de proves**

- Es conserva un registre complet de quan, com i amb quina finalitat es va donar el consentiment (p. ex., registres d'auditoria electrònics o formularis signats).
- Aquests registres es conserven de manera segura durant el període establert per la normativa aplicable.
- En cas de retirada del consentiment, els registres s'actualitzen en conseqüència i les dades corresponents es bloquegen o se'n suspèn la seva tractament.

4.7. COMPARTICIÓ DE DADES PERSONALS

FutureLife ha implementat garanties per als casos en què cal compartir dades personals amb tercers o proveïdors de serveis externs:

> **Asseguradores i entitats d'assegurança mútua (incloent-hi tercers en casos d'assegurança de responsabilitat civil):**

- Les dades personals es poden compartir per verificar la cobertura d'assegurança i gestionar el pagament de les despeses sanitàries.
- Només es comparteixen les dades estrictament necessàries; no es proporcionen dades mèdiques ni dades de salut sensibles, tret que ho exigeixi la llei.
- Si l'asseguradora està situada fora de l'EEE en un país sense un nivell de protecció de dades equivalent:
    - Pot ser necessari transferir dades personals per al processament de reclamacions.
    - La transferència només es realitza amb el consentiment informat i explícit del pacient.
    - Només es transfereix la quantitat mínima de dades necessària.
    - Si es denega el consentiment, l'asseguradora pot denegar la cobertura i el pacient n'assumiria tots els costos.

> **Filials de FutureLife Group:**

- Les dades personals mínimes necessàries es poden compartir entre les clíniques del FutureLife Group per garantir la continuïtat i la qualitat de l'atenció.

> **Proveïdors externs i prestadors de serveis:**

- Les dades personals es poden compartir amb socis que presten serveis en àrees com l'atenció sanitària, el diagnòstic, l'anàlisi de laboratori, l'auditoria, la seguretat, el suport informàtic, l'assessorament jurídic i les activitats administratives.
- Els proveïdors també poden gestionar i mantenir plataformes o aplicacions digitals utilitzades pel FutureLife Group.
- Les dades es comparteixen només en la mesura que sigui necessari per a la prestació dels serveis contractats.

> **Representants legals, assessors i autoritats reguladores:**

- Les dades personals es poden compartir per exercir els drets de FutureLife Group, resoldre reclamacions, cooperar amb les autoritats o obtenir assessorament legal.
- Els destinataris poden operar dins o fora de l'EEE; en cas de transferència fora de l'EEE, s'apliquen les garanties adequades, en particular mitjançant les Clàusules Tipus de Contracte (SCC).
- Tots els destinataris de dades personals estan obligats a protegir-ne la confidencialitat, la integritat i la seguretat d'acord amb el RGPD.

4.8. TRANSFERÈNCIES DE DADES PERSONALS

D'acord amb el Reglament general de protecció de dades (RGPD), les dades relatives a l'atenció sanitària i la salut reproductiva poden circular lliurement dins de la UE i l'Espai Econòmic Europeu (EEE), sempre que es processin amb les garanties adequades. Qualsevol ús secundari de les dades —per exemple, per a la recerca o els registres sanitaris— requereix el consentiment explícit del pacient i una protecció sòlida. L'Espai Europeu de Dades de Salut (EEDS), a partir del 2025, enfortirà els drets dels pacients transfronterers i establirà noves normes per a l'ús secundari de dades de salut sensibles.

4.8.1. FLUX DE DADES PERSONALS I COMPLIMENT NORMATIU

La transferència de dades personals dins de la UE/EEE no està subjecta a restriccions addicionals per motius de protecció de dades; per tant, no es requereixen Clàusules Contractuals Estàndard (CCE) ni avaluacions d'adequació. No obstant això, en qualsevol transferència de dades, és essencial garantir el compliment total del RGPD i de les polítiques internes de l'organització:

> **Minimització de dades:** només s'ha de compartir la informació estrictament necessària per a la finalitat definida.
> **Limitació de la finalitat:** les dades personals només es poden tractar per a finalitats sanitàries clarament definides i legítimes.
> Integr**itat i confidencialitat:** Les dades s'han de protegir contra l'accés, l'alteració, la pèrdua o la destrucció no autoritzats.
> **Transparència:** Els pacients han de ser informats clarament quan les seves dades es comparteixin fora de la UE/EEE.
> **Drets de les persones interessades:** S'ha de garantir l'exercici de tots els drets, incloent-hi l'accés, la rectificació, la limitació del tractament i l'eliminació.
> **Seguretat:** xifratge, control d'accés, registres d'auditoria.

4.8.2. Ús secundari de dades reproductives

Quan les dades s'utilitzen fora del context de l'atenció directa, s'apliquen normes significativament més estrictes. L'ús secundari de les dades reproductives dels pacients (p. ex., recerca, millora de la qualitat, formació, registres, desenvolupament de productes, màrqueting) requereix:

- **Consentiment exprés:** Les dades només es tractaran si el pacient ha donat el seu consentiment explícit.
- **Garanties:** Pseudonimització o anonimització.
- **Transparència:** Els pacients han de ser conscients de quines investigacions es basen en les seves dades personals i tenir la possibilitat de revocar el seu consentiment en qualsevol moment.

4.8.3. Transferències internacionals de dades personals

La transferència de dades relacionades amb la salut o la fertilitat fora de la UE/EEE només es durà a terme d'acord amb el RGPD. Si la Comissió Europea ha emès una decisió d'adequació, les dades es poden transferir a aquests països (p. ex., Suïssa, el Japó). Per a altres destinacions, s'apliquen les Clàusules Contractuals Típiques (SCC) i es duen a terme avaluacions de riscos d'acord amb els requisits de la sentència Schrems II. En situacions excepcionals i específiques, poden aplicar-se derogacions, com ara el consentiment exprés per a una prova de laboratori puntual a l'estranger.

4.9. Períodes de conservació

Les dades personals es conserven durant el temps estrictament necessari per complir la finalitat per a la qual es van recollir, d'acord amb el principi de limitació en el temps establert pel RGPD. En alguns casos, les dades personals es poden tractar fins i tot després que s'hagi complert la finalitat original, per exemple, si el subjecte de les dades esdevé client.

