FutureLife

SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI

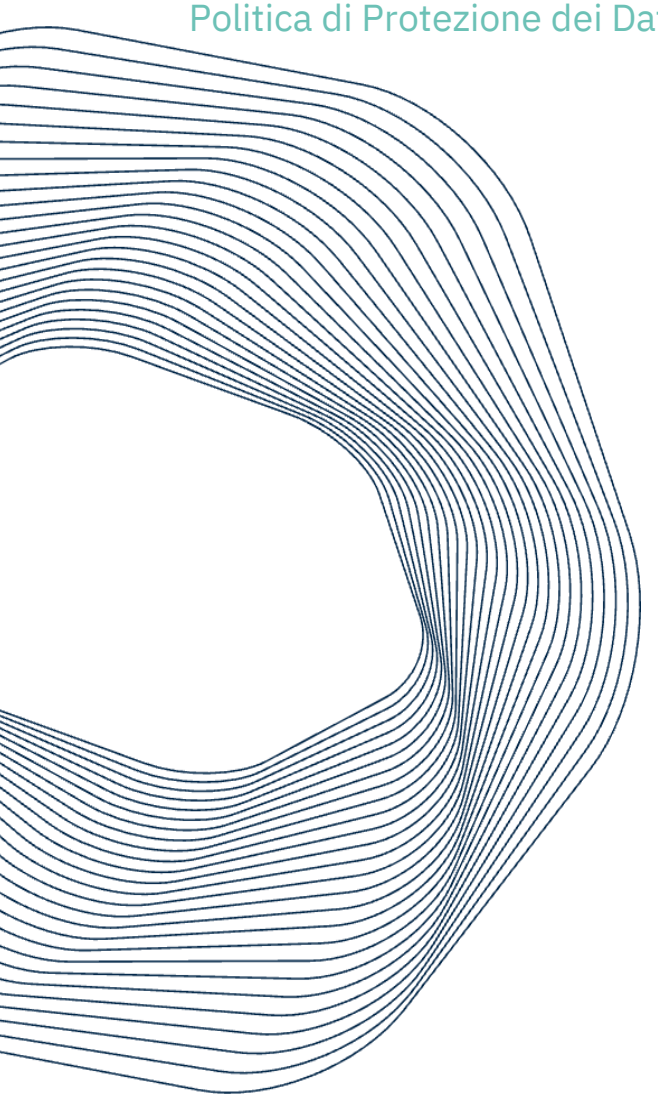
POLITICA DI PROTEZIONE DEI DATI PERSONALI

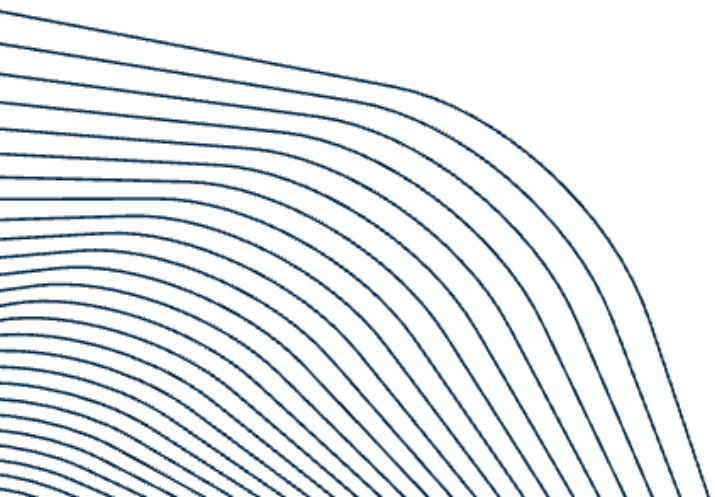
FUTURELIFE A.S.

Versione: 1.0
Data: 15-09-2025
Classificazione: INTERNO

FutureLife

Politica di Protezione dei Dati Personali





FutureLife

Politica di Protezione dei Dati Personali

Titolo del documento:	Politica di Protezione dei Dati Personali	FutureLife a.s.
Sottotitolo:	Sistema di Gestione della Protezione dei Dati Personali	Na příkopě 859/22
Persona di contatto 1:	Maroš Zuba	Nové Město, 110 00
Dipartimento:	Digitale	Praga 1
Contatto Persona 2:	Ilja David	Repubblica Ceca
Dipartimento:	Digitale	
ID del documento:	FL-DP-P1	
Data di emissione:	15-09-2025	

Contenuto del documento:

La Politica di Protezione dei Dati Personali descrive come il gruppo FutureLife tratta i dati personali raccolti dai sistemi interni, dalle piattaforme digitali e da altre fonti pertinenti all'interno dell'organizzazione. Questa Politica è vincolante per l'intera organizzazione, inclusi tutti i dipendenti, collaboratori, società controllate e partner esterni che gestiscono dati personali. La Politica è conforme al GDPR e alle altre leggi applicabili, nonché ai requisiti della norma ISO/IEC 27701, che estende la norma ISO/IEC 27001 integrando ulteriori controlli e linee guida per la gestione dei dati personali e delle informazioni relative alla protezione dei dati.

Redatto da:	**Verificato da:**	**Approvato da:**
Ilja David	Maroš Zuba	Ignacio Couto
Responsabile della Sicurezza Informatica	Responsabile dell'Ufficio Legale	CTO
Digital	Digital	Digital
FutureLife a.s.	FutureLife a.s.	FutureLife a.s.

Parole chiavi:

Politica sulla Privacy, Tecnologia dell'Informazione, Tecnologia Operativa, Protezione, GDPR

Riservatezza del documento:

☐ PUBBLICO. Dati disponibili pubblicamente relativi alle attività quotidiane dell'organizzazione o a processi noti.

☒INTERNO. Dati riservati riguardanti la gestione ordinaria delle attività aziendali o dei processi interni.

☐ RISERVATO. Dati relativi ad attività strategiche, contratti, informazioni finanziarie, dati personali e dati sanitari.