Els períodes de conservació s'estableixen de la manera següent:

- **Documentació clínica:** Es conserva durant el període específicat per la normativa aplicable, normalment 10 anys des del final del tractament o l'alta, d'acord amb la legislació sanitària.
- **Dades genètiques:** Segons la normativa vigent, s'han de conservar durant almenys 30 anys des del final del tractament o l'alta.
- **Dades per a finalitats legals i administratives:** Després del període inicial, les dades es poden conservar durant un màxim de 3 anys, que correspon al termini de prescripció legal, per garantir la protecció legal i el compliment normatiu.
- **Dades amb finalitats de recerca:** Poden conservar-se en forma anonimitzada durant la durada del projecte de recerca, normalment entre 5 i 10 anys, d'acord amb la normativa aplicable. Les dades es poden compartir amb institucions de recerca acreditades amb finalitats legítimes.
- **Dades relacionades amb consultes, reclamacions o sol·licituds d'exercici de drets:** Aquestes dades es conserven durant el temps necessari per tramitar la sol·licitud, normalment entre 1 i 2 anys, i es poden conservar durant més temps si és necessari per motius legals o reguladors o per protegir els interessos legítims del responsable del tractament en cas de litigi.
- **Dades relacionades amb les relacions contractuals:** Aquestes dades es conserven durant la vigència del contracte i durant cinc anys més després de la seva finalització, amb la finalitat de gestionar qualsevol reclamació o litigi potencial.
- **Dades de subscripció al butlletí:** Es conserven fins que es revoca el consentiment o es cancel·la la subscripció.

4.10. SUPRESSIÓ DE DADES PERSONALS

La seguretat dels procediments d'eliminació de dades personals dins el marc del tractament s'assegura mitjançant mesures tècniques i organitzatives adequades. FutureLife Group implementa mètodes documentats, verificables i segurs per a l'eliminació de dades personals, d'acord amb el Reglament general de protecció de dades (RGPD) i el Reglament sobre substàncies d'origen humà (SoHO).

4.10.1. DRET A L'OBLIT

Les persones interessades tenen dret a sol·licitar l'esborrat de les seves dades personals sense dilació indeguda. Això inclou situacions en què les dades personals ja no són necessàries per a la finalitat original, el consentiment ha estat revocat o les dades s'han tractat de manera il·lícita.

4.10.2. LIMITACIONS EN EL CONTEXT DE L'ATENCIÓ SANITÀRIA

El dret a l'oblit en el sector sanitari està limitat per les obligacions legals de conservació de dades i/o per excepcions per motius de salut pública o de recerca. D'acord amb el RGPD, les dades relatives a l'assistència sanitària i la fertilitat pertanyen a categories especials de dades (de vegades anomenades "dades sensibles"). Per tant, el seu tractament requereix el consentiment explícit o una altra base jurídica, juntament amb garanties addicionals. El Reglament de la UE sobre substàncies d'origen humà exigeix una traçabilitat a llarg termini (còdigs únics no identificadors, com ara el Codi Únic Europeu) per a materials reproductius com ara gàmetes i embrions, normalment fins a 30 anys. Per tant, les clíniques poden no poder suprimir determinats registres sanitaris, fins i tot a petició de l'interessat.

4.10.3. TÈCNIQUES D'ELIMINACIÓ SEGURA

Totes les activitats relacionades amb l'eliminació de dades personals han de ser registrades i verificables.

- **Dades digitals**
  - **Supressió criptogràfica:** destrucció de les claus de xifratge per fer que les dades siguin il·legibles.
  - **Sobreescriptura (neteja de dades):** ús d'eines certificades per sobreescriure l'emmagatzematge amb patrons aleatoris.
  - **Eines certificades d'esborrat:** ús de programari aprovat per la UE per a l'eliminació segura de dades.
- **Còpies de seguretat i arxius**
  - Pl**ans de conservació:** garantir l'eliminació automàtica o el sobreescriptura de les dades de còpia de seguretat un cop expirat el termini de conservació.
  - **Separació de funcions:** només el personal autoritzat pot suprimir dades sensibles.
  - **Registres immutables:** garanteixen la traçabilitat de les supressions, fins i tot en les còpies de seguretat.
- **Mèdia físic i paper:** trituració, pulpitació o incineració, o trituració mecànica per a la destrucció física dels mitjans.

4.10.4. DOCUMENTACIÓ I AUDITORIES

Tots els procediments d'eliminació de dades personals s'han de documentar. Això inclou definir els períodes de conservació, els desencadenants per a l'eliminació i les excepcions. Es requereixen auditories periòdiques per verificar el compliment del RGPD i les obligacions relatives a substàncies d'origen humà. Totes les operacions d'eliminació han de ser rastrejables mitjançant registres d'auditoria.

4.11. NOTIFICACIÓ A LES AUTORITATS DE PROTECCIÓ DE DADES

En cas de violació de dades personals, cal informar l'autoritat de control competent sense dilació indeguda i, si és possible, en un termini de 72 hores des que el responsable del tractament n'ha tingut coneixement. Totes les entitats del Grup FutureLife han de complir els procediments interns de notificació d'incidents. La documentació relativa a la violació de seguretat i al procés de notificació s'ha de conservar amb finalitats d'auditoria i compliment normatiu.

El Delegat de Protecció de Dades (DPD) és responsable de:

- Coordinar tot el procés de notificació a l'autoritat de control.
- Mantenir i actualitzar el Registre de Dades Personals, garantint que els registres de les activitats de tractament siguin exactes, complets i actualitzats.
- Preparar l'informe de violació de la seguretat, que ha d'incloure:
  - La naturalesa i l'abast de la bretxa.
  - Categories i nombre de subjectes de dades i d'enregistraments afectats.
  - Dades de contacte per a més accions i comunicacions addicionals.
  - Conseqüències probables de la bretxa i mesures correctives preses o planificades.

L'oficial de seguretat local ha de:

- Assegurar l'escalada oportuna de l'incident des de les entitats locals fins al DPO.

El cap del Departament Jurídic ha de:

- Revisar les implicacions legals de la bretxa i donar suport a la comunicació amb les autoritats pertinents.

4.12. GESTIÓ DE RISCOS DE TERCERS

El FutureLife Group garanteix que tots els proveïdors de serveis i tercers que tracten dades personals en nom de les empreses del Grup compleixin els estrictes requisits de protecció de dades i de seguretat de la informació, d'acord amb les polítiques i regulacions internes de FutureLife. El Grup manté un Registre de Risc de Proveïdors i està regulat per l'Estàndard de Ciberseguretat per a Proveïdors (FL-CS-S2).

4.12.1. AVALUACIÓ PRÈVIA A LA COL·LABORACIÓ

- Totes les terceres parts han de completar un qüestionari sobre protecció de dades i seguretat de la informació.
- Es realitza una avaluació de riscos per avaluar les pràctiques de tractament de dades, les certificacions (p. ex., ISO 27001) i el compliment normatiu intern.
- Els Acords de Tractament de Dades (ATD) s'han de signar abans de compartir qualsevol dada personal.

4.12.2. MONITORATGE

- S'efectuen auditories o avaluacions anuals per als proveïdors d'alt risc.
- Es revisen la història de les violacions de seguretat, les capacitats de resposta a incidents i l'ús de subcontractistes.
- Les terceres parts han d'informar FutureLife Group de qualsevol brec de seguretat de dades personals o de canvis significatius en les activitats de tractament.