MONITORAGGIO DELLE MODIFICHE

Versione	Data	Motivo del cambiamento	Redatto da	Verificato da	Approvato da
1.0	15.09.2025	Prima Edizione	Ilja David	Maroš Zuba	Ignacio Couto

INDICE

1. INFORMAZIONI INTRODUTTIVE

1.1. SCOPO

La presente Politica di Protezione dei Dati Personali (di seguito anche "Politica") stabilisce un quadro uniforme per garantire la protezione dei dati personali all'interno di FutureLife a.s. e di tutte le società affiliate appartenenti allo stesso gruppo societario (di seguito "Gruppo FutureLife").

Il suo scopo è definire principi, ruoli e responsabilità relativi al trattamento dei dati personali in conformità alle normative applicabili, incluso il GDPR e altre disposizioni nazionali pertinenti.

1.2. AMBITO DI APPLICAZIONE

A presente Politica si applica a tutti i processi, le tecnologie e i soggetti del Gruppo FutureLife che trattano dati personali, garantendo un approccio uniforme alla protezione dei dati personali, alla sicurezza delle informazioni e all'esercizio dei diritti degli interessati.

1.3. DOCUMENTI CORRELATI

In questa sezione sono elencati i documenti interni correlati che supportano e integrano la Politica di Protezione dei Dati Personali:

- **FL-CS-P1 – Politica di Sicurezza Informatica (Cybersecurity Policy):** quadro per la gestione della sicurezza informatica dell'organizzazione.
- **FL-CS-S1 – Sicurezza Informatica degli Utenti Finali (End User Cybersecurity):** standard per il comportamento sicuro e la responsabilità degli utenti finali.
- **FL-CS-S2 – Sicurezza Informatica dei Fornitori (Supplier Cybersecurity):** standard per la valutazione e gestione dei rischi di sicurezza informatica legati ai fornitori terzi.
- **FL-CS-S6 – Piano di Continuità Operativa (Business Continuity Plan):** standard per garantire la resilienza operativa e il ripristino in caso di interruzioni.
- **FL-CS-OP2 – Piano di Risposta agli Incidenti Informatici (Cybersecurity Response Plan):** procedura per rilevare, gestire e risolvere incidenti di sicurezza informatica.
- **FL-CS-OP3 – Ciclo di Vita dello Sviluppo Sicuro del Sistema (Secure System Development Lifecycle):** integrazione della sicurezza in tutto il processo di sviluppo.
- **FL-CS-OP7 – Comunicazione degli Incidenti (Incident Communication):** procedura per la comunicazione interna ed esterna in caso di incidenti informatici.
- **FL-CS-OP09 – Nuovi Requisiti di Sicurezza del Sistema (New System Security Requirements):** specifiche dei requisiti di sicurezza per la progettazione e implementazione di nuovi sistemi.
- **FL-CS-S7 – Standard di Sicurezza per l'IA (AI Security Standard):** standard per l'uso sicuro degli strumenti di intelligenza artificiale, inclusa la protezione dei dati aziendali e delle infrastrutture.
- **FL-CS-S4 – Audit Interno (Internal Audit):** requisiti e responsabilità per l'audit interno come parte del sistema di gestione della sicurezza informatica.

1.4. TERMINI

TERMINE	DEFINIZIONE
Titolare del trattamento	Persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali
Responsabile del trattamento	Soggetto che tratta i dati personali per conto del titolare
Dati sensibili	Informazioni riservate che, se divulgate, potrebbero causare danni, discriminazioni o rischi per la sicurezza nazionale (es. dati sanitari personali – PHI, dati finanziari, informazioni identificabili – PII, segreti commerciali)
Categorie particolari di dati	Dati personali sensibili come dati sanitari, genetici, biometrici o relativi all'origine razziale o etnica
Consenso	Manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato
Cookie	Piccoli file di testo scaricati e memorizzati sul dispositivo dell'utente contenenti informazioni limitate
Anonimizzazione	Processo di rimozione o modifica degli identificatori personali per rendere impossibile l'identificazione dell'individuo
Contitolari	Due o più soggetti che determinano congiuntamente le finalità e i mezzi del trattamento
Dati personali	Qualsiasi informazione relativa a persona fisica identificata o identificabile
Dati sanitari personali	Informazioni mediche riservate che identificano l'individuo e riguardano la sua salute fisica o mentale, la prestazione di cure o il pagamento di servizi sanitari
Uso primario dei dati sanitari	Utilizzo delle informazioni raccolte direttamente nel corso della prestazione sanitaria
Uso secondario dei dati sanitari	Utilizzo delle informazioni raccolte per finalità diverse dalla cura diretta (es. ricerca, sanità pubblica, pianificazione dei servizi, miglioramento della qualità)

1.5. ACRONIMI

ACRONIMO	SIGNIFICATO
AI	Intelligenza Artificiale (Artificial Intelligence)
CRA	Regolamento UE sulla resilienza informatica (EU Cyber Resilience Act)
DPA	Allegato sulla protezione dei dati (Data Privacy Annexe)
DPIA	Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment)
DPO	Responsabile della protezione dei dati (Data Protection Officer)
SEE (EEA)	Spazio Economico Europeo (European Economic Area, EEA)
EEHRXF	Formato europeo per lo scambio di cartelle cliniche elettroniche
EHDS	Spazio europeo dei dati sanitari
EHR	Cartella clinica elettronica
GDPR	Regolamento generale sulla protezione dei dati
HDAB	Autorità per l'accesso ai dati sanitari
NIS2	Direttiva sulla sicurezza delle reti e delle informazioni
PDE	Prodotto con elementi digitali
PHI	Informazioni sanitarie personali e dati sensibili
PII	Informazioni personali identificabili
RACI	Matrice di assegnazione delle responsabilità
SAE	Eventi avversi gravi
SAR	Reazioni avverse gravi
SCCs	Clausole contrattuali standard
SoHO	Regolamento sulle sostanze di origine umana

2. POLITICA DI PROTEZIONE DEI DATI PERSONALI

Il Gruppo FutureLife si impegna a rispettare la privacy e a garantire la sicurezza dei dati personali trattati in conformità al Regolamento Generale sulla Protezione dei Dati (GDPR), alla Direttiva NIS2, allo Spazio Europeo dei Dati Sanitari (European Health Data Space, EHDS), al Regolamento UE sulle Sostanze di Origine Umana (Substances of Human Origin, EU SoHO Regulation), al Piano d'Azione UE per la Sicurezza Informatica fino al 2025, all'Artificial Intelligence Act (AI Act), al Cyber Resilience Act (CRA) e alle normative nazionali vigenti in materia di protezione dei dati personali. La presente Politica di Protezione dei Dati Personali contiene informazioni essenziali relative ai dati personali, alle modalità di raccolta, utilizzo e protezione, e deve pertanto essere letta con attenzione.