4.13. MAPES I DIAGRAMES PER AL TRACTAMENT DE DADES PERSONALS

Per garantir la claredat i el compliment del Reglament general de protecció de dades (RGPD) i de la normativa relacionada, cal crear i mantenir diagrames visuals i fluxos de les activitats de tractament de dades personals. Aquests diagrames han de mostrar:

- El flux de dades personals a través de sistemes i departaments.
- Els punts de recollida, emmagatzematge i transmissió de dades personals.
- Interfícies amb processadors externs (tercers).
- La ubicació dels repositoris de dades personals (incloent-hi serveis en el núvol i transferències transfrontereres).

Aquests mapes de dades s'han d'utilitzar per a les finalitats següents:

- Identificació de riscos i deficiències en la protecció de dades personals.
- Suport en la realització d'Avaluacions d'Impacte en la Protecció de Dades (AIPD).
- Facilitar auditories internes i programes de formació.

Tots els diagrames han de ser revisats pel Delegat de Protecció de Dades (DPO) com a mínim cada dos anys o quan es produeixin canvis significatius en les activitats de tractament.

4.14. Avaluació d'Impacte en la Protecció de Dades (EIPD)

Cal dur a terme una Avaluació d'Impacte en la Protecció de Dades (AIPD) abans de començar qualsevol activitat de tractament que probablement comporti un alt risc per als drets i les llibertats de les persones físiques. Això inclou, entre altres coses:

- Tractament a gran escala de categories especials de dades personals.
- Monitoratge sistemàtic d'espais d'accés públic.
- Ús de noves tecnologies o tècniques de perfilatge.

Cada avaluació d'impacte ha d'incloure:

- Descripció del tractament i la seva finalitat.
- Avaluació de la necessitat i la proporcionalitat del tractament en relació amb les finalitats.
- Identificació dels riscos per als drets i llibertats dels interessats.
- Mesures per mitigar els riscos identificats.

El DPO ha de documentar i conservar les avaluacions d'impacte en la protecció de dades. Quan ho exigeixi el RGPD, cal iniciar la consulta amb l'autoritat de control abans que comenci el tractament.

4.15. Formació i conscienciació dels empleats

Tot el personal amb accés a dades personals, incloses les dades de salut, salut reproductiva i fertilitat, rep una formació anual obligatòria sobre el RGPD, l'Espai Europeu de Dades de Salut (EEDS) i la ciberseguretat, amb mòduls dedicats a tècnics de laboratori (tractament segur de les dades de donants i embrions), clínics (principis de confidencialitat i gestió del consentiment) i personal informàtic (seguretat dels sistemes d'informació i controls d'accés). Per promoure la conscienciació, les clíniques duen a terme simulacions de phishing i campanyes de ciberseguretat, i es fa un seguiment del progrés i la finalització de la formació per garantir el compliment continu i la privadesa (incloses les categories especials de dades personals relacionades amb la fertilitat i els donants).

4.16. Revisió i gestió de la Política de protecció de dades personals

La Política de protecció de dades personals del FutureLife Group s'ha de revisar com a mínim un cop l'any o immediatament després de qualsevol canvi significatiu en els requisits normatius. El procés de revisió està coordinat pel DPO en col·laboració amb el cap jurídic, el director de ciberseguretat i el director de transformació.

La direcció de la clínica i els assessors legals locals són responsables de verificar l'aplicabilitat de la política a nivell de filial i de garantir el compliment de la normativa local. Totes les actualitzacions s'han de documentar a la taula de control de versions i comunicar-se a les parts interessades. El resum dels canvis s'ha d'incloure a l'avís d'actualització de la Política.

4.17. Disponibilitat de la Política

FutureLife Group es compromet a garantir que aquesta Política de protecció de dades personals sigui accessible a totes les persones. Les sol·licituds per obtenir-la en formats alternatius s'han d'adreçar al DPO.

Mesures d'accessibilitat:

- La Política està disponible a tots els llocs on opera el FutureLife Group.
- Els formats accessibles (p. ex., lletra de gran mida, arxius PDF compatibles amb lectors d' pantalla) estan disponibles a petició.

- Les clíniques exposen còpies impreses a les taules de recepció i ofereixen accés digital a través de llocs web i/o portals de pacients.
- El personal està format per ajudar els pacients a entendre la Política i a exercir els seus drets.

4.18. Actualització de la Política de protecció de dades personals

El FutureLife Group es reserva el dret de modificar, actualitzar o substituir aquesta Política de protecció de dades personals en qualsevol moment i a la seva discreció. La continuació de l'ús dels serveis després de qualsevol modificació s'entendrà com l'acceptació de la versió actualitzada d'aquesta Política.

Les parts interessades (usuaris) són informades que revisen periòdicament aquesta Política per mantenir-se informades de qualsevol canvi. Si la part interessada no està d'acord amb aquest document, en tot o en part, o amb qualsevol modificació posterior, ha de deixar d'utilitzar els serveis immediatament.

4.19. Annex de privacitat de dades (DPA)

L'Annex de privacitat de dades (DPA) és una part obligatòria del marc de protecció de dades de FutureLife Group. Actua com a document formal que defineix els requisits específics de privacitat i protecció de dades aplicables a cada aplicació, sistema o servei que processi dades personals, garantint la transparència, la responsabilitat i la coherència en la gestió de les dades personals dins de FutureLife Group.

L'objectiu de la DPA és garantir que totes les activitats de tractament estiguin clarament definides i es duguin a terme d'acord amb la normativa aplicable de protecció de dades (com ara el RGPD) i els estàndards interns del FutureLife Group. La DPA ha d'incloure detalls sobre:

- Categories de dades personals tractades.
- Basa jurídica del tractament.
- Període de conservació de les dades personals.
- Mesures de seguretat implementades.
- Rols i responsabilitats de les parts implicades.
- Qualsevol transferència de dades personals fora de la UE/EEE, si és rellevant per a l'activitat de tractament.

4.20. Incident de seguretat de dades – Notificació a les persones físiques

A més de notificar les autoritats de supervisió, FutureLife Group es compromet a informar les persones interessades (titulars de les dades) sense dilació indeguda en cas d'una violació de dades personals, quan aquesta violació pugui comportar un alt risc per als seus drets i llibertats.

4.20.1. Condicions per a la notificació

- La bretxa de seguretat afecta categories especials de dades personals, en particular dades de salut, de fertilitat o genètiques.
- La violació pot comportar robatori d'identitat, discriminació, danys a la reputació o altres conseqüències greus per a l'interessat.

4.20.2. MÈTODES I TERMINIS PER INFORMAR ELS INTERESSATS

- Les persones afectades seran informades sense dilació indeguda i, sempre que sigui possible, en un termini màxim de 72 hores des de la confirmació de la bretxa, per correu electrònic, telèfon o portal de pacients segur.
- La notificació inclourà una descripció de la naturalesa de la bretxa, les conseqüències probables, les mesures preses o planificades per mitigar-ne els efectes i les dades de contacte per a més informació.
- Quan no sigui possible la comunicació directa amb les persones interessades, s'publicaran avisos al lloc web de la clínica o a través d'altres canals adequats.

4.21. ÚS DE LA INTEL·LIGÈNCIA ARTIFICIAL I DE LA PRESA DE DECISIONS AUTOMATITZADA

El FutureLife Group pot utilitzar eines d'intel·ligència artificial (IA) i processos de presa de decisions automatitzada per donar suport als processos clínics i operatius. Aquestes eines s'utilitzen per millorar la precisió, l'eficiència i la qualitat de l'atenció prestada. No es prenen decisions amb un impacte legal o mèdic significatiu únicament mitjançant el processament automatitzat: totes aquestes decisions estan subjectes a la supervisió humana i a la revisió clínica.

Cada sistema que utilitza dades personals i incorpora models d'IA ha de complir:

- Desenvolupament d'IA intern o extern:
  - **FL-CS-OP09 Requisits de seguretat de sistemes nous.**
  - **FL-CS-S7 Estàndard de seguretat de la IA.**
  - Avaluació específica de l'impacte en el negoci (BIA).
- Sistemes adquirits i implementats internament o externament:
  - **FL-CS-OP-03 Cicle de vida de desenvolupament de sistemes segurs.**

Exemples d'eines i processos automatitzats:

- Classificació i selecció d'embrions.
- Algorismes per a l'emparellament de donants i receptors.
- Anàlisi de risc genètic.
- Models predictius de resultats del tractament.
- Classificació automatitzada i programació de cites.

Drets del pacient:

- Ser informats sobre l'ús de la IA en la seva atenció.
- Expressar la seva opinió sobre aquest tractament.
- Per sol·licitar la intervenció humana en la decisió.
- Impugnar les decisions preses exclusivament mitjançant el tractament automatitzat.

Quan sigui pertinent, es durà a terme una avaluació d'impacte en la protecció de dades (AIPD) per avaluar els riscos associats al tractament de dades personals i per garantir el compliment del RGPD, en particular l'article 22 i les disposicions relacionades.

4.22. PROTECCIÓ DE DADES PER A DONANTS I INFANTS CONCEBUTS MITJANÇANT DONACIÓ

El FutureLife Group compleix el marc regulador de la UE sobre Substàncies d'Origen Humà (SoHO) per garantir els estàndards més alts de seguretat, traçabilitat i protecció de dades personals en el tractament de la informació relativa als donants i als infants concebuts mitjançant donació. Aquests estàndards estan dissenyats per garantir la traçabilitat a llarg termini i la protecció de la salut pública, alhora que preserven l'anonimat dels donants, la confidencialitat dels pacients i la privacitat dels infants concebuts mitjançant donació.

4.22.1. CODIFICACIÓ ÚNICA I TRAÇABILITAT

Tot el material dels donants s'identifica amb un codi únic no identificatiu (p. ex., el Codi Europeu Únic), que permet una traçabilitat completa des de la donació fins a l'ús clínic, mantenint l'anonimat tant del donant com del pacient. Qualsevol dada d'identificació directa s'emmagatzema per separat i de manera segura, amb accés restringit al personal autoritzat i només per a finalitats permeses per la normativa. La separació entre el codi i la identitat garanteix el compliment normatiu, facilita el seguiment de la qualitat i la seguretat, i protegeix la confidencialitat dels donants i dels receptors.

4.22.2. ESDEVENIMENTS ADVERSOS GREUS I REACCIONS

Hi ha procediments formals per a la identificació, la documentació i la notificació dels Esdeveniments Adversos Greus (EAG) i les Reaccions Adverses Greus (RAG), d'acord amb la normativa de la UE i els requisits normatius nacionals. Tots els incidents s'enregistren, s'investiguen i, quan ho exigeix la llei, es notifiquen a les autoritats competents dins dels terminis establerts. Els pacients i els donants són informats sense demora quan l'esdeveniment o la reacció és rellevant per a la seva atenció, seguretat o tractament en curs.

4.22.3. DRET A LA LIMITACIÓ DEL TRACTAMENT I A L'ACCÉS A LES DADES PERSONALS

D'acord amb el RGPD, pacients i donants tenen dret a limitar el tractament de les seves dades personals i reproductives. Atès que les dades de fertilitat i reproducció constitueixen categories especials de dades personals, les persones (interessats) gaudeixen de drets ampliats, especialment pel que fa al consentiment exprés per al tractament i la possibilitat de revocar-lo en qualsevol moment.

Les mesures tècniques i organitzatives implementades per la clínica per garantir la restricció del tractament i l'accés inclouen:

- **Control d'accés basat en rols (RBAC):** Assegura que només les persones autoritzades puguin consultar els registres sensibles.
- **Separació dels registres entre donants i receptors:** Evita l'enllaç no desitjat o no autoritzat de dades.
- **Registre d'accés complet:** Permet el seguiment i l'auditoria de tots els accessos a les dades reproductives.

4.22.4. ANONIMAT DEL DONANT VS. DRETS DELS PACIENTS I DELS INFANTS

En alguns Estats membres de la UE, la normativa nacional atorga als infants concebuts mitjançant donació el dret d'accedir a les dades d'identificació del donant quan arriben a la majoria d'edat. En aquests casos, quan és legalment possible, FutureLife Group compleix les obligacions legals, mantenint els estàndards més alts de seguretat i minimització de dades personals.

4.22.5. MINIMITZACIÓ DEL RISC GENÈTIC

Minimitzar el risc genètic és una obligació essencial en virtut del Reglament de la UE sobre substàncies d'origen humà (que estableix requisits de qualitat i seguretat), del RGPD (que regula el tractament de dades genètiques) i de les normatives sanitàries nacionals. L'objectiu és reduir la probabilitat de transmetre malalties hereditàries o anomalies genètiques dels gamets (esperma/òvuls) o embrions donats al receptor i als seus futurs fills.