2.1. IDENTIFICAZIONE DEL TITOLARE DEL TRATTAMENTO

I dati personali sono trattati, a seconda delle circostanze specifiche, da FutureLife e/o dalle società controllate come titolari del trattamento per le finalità descritte nella presente Politica.

2.2. FUTURELIFE COME TITOLARE DEL TRATTAMENTO

I dati personali sono raccolti e trattati dal Gruppo FutureLife in qualità di titolare del trattamento nell'ambito delle proprie attività organizzative, ad esempio per l'iscrizione alla newsletter o per la richiesta di informazioni tramite moduli di contatto. I dati identificativi di FutureLife, in qualità di titolare del trattamento, sono i seguenti:

2.2.1. SOCIETÀ CONTROLLATE DEL GRUPPO FUTURELIFE COME TITOLARI DEL TRATTAMENTO

Il Gruppo FutureLife è considerato titolare del trattamento dei dati personali trattati nell'ambito delle proprie attività operative, inclusa la prestazione di servizi sanitari, la gestione della documentazione clinica dei pazienti e altre attività aziendali legittime. La società controllata che gestisce la struttura sanitaria o la clinica e che raccoglie e tratta i dati personali per le finalità sopra indicate è considerata titolare di tali dati. L'elenco completo delle società controllate del Gruppo FutureLife e delle relative cliniche è disponibile su richiesta.

La documentazione sanitaria è trattata esclusivamente dalla clinica del Gruppo FutureLife che fornisce i servizi sanitari. FutureLife non ha in alcun caso accesso a informazioni sanitarie chiaramente identificabili.

2.2.2. FUTURELIFE E LE SOCIETÀ CONTROLLATE COME CONTITOLARI DEL TRATTAMENTO

In base alla natura delle attività, il Gruppo FutureLife può agire congiuntamente alle proprie società controllate come contitolare del trattamento dei dati personali degli utenti, in particolare per finalità di marketing, invio di comunicazioni commerciali relative al Gruppo FutureLife, indagini di mercato e di soddisfazione, nonché per altre funzioni operative e organizzative a livello di gruppo.

2.3. GESTIONE DEGLI INCIDENTI DI SICUREZZA NEL FUTURELIFE GRUPPO

Gli incidenti relativi alla protezione dei dati personali sono gestiti in conformità al **Piano di Risposta agli Incidenti Informatici** (**FL-CS-OP2**) del Gruppo FutureLife.

Tale piano definisce le procedure per l'identificazione tempestiva, la valutazione, la segnalazione e la risoluzione degli incidenti di sicurezza che possono compromettere la protezione dei dati personali.

L'obiettivo di tali procedure è ridurre al minimo l'impatto sugli interessati, garantire l'adozione di misure correttive adeguate e adempiere agli obblighi di legge, inclusa l'eventuale notifica alle autorità di controllo e agli interessati.

3. RUOLI E RESPONSABILITÀ

Questa sezione definisce i ruoli chiave all'interno del Gruppo FutureLife e le relative responsabilità nella protezione dei dati personali.

Per una panoramica dettagliata della distribuzione dei ruoli e delle responsabilità nell'attuazione della presente Politica di Protezione dei Dati Personali, è allegata una matrice RACI informativa nell'Appendice B.

3.1. RESPONSABILE DELLA PROTEZIONE DEI DATI (DATA PROTECTION OFFICER, DPO)

Dal punto di vista della protezione dei dati, il **Data Protection Officer** (DPO) deve:

- monitorare la conformità ai principi e ai requisiti del GDPR e alle altre normative applicabili in materia di protezione dei dati personali;
- fungere da punto di contatto con le autorità di controllo competenti;
- fornire linee guida metodologiche e formazione sulle questioni relative alla protezione dei dati personali;
- effettuare audit interni e valutazioni sul trattamento dei dati personali;
- fornire consulenza in merito alle valutazioni d'impatto sulla protezione dei dati (Data Protection Impact Assessment, DPIA);
- riesaminare e aggiornare il registro dei dati personali;
- aggiornare la documentazione relativa alle attività di trattamento, inclusa la mappatura dei processi e i relativi diagrammi;
- mantenere e gestire i registri delle attività di trattamento.

3.2. CHIEF TRANSFORMATION OFFICER (CTO)

Dal punto di vista **della privacy, il** Chief Transformation Officer (CTO) deve:

- approvare e supervisionare l'implementazione della Politica di Protezione dei Dati Personali;
- guidare iniziative strategiche relative alla protezione dei dati in tutta l'organizzazione;
- garantire la coerenza delle procedure di protezione dei dati con gli obiettivi di trasformazione aziendale;
- promuovere la collaborazione interdisciplinare sulle questioni di privacy;
- assicurare l'attuazione di programmi di formazione e sensibilizzazione dei dipendenti;
- sostenere l'applicazione di misure disciplinari adeguate in caso di violazioni delle norme sulla protezione dei dati.

3.3. RESPONSABILE DELL'UFFICIO LEGALE (HEAD OF LEGAL)

Il **Head of Legal**, che ricopre il ruolo di Group Data Protection Officer (Group DPO), deve:

- implementare e mantenere misure tecniche di sicurezza per la protezione dei dati personali;
- gestire le violazioni della sicurezza dei dati e gli incidenti di cybersecurity;
- supportare i processi di conservazione e cancellazione dei dati personali;
- collaborare con il DPO locale per garantire la conformità a livello di sistema;
- effettuare test di sicurezza, penetration test e analisi dei rischi;
- fornire formazione ai dipendenti sulla sicurezza informatica e sulla gestione sicura dei dati personali;

- collaborare con fornitori esterni per garantire la sicurezza dei sistemi e dei flussi di dati;
- assicurare l'adozione di misure tecniche come crittografia e controllo degli accessi.