Elements clau per minimitzar el risc genètic:

- **Historial de salut i familiar**
  - Els donants omplen qüestionaris detallats sobre els antecedents familiars de salut (que normalment cobreixen 2-3 generacions).
  - En particular, es controlen les malalties cardiovasculars, els síndromes tumorals, les malalties neurològiques, els trastorns metabòlics i els defectes de desenvolupament congènits.
- **Examen físic**
  - Examen clínic per descartar factors de risc evidents (p. ex., anomalies del desenvolupament).
- **Proves de laboratori**
  - cribratge estàndard de malalties infeccioses (VIH, VHB, VHC, sífilis, CMV).
  - Detecció de portadors de malalties genètiques (p. ex., fibrosi quística, talassèmia, malaltia de Tay-Sachs, SMA).
  - Anàlisi cromosòmica (cariotipatge), si s'escau.
- **Assessorament genètic**
  - Si s'identifiquen factors de risc, s'ofereix assessorament genètic professional als donants i, si s'escau, als futurs pares.
  - L'assessorament ajuda a avaluar els riscos residuals i informa els donants sobre la seva idoneïtat a l'hora de prendre decisions.
- **Criteri d'exclusió del donant**
  - Els donants amb malalties hereditàries conegudes o amb un alt risc de portar malalties genètiques greus queden exclosos del programa de donació.
  - En algunes jurisdiccions, la llei pot permetre excepcions basades en el consentiment informat explícit del receptor, però aquests casos són rars.
- **Historial mèdic i familiar:**
  - Els donants omplen qüestionaris detallats sobre la seva història familiar (normalment cobrint 2–3 generacions).
  - S'avaluen malalties cardiovasculars, síndromes tumorals, trastorns neurològics, malalties metabòliques i malformacions congènites.
- **Exploració física:**
  - Avaluació clínica per descartar factors de risc evidents (p. ex., anomalies del desenvolupament).
- **Proves de laboratori:**

- Cribratge estàndard de malalties infeccioses (VIH, VHB, VHC, sífilis, CMV).
- Detecció de portadors de malalties genètiques (p. ex., fibrosi quística, talassèmia, malaltia de Tay-Sachs, SMA).
- Anàlisi cromosòmica (cariótip), quan sigui necessari.

> **Assessorament genètic:**

- Si s'identifiquen factors de risc, s'ofereix assessorament especialitzat als donants i, si s'escau, als futurs pares.
- L'assessorament ajuda a avaluar els riscos residuals i a prendre decisions sobre l'aptitud del donant.

> **Criteris d'exclusió del donant:**

- Els donants amb malalties hereditàries conegudes o un alt risc de ser portadors de greus trastorns genètics queden exclosos del programa.
- En algunes jurisdiccions, la normativa pot permetre excepcions basades en el consentiment informat del receptor, tot i que aquests casos són poc freqüents.

4.23. DADES DE MENORS I CONSENTIMENT PARENTAL

Els serveis i les activitats comercials del FutureLife Group no estan dirigits a menors d'edat, i no es recullen ni es processen intencionadament les dades personals dels menors d'edat. Els serveis del FutureLife Group estan destinats exclusivament a persones majors d'edat.

En els casos en què determinats serveis estiguin expressament dirigits a menors d'edat, serà obligatori obtenir el consentiment dels pares o tutors legals per a la recollida i el tractament de les seves dades personals, d'acord amb la normativa aplicable. Si el titular de les dades és menor d'edat, cal obtenir el consentiment previ abans de proporcionar cap dada personal a una empresa del grup FutureLife.

4.23.1. VERIFICACIÓ D'EDAT I DOCUMENTACIÓ

Les clíniques han de verificar l'edat del titular de les dades mitjançant documents oficials abans de recollir qualsevol dada personal o de prestar tractament.

Tots els formularis de consentiment han d'estar degudament signats, datats i emmagatzemats de manera segura. Es conserven registres d'auditoria electrònics del consentiment atorgat i de la seva revocació durant el període que exigeixen la normativa i les polítiques internes.

4.23.2. PROCEDIMENTS DE PRESERVACIÓ DE LA FERTILITAT EN MENORS

En certs casos excepcionals, és possible i necessari tractar menors. Aquests casos solen implicar la preservació de la fertilitat en nens amb malalties greus, com el càncer.

A) Cryopreservació de teixit ovàric

La criopreservació de teixit ovàric és el mètode principal per preservar la fertilitat en nenes prepuberals. Aquest procediment implica l'extracció quirúrgica de teixit ovàric que conté ovòcits immadurs, que es congelen per al seu ús posterior. Posteriorment, si la pacient vol tenir fills, el teixit preservat es pot reimplantar al seu cos; els oòcits immadurs també es poden madurar en condicions de laboratori i utilitzar-se més endavant, especialment en procediments de reproducció assistida.

B) Estimulació ovàrica i obtenció d'òvuls madurs

En adolescents que ja han passat la pubertat i han desenvolupat òvuls madurs, és possible dur a terme una estimulació ovàrica controlada i la posterior extracció d'òvuls madurs. Els ovaris s'estimulen amb tractament hormonal i els òvuls obtinguts es conserven mitjançant criopreservació.

4.23.3. Aspectes mèdics i legals

- **Necessitat mèdica:** Els procediments generalment es realitzen quan l'estat de salut o el tractament del menor pot provocar infertilitat.
- **Consentiment:** Sempre es requereix el consentiment tant de la pacient (si és prou madura per entendre la naturalesa del procediment) com dels seus pares/tutors legals; el consentiment ha de ser informat i d'acord amb la normativa aplicable.
- **Recerca:** S'està duent a terme recerca per trobar noves opcions de preservació de la fertilitat per a nens que encara no han arribat a la pubertat.

4.23.4. Dret a revocar el consentiment

Els pares o tutors legals poden retirar el seu consentiment en qualsevol moment. Un cop retirat el consentiment, el tractament de les dades personals del menor quedarà restringit o cancel·lat, llevat que la normativa aplicable exigeixi que el tractament continuï.

4.23.5. Compliment de les normatives nacionals

FutureLife Group ha de garantir el compliment de la normativa nacional de cada país on opera, especialment pel que fa a l'edat mínima per rebre tractament mèdic i l'elegibilitat per als tractaments de fertilitat.

5. COMPLIMENT D'ALTRES REGLAMENTACIONS

5.1. Reglament de Resiliència Cibernètica (CRA)

La Llei de Resiliència Cibernètica (CRA), que va entrar en vigor el 2024 i les principals obligacions de la qual seran plenament aplicables a partir del desembre de 2027, estableix requisits de ciberseguretat per als productes amb elements digitals (PDE), incloent-hi el maquinari i el programari comercialitzats a la Unió Europea. Els fabricants, importadors i distribuïdors d'aquests productes tindran obligacions de ciberseguretat, que inclouen dur a terme avaluacions de riscos i documentar els esforços de compliment.

FutureLife Group ha de preparar-se per complir els requisits de la CRA mitjançant:

- Identificar tots els productes amb elements digitals (PDE), com ara els sistemes de registres de salut electrònics (RSE) i les eines basades en la intel·ligència artificial.
- Garantir el principi de seguretat per disseny.
- Implementació de procediments formalitzats per a la gestió de vulnerabilitats.
- Coordinació del procés de certificació CRA a través del gestor de ciberseguretat.

5.2. Espai Europeu de Dades de Salut (EEDS)

El FutureLife Group ha de comprometre's a implementar l'Espai Europeu de Dades de Salut (EEDS), un marc regulador que entrarà en vigor el 2025 i que té com a objectiu facilitar l'accés, l'intercanvi i l'ús segurs i eficients de les dades de salut, incloses les dades de salut reproductiva, a tots els estats membres de la UE.