3.4. Local Security Officer

Dal punto di vista della privacy, **Local Security Officer** deve:

- garantire la conformità locale alla Politica di Protezione dei Dati Personali e al GDPR;
- supervisionare la gestione sicura della documentazione sanitaria e di altri dati sensibili;
- formare il personale della clinica sulle procedure di protezione dei dati;
- segnalare gli incidenti relativi ai dati personali alla gestione centrale;
- ricoprire il ruolo di Local DPO, se previsto dalla direzione;
- coordinare con il DPO e il responsabile IT i rischi a livello di clinica.

3.5. Responsabile della Sicurezza Informatica (Cybersecurity Manager)

Dal punto di vista della privacy, il **Cybersecurity Manager** deve:

- progettare, implementare e mantenere misure di sicurezza per la protezione dei dati personali;
- monitorare le minacce informatiche e le vulnerabilità che possono compromettere i dati personali;
- coordinare le risposte agli incidenti di sicurezza in collaborazione con il DPO locale e il responsabile legale.

3.6. Business Owner

Dal punto di vista della privacy, **un Business Owner** (BO) deve:

- garantire che le attività di trattamento dei dati personali nella propria area siano conformi alla Politica e alle normative vigenti (es. GDPR);
- collaborare con il DPO per identificare e mitigare i rischi legati alla protezione dei dati;
- assicurare che fornitori e sistemi rispettino i requisiti di protezione dei dati e sicurezza informatica.
- È responsabile dell'uso legittimo dei dati personali nelle applicazioni e nei servizi di propria competenza.

3.7. Functional Owner

Dal punto di vista della privacy, **un Functional Owner** (FO) deve:

- garantire la conformità operativa ai requisiti di protezione dei dati nella propria area funzionale;
- guidare la realizzazione delle DPIA in collaborazione con il BO e il DPO;
- assicurare che le procedure di trattamento siano documentate e conformi agli standard interni;
- supportare audit, revisioni e aggiornamenti dei sistemi che trattano dati personali;
- avviare e supervisionare la DPIA per nuove o modificate attività di trattamento;
- coordinare con IT e ufficio legale l'implementazione delle misure tecniche e organizzative.

3.8. UFFICIO RISORSE UMANE

Dal punto di vista della protezione dei dati, le risorse umane devono:

- garantire il trattamento legittimo dei dati dei dipendenti;
- gestire la protezione dei dati durante assunzione, onboarding e offboarding;
- assicurare la riservatezza e la conservazione sicura dei registri del personale.

3.9. TUTTI I DIPENDENTI

Dal punto di vista della privacy, tutti i dipendenti devono:

- rispettare l'Informativa e le procedure interne sulla privacy;
- partecipare a corsi obbligatori nel campo della protezione dei dati personali e della cybersecurity,
- segnalare prontamente qualsiasi sospetta violazione o uso improprio di dati personali;
- Gestisci i dati personali in modo responsabile e in conformità con i principi di sicurezza.

3.10. FORNITORI ESTERNI E TERZE PARTI

Dal punto di vista della privacy , tutti i fornitori terzi devono:

- trattare i dati personali esclusivamente secondo le istruzioni di FutureLife;
- rispettare tutti gli obblighi contrattuali in materia di protezione dei dati;
- adottare e mantenere misure tecniche e organizzative adeguate;
- sottoscrivere accordi di riservatezza e contratti di trattamento dei dati (DPA);
- collaborare durante audit, controlli e verifiche di conformità.

4. GESTIONE DEI DATI PERSONALI

Alcuni servizi sono accessibili senza fornire dati personali. Tuttavia, per utilizzare funzionalità come la registrazione, l'iscrizione alla newsletter o la comunicazione personalizzata, è necessario fornire i dati personali.

I dati personali possono essere raccolti:

- direttamente, ad esempio tramite moduli, chiamate o e-mail;
- indirettamente, tramite cookie e altre tecnologie di tracciamento.

I campi obbligatori sono contrassegnati da un asterisco (*); senza la loro compilazione non è possibile fornire il servizio.

Informazioni dettagliate sulle categorie di dati personali, sulle finalità del trattamento e sui tempi di conservazione sono riportate nell 'Allegato A: Categorie di dati personali e scopi di trattamento.

4.1. SICUREZZA

La sicurezza e la riservatezza dei dati personali nel Gruppo FutureLife sono garantite attraverso un insieme di misure tecniche e organizzative indicate nella **Politica di Sicurezza Informatica** (**FL-CS-P1**).

Tali misure sono state adottate per prevenire perdita, uso improprio, accesso non autorizzato o altro trattamento illecito dei dati personali, in conformità al GDPR e alle normative nazionali applicabili.

L'interessato è altresì responsabile della protezione dei propri dati personali e deve agire con prudenza nella condivisione di informazioni e contenuti.

Il Gruppo FutureLife non monitora i contenuti o le informazioni che l'interessato decide di condividere con altri e non è responsabile delle conseguenze di tale condivisione.

4.2. COOKIE

Molte informazioni indicate nella presente Politica sono raccolte tramite cookie. I cookie sono piccoli file di testo contenenti informazioni limitate, scaricati e memorizzati sul dispositivo dell'utente (computer, smartphone o tablet) durante la visita al sito web. I cookie sono utilizzati principalmente per memorizzare le impostazioni dell'account, la lingua e il Paese preferiti, nonché per analizzare il comportamento degli utenti sul sito e mostrare pubblicità personalizzata sul sito o su siti di terze parti. Quando richiesto dalla legge, è necessario il consenso dell'utente per l'uso dei cookie.

Ulteriori informazioni sull'uso dei cookie e sulle modalità di gestione o disattivazione sono disponibili nella nostra Cookie Policy.

4.3. DIRITTI DEGLI UTENTI INTERESSATI RELATIVI ALLA PROTEZIONE DEI DATI PERSONALI

I soggetti interessati i cui dati personali vengono trattati possono esercitare i loro diritti ai sensi della legge applicabile in qualsiasi momento, incluso il diritto di accesso, rettifica, restrizione del trattamento, cancellazione, obiezione e portabilità dei dati personali:

I seguenti ruoli sono responsabili della gestione e gestione delle richieste per l'esercizio dei diritti dei soggetti in dato:

- **DPO (Responsabile della Protezione dei Dati):** gestisce e verifica tutte le richieste di esercizio dei diritti.