5.2.1. Ús Primari de les Dades de Salut

FutureLife garantirà el compliment de les normes de l'EHDS sobre el tractament de dades de salut personals per a l'atenció directa al pacient aplicant els principis següents:

- **Interoperabilitat:** Els sistemes s'han d'actualitzar per donar suport als estàndards tècnics EEDS en els formats de dades, els protocols de comunicació/intercanvi i la coherència semàntica.
- **Drets d'accés:** Els pacients han de poder accedir a les seves dades de salut de manera segura i senzilla, fins i tot a través de fronteres, inclosos els registres relacionats amb la reproducció i la fertilitat.
- **Portabilitat de dades:** S'han de desenvolupar mecanismes que permetin als pacients transferir les seves dades de salut entre les clíniques FutureLife i altres proveïdors autoritzats dins de la UE, d'acord amb el dret a la portabilitat previst en el RGPD.

5.2.2. Ús secundari de dades de salut

FutureLife dona suport a l'ús secundari ètic i legal de les dades de salut per a la recerca, la innovació i la salut pública dins del marc de l'EEDS, sota les condicions següents:

- **Consentiment exprés:** L'ús secundari de dades de fertilitat i de dades genètiques requereix el consentiment informat, documentat i exprés de la persona interessada, tret que hi hagi una altra base jurídica d'acord amb el RGPD i l'EEDS.

- **Minimització i seudonimització:** Només s'utilitzen les dades mínimes necessàries i s'eliminen o seudonimitzen els identificadors per garantir la protecció de les dades personals.
- **Transparència:** Els pacients han de ser informats de manera clara sobre la naturalesa, la finalitat i els destinataris de l'ús secundari de les seves dades, i han de poder revocar el seu consentiment en qualsevol moment. Es proporcionaran mecanismes d'exclusió clars i reversibles, sempre que ho permetin les normatives aplicables.

5.2.3. Format Europeu d'Intercanvi de l'Historial de Salut Electrònic (EEHRXF)

El FutureLife Group està implementant activament el Format Europeu d'Intercanvi de l'Historial Mèdic Electrònic (EEHRXF). L'EEHRXF és la base tècnica de l'EEDS, que garanteix l'ús principal de les dades de salut per a l'atenció directa al pacient i assegura la interoperabilitat entre els Estats Membres. És un estàndard que permet l'intercanvi transfronterer de dades controlat pel pacient dins de l'EEDS. Cobreix l'estructuració i l'intercanvi de categories clau de dades de salut electròniques, com ara resums de pacient, receptes electròniques, resultats de laboratori, imatges i informes mèdics, informes d'alta hospitalària i dades de malalties rares.

5.2.4. Mecanisme de portabilitat de dades

FutureLife permetrà als pacients rebre i transferir les seves dades personals de salut en un format estructurat, d'ús comú i llegible per màquina, d'acord amb el dret a la portabilitat reconegut pel RGPD.

Mecanismes de portabilitat:

- Els pacients poden sol·licitar les seves dades a través de portals segurs o mitjançant una sol·licitud per escrit al DPO.
- Les dades es proporcionaran en formats compatibles amb l'EEDS, com ara HL7 FHIR, CDA o EEHRXF XML.
- Les transferències a altres proveïdors es faran mitjançant interfícies d'API segures o protocols xifrats per a la transmissió de fitxers.

5.2.5. Centres Nacionals EEDS

FutureLife reconeix que cada Estat membre ha d'establir un centre nacional d'EEDS per coordinar l'intercanvi de dades de salut. FutureLife es compromet a:

- Col·laborar amb els centres nacionals EEDS als països on opera.
- Registrar els conjunts de dades elegibles als centres nacionals per a ús secundari, quan es requereixi el consentiment del pacient i l'aprovació reguladora.
- Participar en programes pilot i en processos tècnics d'incorporació dirigits per les autoritats nacionals per provar i validar sistemes compatibles amb EEDS.

5.2.6. Intercanvi transfronterer de dades

- Les dades de salut transfrontereres només es poden reutilitzar amb finalitats de recerca en entorns segurs aprovats per l'organisme nacional d'accés a les dades de salut (HDAB).
- Les institucions sanitàries han de catalogar els conjunts de dades i indicar a l'HDAB tots els drets de propietat intel·lectual i els secrets comercials aplicables.
- L'ús secundari de dades personals amb finalitats de màrqueting o per a qualsevol perfils discriminatori està estrictament prohibit.

5.2.7. IMPLEMENTACIÓ DE LA CIBERSEGURETAT A L'EEDS

L'objectiu de l'Espai Europeu de Dades de Salut és permetre l'intercanvi transfronterer i l'ús secundari de dades de salut amb finalitats de recerca, implicant un nombre més gran d'entitats i un volum més gran de dades, la qual cosa augmenta els possibles punts d'entrada per als actors malintencionats. Donada la sensibilitat de les dades de salut reproductiva, la implementació segura de l'EEDS dins del FutureLife Group requereix un marc de ciberseguretat adaptatiu i robust.

A més del compliment dels documents interns, s'implementaran les mesures organitzatives següents:

- **Prevenció de violacions de la seguretat de les dades personals:** Alinear els procediments amb el **Pla de Resposta a Incidents de Ciberseguretat (FL-CS-OP2)** i garantir la detecció, la notificació i la mitigació oportunes dels incidents que afectin la seguretat de les dades relacionades amb l'EEDS.
- **Implementació de sistemes HCE certificats:** Abans d'utilitzar-los en intercanvis transfronterers, assegureu-vos que tots els sistemes de Historias Clínicas Electròniques **(HCE)** utilitzats a les clíniques estiguin certificats segons l'EEDS pel que fa a la interoperabilitat, la seguretat i la protecció de la privacitat.
- **Intercanvi segur de dades:** Utilitzeu canals de comunicació xifrats i API segures per compartir dades amb els centres nacionals EEDS i amb la infraestructura **HealthData@EU** (nucli central que agrupa conjunts de dades de salut de tota Europa).
- **Col·laboració amb els centres nacionals de l'EEDS:** Col·laborar activament amb els organismes nacionals d'accés a les dades de salut (**HDABs**) per garantir una integració segura i el compliment dels requisits legals.

5.2.8. GESTIÓ I COMPLIMENT NORMATIU

- El rol de coordinador/a d'EEDS (dins de l'equip del DPO) s'establirà per supervisar la implementació, col·laborar amb els centres nacionals d'EEDS i garantir la preparació per al compliment progressiu dels requisits.
- El cap jurídic supervisarà periòdicament els desenvolupaments normatius i garantirà el compliment de les disposicions del RGPD, del SoHO i de l'EEDS.
- Totes les activitats de tractament relacionades amb l'EEDS es documentaran al Registre de tractament de dades personals i estaran subjectes a auditories.