- **Responsabile Ufficio Legale:** garantisce la conformità normativa e supporta nei casi complessi.
- **Security Officer Locale:** coordina l'implementazione locale delle misure di sicurezza e la reportistica.
- **Ufficio Risorse Umane:** gestisce le richieste relative ai dati dei dipendenti.
- **Business Owner:** assicura la corretta gestione delle richieste per i sistemi di propria competenza.
- **Functional Owner:** supporta l'esecuzione tecnica, inclusi i blocchi dei dati quando possibile.

Dopo la ricezione di una richiesta valida:

- il trattamento dei dati interessati deve essere immediatamente sospeso;
- i dati devono essere bloccati per tutta la durata della verifica;
- in caso di opposizione, i dati non possono essere ulteriormente trattati, salvo dimostrazione di motivi legittimi prevalenti da parte del titolare.

Le richieste devono essere inviate via e-mail a dpo@futurelifegroup.com con oggetto "Interessato – Protezione dei Dati" e chiara indicazione del diritto esercitato.

Gli interessati hanno inoltre il diritto di presentare reclamo all'autorità di controllo competente se ritengono che i loro dati siano trattati in violazione della normativa.

4.4. TIPI E ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONALI

Di seguito sono elencati i principali tipi e attività di trattamento dei dati personali effettuati dal Gruppo FutureLife, in conformità al GDPR e alle normative nazionali:

- **Gestione dei dati dei pazienti:** raccolta, conservazione e trattamento dei dati personali e sanitari per fornire servizi sanitari, gestire la documentazione clinica e adempiere agli obblighi di legge.
- **Pianificazione degli appuntamenti:** trattamento dei dati di contatto e identificativi per la gestione delle prenotazioni e la comunicazione con i pazienti.
- **Comunicazione e assistenza clienti:** utilizzo dei dati personali per rispondere a richieste e fornire supporto.
- **Marketing e comunicazioni commerciali:** trattamento dei dati di contatto per invio di newsletter, materiale promozionale e sondaggi di soddisfazione, sempre previa acquisizione del consenso.
- **Monitoraggio dei siti web e cookie**: raccolta di dati tramite cookie e tecnologie simili per analisi dell'uso del sito e personalizzazione dei contenuti.
- **Recruiting e gestione HR:** trattamento dei dati dei candidati e dei dipendenti per assunzione, onboarding, calcolo stipendi e valutazione delle performance.
- **Conformità legale e regolamentare:** trattamento dei dati necessari per adempiere agli obblighi di legge, inclusi archiviazione, audit e segnalazioni alle autorità.
- **Assicurazioni e fatturazione:** condivisione dei dati con assicurazioni e soggetti di fatturazione per la gestione dei sinistri e dei pagamenti.
- **Operazioni IT e sicurezza:** utilizzo dei dati nei log di sistema, gestione degli accessi, crittografia, monitoraggio e gestione degli incidenti di sicurezza.
- **Ricerca e analisi statistica:** uso di dati anonimizzati o pseudonimizzati per ricerca scientifica e analisi interne.
- **Gestione dei diritti degli interessati:** trattamento dei dati per gestire richieste di accesso, rettifica, cancellazione e altri diritti previsti dal GDPR.

- **Gestione fornitori e partner:** condivisione dei dati con terze parti sulla base di obblighi contrattuali e garanzie.
- **Trasferimenti transfrontalieri:** trasferimento di dati personali verso Paesi extra SEE solo con adeguate garanzie e in conformità ai meccanismi legali applicabili.

4.5. Registro dei Dati Personali

Il Registro dei Dati Personali rappresenta l'archivio centrale di tutte le attività di trattamento dei dati personali effettuate dal Gruppo FutureLife. Garantisce trasparenza, responsabilità e conformità al GDPR. Il registro documenta la gestione legittima, sicura ed etica dei dati personali, inclusi quelli sensibili o appartenenti a categorie particolari.

4.5.1. Ambito

Nel Registro dei Dati Personali sono incluse tutte le categorie di dati trattati dal Gruppo FutureLife, tra cui:

- documentazione sanitaria del paziente e del partner;
- dati genetici, biometrici e di laboratorio;
- dati relativi alla salute riproduttiva e ai trattamenti;
- dati amministrativi, finanziari e assicurativi;
- informazioni su dipendenti e fornitori;
- dati trattati tramite terze parti (es. laboratori, magazzini o fornitori IT).

4.5.2. Responsabilità

- Il DPO è responsabile della gestione, del controllo e dell'aggiornamento del Registro dei Dati Personali.
- Le parti interessate devono informare il DPO di tutte le nuove o modificate attività di trattamento.
- Il DPO garantisce che il registro sia accurato, completo e aggiornato, e che sia disponibile per la revisione da parte dell'autorità di controllo (DPA) su richiesta.

4.5.3. Contenuto

Per ogni attività di trattamento, il registro deve includere:

- **Dati del titolare:** nome, indirizzo e contatti della clinica;
- **Finalità del trattamento:** erogazione di cure cliniche, diagnostica, ricerca (se applicabile), fatturazione o attività amministrative;
- **Categorie di interessati:** pazienti, partner, donatori, bambini nati da trattamenti, dipendenti e fornitori;
- **Categorie di dati personali:** dati identificativi, di contatto, anamnesi, dati sulla salute riproduttiva, dati genetici, risultati di laboratorio, dati di fatturazione e assicurativi;
- **Categorie particolari di dati:** informazioni esplicitamente sensibili, in particolare dati genetici e riproduttivi;
- **Destinatari dei dati:** team interni, laboratori, ospedali, fornitori di storage, assicurazioni e autorità di regolamentazione;
- **Trasferimenti verso Paesi terzi:** dettagli su eventuali trasferimenti extra SEE, incluse le garanzie di sicurezza e legali adottate (vedi paragrafo 4.8);

- **Tempi di conservazione:** periodi definiti in base a requisiti medici, legali e regolamentari (vedi paragrafo 4.9);
- **Misure di sicurezza:** controlli implementati (es. crittografia, pseudonimizzazione, controllo degli accessi).

4.5.4. Collegamento al registro degli incidenti

Il registro dei dati personali è collegato al processo di gestione delle violazioni dei dati personali. Per ogni violazione della sicurezza rilevata, l'attività di elaborazione corrispondente deve essere elencata nel registro per garantire responsabilità, tracciabilità e trasparenza in conformità con i requisiti del GDPR.

4.5.5. Revisioni e aggiornamenti

Il registro dei dati personali viene esaminato almeno una volta all'anno o ogni volta che ci sono cambiamenti significativi nelle attività di trattamento dei dati personali. Gli aggiornamenti del registro sono obbligatori, in particolare nei seguenti casi:

- vengono introdotti nuovi trattamenti, tecnologie o metodi diagnostici;
- Sono coinvolti nuovi processori di dati personali o fornitori di servizi terzi,
- Ci sono cambiamenti nei requisiti legali o normativi riguardanti la protezione dei dati personali.

4.6. Gestione del consenso del paziente

Data la natura altamente sensibile dei dati trattati (salute riproduttiva e dati sanitari), il Gruppo FutureLife acquisisce, registra e rispetta i consensi dei pazienti:

- **Raccolta del consenso**
  - Il consenso è richiesto nei casi previsti dalla legge, in particolare per il trattamento di categorie particolari di dati (es. fertilità, dati genetici e sanitari) e per qualsiasi uso secondario dei dati.
  - Il consenso è ottenuto tramite un modulo che spiega chiaramente finalità, ambito dei dati e diritti del paziente.
  - Deve essere sempre libero, specifico, informato e inequivocabile.
- **Gestione dei consensi**
  - Le preferenze e lo stato del consenso sono conservati in modo sicuro.
  - Solo personale autorizzato può accedere e aggiornare tali informazioni.
  - Nei casi di consensi a lungo termine (es. trattamenti o ricerca), ai pazienti è offerta la possibilità di confermare o aggiornare periodicamente il consenso.
- **Revoca del consenso**
  - Il paziente può revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento precedente.
  - La revoca non influisce sulla qualità o sull'estensione delle cure fornite.
  - Le richieste di revoca o modifica sono gestite senza ritardi ingiustificati.
- **Registrazione e manutenzione**

- È mantenuta una documentazione completa su quando, come e per quale scopo è stato fornito il consenso (es. log elettronici o moduli firmati).
- I registri sono conservati in modo sicuro per il periodo previsto dalla legge.
- In caso di revoca, i registri sono aggiornati e i dati bloccati o il trattamento interrotto.

4.7. CONDIVISIONE DI INFORMAZIONI PERSONALI

FutureLife ha implementato misure di protezione per i casi in cui sia necessario condividere dati personali con terze parti o fornitori esterni:

> **Assicurazioni e soggetti assicurativi (incluse terze parti per responsabilità civile):**

- I dati possono essere condivisi per verificare la copertura assicurativa e gestire i rimborsi delle spese sanitarie.
- Sono condivisi solo i dati strettamente necessari; i dati sanitari sensibili non sono forniti salvo obbligo di legge.
- Se l'assicuratore si trova fuori dallo SEE in un Paese senza livello di protezione equivalente:
  - l trasferimento può essere richiesto per la gestione del reclamo;
  - è possibile solo con consenso esplicito e informato del paziente;
  - si trasferisce solo il minimo indispensabile;
  - in caso di rifiuto, la copertura può essere negata e il paziente sostenere i costi.

> **Società controllate del Gruppo FutureLife:**

- Possono essere condivisi dati minimi tra cliniche per garantire continuità e qualità delle cure.

> **Fornitori esterni e prestatori di servizi:**

- I dati possono essere condivisi con partner che forniscono servizi sanitari, diagnostici, analisi di laboratorio, audit, sicurezza, supporto IT, consulenza legale e attività amministrative.
- I fornitori possono gestire piattaforme digitali o applicazioni utilizzate dal Gruppo FutureLife.
- I dati sono condivisi solo nella misura necessaria per fornire i servizi concordati.

> **Avvocati, consulenti e autorità di regolamentazione:**

- I dati possono essere condivisi per tutelare i diritti del Gruppo FutureLife, gestire reclami, collaborare con le autorità o ottenere consulenza legale.
- I destinatari possono operare all'interno o all'esterno dello SEE; in caso di trasferimento extra SEE, sono adottate garanzie adeguate, in particolare le Clausole Contrattuali Standard (SCCs).
- Tutti i destinatari devono proteggere la riservatezza, l'integrità e la sicurezza dei dati in conformità al GDPR.

4.8. TRASFERIMENTI DI DATI PERSONALI

Ai sensi del GDPR, i dati relativi alla salute e alla fertilità possono circolare liberamente all'interno dell'UE e dello Spazio Economico Europeo (SEE), purché siano trattati nel rispetto di rigorose garanzie.

Qualsiasi utilizzo secondario dei dati – ad esempio per ricerca o registri sanitari – richiede il consenso esplicito del paziente e solide misure di protezione. Lo Spazio Europeo dei Dati Sanitari (EHDS), a partire dal 2025, rafforzerà ulteriormente i diritti transfrontalieri dei pazienti e introdurrà nuove regole per l'uso secondario dei dati sanitari sensibili.

4.8.1. Flusso dei dati personali e conformità normativa

Il trasferimento di dati personali all'interno dell'UE/SEE non è soggetto a ulteriori restrizioni dovute alla protezione dei dati; pertanto, non sono richieste clausole contrattuali standard (SCC) e valutazioni di adeguatezza. Tuttavia, è essenziale garantire la piena conformità al GDPR e alle regole interne dell'organizzazione in qualsiasi trasferimento di dati:

- **Minimizzazione dei dati:** condividere solo le informazioni strettamente necessarie per lo scopo.
- **Limitazione delle finalità:** i dati possono essere trattati esclusivamente per finalità sanitarie chiaramente definite e legittime.
- **Integrità e riservatezza:** i dati devono essere protetti da accessi non autorizzati, alterazioni, perdite o distruzione.
- **Trasparenza:** i pazienti devono essere informati in modo chiaro se i loro dati sono condivisi al di fuori dell'UE/SEE.
- **Diritti dell'interessato:** garantire l'esercizio di tutti i diritti (accesso, rettifica, limitazione, cancellazione).
- **Sicurezza:** crittografia, controllo degli accessi, registri di audit.