ANNEX A – CATEGORIES DE DADES PERSONALS I FINALITATS DEL TRACTAMENT

Les categories de dades personals recollides, les finalitats per a les quals s'utilitzen i el període durant el qual es conserven es detallen a continuació.

Taula 1: Categories de dades personals i finalitats del tractament

Finalitat del tractament de dades personals	Categories de dades personals	Base jurídica del tractament	Responsable/Responsables conjunts
1. Gestió de sol·licituds d'informació, queixes o suggeriments			
Les sol·licituds es processen per respondre a consultes, resoldre dubtes i atendre les sol·licituds rebudes.	Dades de contacte: nom, adreça de correu electrònic, número de telèfon. Dades de contingut: informació inclosa en la sol·licitud o comunicació.	Consentiment de l'interessat (art. 6.1.a RGPD). Interès legítim del responsable del tractament en el control de qualitat, la resolució de conflictes i la millora del servei (art. 6.1.f RGPD).	Grup FutureLife, juntament amb la clínica corresponent del grup a la qual s'adreça la sol·licitud.
2. Prestació de serveis sanitaris			
Les dades personals es tracten per garantir la prestació adequada dels serveis sanitaris, incloent-hi la gestió de l'historial clínic i el tractament de les dades i dels documents generats en relació amb l'atenció mèdica.	Dades de contacte: nom, adreça de correu electrònic, número de telèfon, adreça postal. Dades d'identificació: número de document d'identitat, número de passaport, sexe/gènere, data de naixement. Dades d'imatge: fotografies, escanejats o altres documents gràfics. Dades de salut i dades de salut reproductiva (categories especials de dades personals): historials clínics, informes mèdics, resultats de diagnòstic, informació sobre tractaments, mostres biològiques, proves de laboratori, dades relacionades amb la fertilitat i altra informació de salut rellevant.	Execució d'un contracte amb l'interessat (art. 6.1.b RGPD). Compliment de les obligacions legals del responsable del tractament (art. 6.1.c RGPD).	La clínica FutureLife pertinent que proporciona serveis sanitaris i actua com a responsable del tractament (o com a responsable conjunt amb el Grup FutureLife, si s'escau).

FINALITAT DEL TRACTAMENT DE DADES PERSONALS	CATEGORIES DE DADES PERSONALS	BASE JURÍDICA DEL TRACTAMENT	RESPONSABLE/RESPONSABLES CONJUNTS
3. Gestió de l'expedient del pacient			
Les dades personals es tracten amb la finalitat de mantenir els historials mèdics dels pacients i garantir la gestió administrativa i organitzativa adequada dels centres sanitaris.	- Dades de contacte: nom, adreça de correu electrònic, número de telèfon, adreça postal, etc. – Dades de salut: antecedents mèdics, diagnòstics, tractaments, al·lèrgies, medicaments, signes vitals i altra informació de salut rellevant sobre el pacient i la seva parella. – Dades d'identificació: número d'identificació personal, número de pacient, número de passaport, sexe/gènere, data de naixement. – Dades administratives: detalls de la cita, informació de facturació, detalls de l'assegurança, formularis de consentiment i registres de comunicació.	Execució d'un contracte amb l'interessat (article 6.1.b del RGPD). Compliment de les obligacions legals del responsable del tractament (article 6.1.c del RGPD). Per a les categories especials de dades personals, el tractament es basa en la prestació d'atenció sanitària d'acord amb la legislació de la UE o de l'Estat membre (article 9.2.h del RGPD).	Clíniques del Grup FutureLife.
4. Gestió de la relació amb el donant			
Les dades personals es tracten amb la finalitat de crear perfils de donants i gestionar la relació contractual entre el donant i la clínica. Això inclou la prestació de l'assistència sanitària necessària i el pagament de la compensació acordada.	– Dades de contacte: nom, adreça de correu electrònic, número de telèfon, adreça postal. – Dades d'identificació: número de document d'identitat, número de passaport, sexe/gènere, data de naixement. – Dades de salut i genètiques (categories especials de dades personals): antecedents mèdics i familiars, resultats de proves, informació sobre fertilitat, proves genètiques i altra informació de salut rellevant. – Dades administratives i financeres: dades sobre la relació contractual, programació de visites, dades de remuneració/compensació, dades de pagament i comptables, formularis de consentiment i registres de comunicacions.	Execució d'un contracte amb l'interessat (article 6.1.b del RGPD). Compliment de les obligacions legals del responsable del tractament (article 6.1.c del RGPD). Per a les categories especials de dades personals, el tractament es basa en la prestació de serveis sanitaris d'acord amb la normativa de la UE o dels Estats membres (article 9.2.h del RGPD).	Clíniques del Grup FutureLife.

FINALITAT DEL TRACTAMENT DE DADES PERSONALS	CATEGORIES DE DADES PERSONALS	BASE JURÍDICA DEL TRACTAMENT	RESPONSABLE/RESPONSABLES CONJUNTS
5. Referència de pacient			
Les dades personals es processen i s'envien a la clínica recomanada per garantir que el tractament necessari es pugui proporcionar en un centre sanitari alternatiu a petició del pacient.	– Dades de contacte: nom, adreça de correu electrònic, número de telèfon, adreça postal. – Dades d'identificació: número de document d'identitat, número de passaport, sexe/gènere, data de naixement.	Consentiment de l'interessat per a la transferència de dades personals a altres clíniques dins del FutureLife Group (article 6.1.a del RGPD).	Clíniques del Grup FutureLife.
6. Finalitats administratives i de gestió internes			
Les dades personals es tracten amb la finalitat de garantir la correcta gestió administrativa i organitzativa de les clíniques, així com per a finalitats estadístiques internes.	– Dades de contacte: nom, adreça de correu electrònic, número de telèfon. – Dades administratives: detalls de les reunions, informació de facturació, dades de l'assegurança i registres de comunicació. – Dades estadístiques internes.	L'interès legítim del responsable del tractament en la gestió i el control de les activitats organitzatives i les relacions comercials (article 6.1.f del RGPD).	Grup FutureLife juntament amb la clínica corresponent del grup implicada en l'activitat de tractament (codirectors).
7. Finalitat de l'enquesta			
Les dades personals es tracten amb la finalitat d'enviar enquestes de qualitat i satisfacció relacionades amb els serveis prestats i l'atenció dispensada.	– Dades de contacte: nom, adreça de correu electrònic, número de telèfon. –Dades estadístiques internes.	Interès legítim en el control de qualitat, l'adaptació d'activitats i el desenvolupament de productes i serveis millorats (art. 6, paràgraf 1, lletra f del RGPD).	El Grup FutureLife juntament amb la clínica corresponent del grup a la qual s'adreça la sol·licitud.
8. Finalitats de màrqueting. Enviament de missatges comercials i butlletins informatius.			