4.8.2. Uso secondario dei dati riproduttivi

Quando i dati sono utilizzati al di fuori del contesto di cura diretta, si applicano regole più rigorose.
L'uso secondario dei dati riproduttivi (es. ricerca, miglioramento qualità, formazione, registri, sviluppo prodotti, marketing) richiede:

- **Consenso esplicito:** I dati saranno trattati solo se il paziente ha dato il suo consenso esplicito.
- **Garanzie:** pseudonimizzazione o anonimizzazione.
- **Trasparenza:** I pazienti devono sapere quali ricerche supportano i loro dati personali e poter ritirare il consenso in qualsiasi momento.

4.8.3. Trasferimenti internazionali di dati personali

Il trasferimento di dati sanitari o relativi alla fertilità al di fuori dell'UE/SEE avviene solo in conformità al GDPR. Se la Commissione Europea ha adottato una decisione di adeguatezza, i dati possono essere trasferiti verso tali Paesi (es. Svizzera, Giappone). Per altre destinazioni si utilizzano le Clausole Contrattuali Standard (SCC) e si effettuano valutazioni dei rischi in conformità alla sentenza Schrems II. In situazioni eccezionali e specifiche possono essere applicate deroghe, ad esempio previo consenso esplicito per un test di laboratorio una tantum all'estero.

4.9. Periodo di conservazione

I dati personali sono conservati per il tempo strettamente necessario a raggiungere la finalità per cui sono stati raccolti, in conformità al principio di limitazione della conservazione previsto dal GDPR. In alcuni casi, i dati possono essere trattati anche dopo il raggiungimento dello scopo originario (es. se l'interessato diventa cliente).

Durate di conservazione:

- **Documentazione sanitaria:** 10 anni dalla fine del trattamento o dalla dimissione, secondo le norme sanitarie.
- **Dati genetici:** almeno 30 anni dalla fine del trattamento, come previsto dalla legge.
- **Dati per finalità legali/amministrative:** fino a 3 anni dopo il periodo iniziale, in linea con i termini di prescrizione.
- **Dati per ricerca:** in forma anonimizzata per la durata del progetto (5–10 anni), secondo le norme vigenti; possono essere condivisi con istituti di ricerca accreditati.
- **Dati relativi a richieste, reclami o esercizio dei diritti:** 1–2 anni, prorogabili per motivi legali o di tutela degli interessi del titolare.
- **Dati relativi a rapporti contrattuali:** per tutta la durata del contratto e successivamente per 5 anni per la gestione di eventuali reclami o contenziosi.
- **Dati per iscrizione alla newsletter:** fino alla revoca del consenso o alla cancellazione dell'iscrizione.

4.10. CANCELLAZIONE DEI DATI PERSONALI

La sicurezza delle procedure di cancellazione è garantita mediante misure tecniche e organizzative adeguate. Il Gruppo FutureLife applica metodi documentati, verificabili e sicuri per la cancellazione dei dati personali in conformità al GDPR e al Regolamento SoHO.

4.10.1. DIRITTO ALLA CANCELLAZIONE

I soggetti dati hanno il diritto di richiedere la cancellazione dei propri dati personali senza indebito ritardo. Ciò include situazioni in cui i dati personali non sono più necessari per lo scopo originale, il consenso viene revocato o i dati personali sono stati trattati illegalmente.

4.10.2. LIMITAZIONI NEL CONTESTO SANITARIO

Il diritto alla cancellazione in ambito sanitario è limitato da obblighi legali di conservazione e/o eccezioni per salute pubblica e ricerca. I dati sanitari e riproduttivi rientrano nelle categorie particolari di dati e richiedono consenso esplicito o altro fondamento giuridico, con ulteriori garanzie. Il Regolamento SoHO impone la tracciabilità a lungo termine (codici univoci non identificativi, es. Codice Europeo Unico) per gameti ed embrioni, spesso fino a 30 anni. Le cliniche potrebbero non essere in grado di cancellare determinati dati sanitari anche su richiesta.

4.10.3. TECNICHE DI CANCELLAZIONE SICURA

Tutte le attività relative alla cancellazione dei dati personali devono essere registrate e verificabili.

- **Dati digitali**
  - **Cancellazione crittografica:** la distruzione delle chiavi di crittografia per rendere i dati illeggibili.
  - **Cancellazione dati:** l'uso di strumenti certificati per sovrascrivere la memoria con pattern casuali.
  - **Strumenti di cancellazione certificati:** utilizzo di software approvati dall'UE per cancellare i dati in modo sicuro.
- **Backup e archivi**
  - **Programmi di conservazione:** Assicurarsi che i dati di backup scaduti vengano automaticamente cancellati o sovrascritti.

- **Separazione dei compiti:** I dati sensibili possono essere cancellati solo da dipendenti autorizzati.
- **Registrazione immutabile:** garantisce il monitoraggio delle cancellazioni effettuate anche nei backup.

> **Carta e supporti fisici:** o incenerimento, oppure triturazione o macinazione con lo scopo di distruggere fisicamente il supporto.

4.10.4. Documentazione e audit

Tutte le procedure per la cancellazione dei dati personali devono essere documentate. Questo include la specificazione dei periodi di conservazione, dei trigger di cancellazione e delle eccezioni. Sono necessari audit regolari per verificare la conformità agli obblighi GDPR e SoHO. Le tracce di audit devono essere mantenute per tutte le operazioni di cancellazione.

4.11. Notifica alle autorità di controllo

In caso di violazione della sicurezza dei dati personali, l'autorità di controllo competente deve essere informata senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare ne viene a conoscenza. Tutte le entità del Gruppo FutureLife devono rispettare le procedure interne per la segnalazione degli incidenti. La documentazione relativa alla violazione e al processo di notifica deve essere conservata per finalità di audit e per dimostrare la conformità normativa.

Il Data Protection Officer (DPO) è responsabile di:

> coordinare l'intero processo di notifica all'autorità di controllo;
> mantenere e aggiornare il registro dei dati personali, garantendo che le registrazioni delle attività di trattamento siano accurate, complete e aggiornate;
> preparare la comunicazione della violazione, includendo:
  - natura e portata della violazione;
  - categoria e numero di interessati e di record coinvolti;
  - dati di contatto per ulteriori azioni e comunicazioni;
  - conseguenze probabili e misure correttive adottate o pianificate.