FINALITAT DEL TRACTAMENT DE DADES PERSONALS	CATEGORIES DE DADES PERSONALS	BASE JURÍDICA DEL TRACTAMENT	RESPONSABLE/RESPONSABLES CONJUNTS
Les dades personals es tracten amb la finalitat de gestionar les subscripcions als serveis de notificació i comunicació (p. ex., butlletins informatius) i de proporcionar informació sobre serveis o ofertes especials.	– Dades de contacte: nom, adreça de correu electrònic, número de telèfon.	El consentiment de l'interessat atorgat mitjançant la subscripció (article 6.1.a del RGPD). En cas d'existir una relació contractual, l'interès legítim del responsable del tractament en l'enviament d'informació sobre productes i serveis similars (article 6.1.f del RGPD).	El Grup FutureLife, juntament amb la clínica corresponent del grup a la qual s'envien les comunicacions comercials.
9. Científica i de recerca			
Les dades personals es tracten amb finalitats científiques i de recerca per tal d'ampliar el coneixement sobre la fertilitat i les condicions de salut reproductiva, millorar els mètodes de tractament de reproducció assistida i donar suport a la formació professional en aquest àmbit.	- Dades mèdiques i de salut: historial mèdic, resultats de diagnòstic, informació sobre tractaments, signes vitals, dades de salut mental/conductual, dades de salut reproductiva, etc.	Interès legítim en dur a terme investigació científica en l'àmbit de la fertilitat i la salut reproductiva (article 6.1.f del RGPD). Si les dades no s'anonimitzen, es requereix el consentiment explícit dels interessats (article 6.1.a del RGPD).	El Grup FutureLife, juntament amb la clínica pertinent del Grup a la qual es refereix la investigació.
10. Manteniment i anàlisi del lloc web			

FINALITAT DEL TRACTAMENT DE DADES PERSONALS	CATEGORIES DE DADES PERSONALS	BASE JURÍDICA DEL TRACTAMENT	RESPONSABLE/RESPONSABLES CONJUNTS
Les dades personals es tracten amb la finalitat de garantir i optimitzar el rendiment del sistema, avaluar la seguretat i l'estabilitat, i oferir publicitat personalitzada basada en el comportament de l'usuari. Això s'aconsegueix mitjançant l'ús de la tecnologia de galetes. Per a més informació detallada, consulteu la Política de galetes.	- L'adreça IP del dispositiu connectat a Internet. - Data i hora d'accés. - L'URL de referència, el tipus de navegador i el sistema operatiu. - El nom del proveïdor d'accés.	Per a les galetes que no són necessàries: consentiment atorgat a través de la configuració/preferències de galetes (article 6.1.a del RGPD). Per a les galetes tècniques i necessàries: interès legítim en garantir la seguretat, l'estabilitat i la usabilitat del lloc web (article 6, paràgraf 1, lletra f, del RGPD).	Grup FutureLife.
11. Compliment de les obligacions legals			
Les dades personals es tracten amb la finalitat de complir amb les obligacions legals, incloses les relatives a la protecció de dades personals, les obligacions fiscals i comptables, la salut i altres normatives legals aplicables. Les dades també es poden posar a disposició de les forces de l'ordre, els tribunals, els organismes governamentals o altres autoritats públiques si ho requereix la llei.	– Dades de contacte: nom, adreça de correu electrònic, número de telèfon. - Dades de contingut: informació continguda en documents i comunicacions relacionats amb el compliment de requisits legals o normatius.	Compliment de les obligacions legals (article 6.1.c del RGPD).	Grup FutureLife, juntament amb la clínica corresponent del grup a la qual es refereix l'obligació i el tractament de les dades personals.

ANNEX B – MATRIU RACI

Aquesta matriu RACI descriu els rols i les responsabilitats relacionats amb el compliment de la Política de Protecció de Dades Personals entre les parts interessades clau. A continuació, es mostra una llegenda que explica el significat de cada designació utilitzada a la matriu RACI:

- **R (Responsible):** Persona que ha de dur a terme directament la tasca o activitat.
- **A (Accountable):** Persona que ha d'assumir la responsabilitat final de l'execució correcta i completa de la tasca.
- **C (Consulted):** Persona a qui cal consultar per obtenir informació, opinions o coneixements especialitzats abans de completar la tasca.
- **I (Informed):** Persona a qui s'ha de mantenir informada del progrés i les decisions preses, però que no participa activament en l'execució de la tasca.

Taula 2: Matriu RACI

Activitat / Rol	DPO	CTO	Cap del Departament Jurídic	Responsable de Seguretat Local	Departament de Recursos Humans	Treballadors	Proveïdors	Director/a de Ciberseguretat	Propietari de negoci (BO)	Propietari funcional (FO)
Supervisar el compliment del RGPD	R	A	A	C	I	I	I	C	A	C
Punt de contacte amb les autoritats de supervisió	R	I	I	I	I	I	I	I	I	I
Formació i consultoria en l'àmbit de la protecció de dades personals	R	C	C	C	C	I	I	C	I	C
Auditories i avaluacions internes	R	A	C	C	I	I	C	C	C	C
Avaluació d'impacte en la protecció de dades (DPIA)	A	I	C	C	I	I	C	C	R	R
Registres d'activitats de tractament	R	I	C	C	I	I	C	I	C	R

Aprovació de la política i seguiment posterior	I	A	R	I	I	I	I	C	C	I
Garanties tècniques per a les dades personals	C	I	R	C	I	I	R	A	C	C
Resposta a incidents i a violacions de la seguretat de les dades personals	C	I	R	C	C	I	C	A	I	I
Compliment local del RGPD	I	I	R	R	I	I	I	C	R	R
Tractament de les dades personals dels empleats	I	I	I	I	R	I	I	I	R	R
Formació del personal	C	I	C	R	R	R	I	C	I	C
Tractament responsable de les dades personals	I	I	I	I	I	R	R	C	R	R
Tractament contractual de dades personals	I	I	I	I	I	I	R	C	R	C
Proves de penetració i anàlisi de riscos	I	C	C	I	I	I	I	R	C	C
Xifratge i control d'accés	I	I	C	I	I	I	I	R	C	C

FutureLife

Política de protecció de dades personals

SOBRE FUTURELIFE

Des que es va fundar el FutureLife Group el 2014, hem continuat creixent cada any. Avui tenim més de 50 clíniques en 16 països europeus, operades per més de 1.500 membres qualificats de l'equip i 600 metges. Les nostres clíniques ofereixen tractaments integrals de fertilitat, incloent-hi proves genètiques, proves immunològiques i altres anàlisis complementàries.

El nostre objectiu principal és oferir una atenció de qualitat i tractaments eficaços per crear infants sans i famílies felices. Invertiem contínuament en les nostres clíniques, la investigació i la formació. Això ens permet oferir als nostres equips coneixements especialitzats, estabilitat financera, bones condicions laborals i una remuneració competitiva.