L'Security Officer Locale deve:

> garantire l'escalation tempestiva dell'incidente da entità/entità locali ai DPO.

Il Responsabile Ufficio Legale deve:

> Esaminare le implicazioni legali della violazione e promuovere la comunicazione con le autorità di controllo competenti.

4.12. Gestione del rischio da parte di terzi

Il FutureLife Group garantisce che tutti i fornitori di servizi terzi e fornitori che trattano dati personali per conto delle aziende del gruppo FutureLife siano soggetti a rigorosi requisiti di protezione dei dati e sicurezza delle informazioni conformi alle politiche e regolamenti interni di FutureLife. Il FutureLife Group mantiene il Vendor Risk Register e segue lo **Standard interno di Cybersecurity dei Fornitori (FL-CS-S2).**

4.12.1. Proiezione pre-collaborazione

> Tutte le terze parti devono compilare un questionario riguardante la protezione dei dati personali e la sicurezza delle informazioni.

- Le valutazioni del rischio vengono effettuate per esaminare le pratiche di gestione dei dati personali, la certificazione (např. ISO 27001) e la conformità alle normative legali e agli standard interni.
- Gli Accordi di Trattamento dei Dati (DPA) vengono stipulati prima che vengano condivisi dati personali.

4.12.2. MONITORAGGIO

- Audit o valutazioni annuali vengono condotti per fornitori terzi ad alto rischio.
- Vengono verificati la storia delle violazioni dei dati personali, la capacità di rispondere a incidenti di sicurezza e l'uso di subappaltatori.
- Le terze parti devono informare il FutureLife Group di qualsiasi violazione della sicurezza dei dati personali o di cambiamenti significativi nelle attività di elaborazione.

4.13. MAPPAMENTI E SCHEMI DEL TRATTAMENTO DEI DATI PERSONALI

Per garantire chiarezza e conformità al GDPR, è necessario creare e mantenere mappe visive e diagrammi di flusso delle attività di trattamento.

Questi devono mostrare:

- il flusso dei dati personali tra sistemi e reparti;
- i punti di raccolta, archiviazione e trasferimento;
- le interfacce con responsabili esterni (terze parti);
- la posizione degli archivi (inclusi servizi cloud e trasferimenti transfrontalieri).

Utilizzi principali:

- identificare rischi e lacune nella protezione dei dati;
- supportare le DPIA (Data Protection Impact Assessment);
- facilitare audit e formazione interna.

Tutti i diagrammi devono essere esaminati dal Data Protection Officer (DPO) almeno ogni due anni o in caso di cambiamenti significativi nelle attività di elaborazione.

4.14. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) deve essere effettuata prima dell'inizio di qualsiasi attività di trattamento che possa comportare un alto rischio per i diritti e le libertà degli individui. Questo include, ma non è limitato a:

- Trattamento esteso di categorie speciali di dati personali.
- Monitoraggio sistematico degli spazi accessibili al pubblico.
- Uso di nuove tecnologie o tecniche di profiling.

Ogni valutazione dell'impatto sulla protezione dei dati personali deve includere:

- Descrizione del processo e del suo scopo.
- Valutazione della necessità e della proporzionalità del trattamento in relazione agli scopi.
- Identificazione dei rischi per i diritti e le libertà dei soggetti in data.
- Misure per mitigare i rischi identificati.

Il Data Protection Officer (DPO) deve documentare e mantenere la valutazione DPA. Nei casi in cui il GDPR lo richieda, è necessario avviare una consultazione con l'autorità di supervisione competente prima di iniziare il trattamento.

4.15. Formazione e sensibilizzazione dei dipendenti

Tutto il personale con accesso ai dati personali, inclusi dati sulla salute e sulla salute riproduttiva e sulla fertilità, riceve una formazione annuale obbligatoria sul GDPR, sullo Spazio Europeo dei Dati Sanitari (EHDS) e sulla cybersecurity, con moduli dedicati ai tecnici di laboratorio (gestione sicura dei dati di donatori ed embrioni), ai clinici (principi di gestione della riservatezza e del consenso) e al personale IT (sicurezza dei sistemi informativi e controlli di accesso). Per sensibilizzare, le cliniche conducono simulazioni di phishing e campagne di igiene informatica, e i progressi e il completamento della formazione vengono monitorati per garantire la conformità e la privacy (incluse categorie speciali di dati personali relativi alla fertilità e ai donatori).

4.16. Revisione e Gestione della politica di protezione dei dati

La Politica di Protezione dei Dati Personali del FutureLife Group deve essere rivista almeno una volta all'anno o immediatamente dopo cambiamenti significativi ai requisiti normativi. Il processo di revisione è coordinato dal Data Protection Officer (DPO) in collaborazione con il Capo Legale, il Responsabile della Cybersecurity e il Chief Transformation Officer. La direzione della clinica e il consulente legale locale sono responsabili di verificare l'applicabilità della politica a livello sussidiale e di garantire la conformità alle normative locali. Tutti gli aggiornamenti devono essere documentati in una tabella di controllo delle versioni e comunicati agli stakeholder appropriati. Un riassunto delle modifiche deve essere incluso nell'avviso di aggiornamento della Politica.

4.17. Disponibilità delle polizze

Il FutureLife Group si impegna a garantire che questa Politica di Protezione dei Dati Personalisia accessibile a tutti. Le richieste di divulgazione in formati alternativi possono essere indirizzate al Data Protection Officer (DPO).

Misure di accessibilità:

- La polizza è disponibile in tutte le sedi in cui opera il FutureLife Group.
- Formati accessibili (ad esempio font di grande dimensione, file PDF compatibili con lettori di schermo) sono disponibili su richiesta.
- Le cliniche espongono copie cartacee della Politica ai banchi di accoglienza e forniscono accesso digitale tramite siti web e/o portali dei pazienti.
- Il personale è formato per aiutare i pazienti a comprendere la Politica e a esercitare i propri diritti.

4.18. Aggiornamenti dell'Informativa sulla Privacy

Il FutureLife Group si riserva il diritto di modificare, modificare o sostituire questa Privacy Policy in qualsiasi momento a sua esclusiva discrezione. Il tuo utilizzo continuativo dei Servizi dopo qualsiasi modifica sarà considerato accettazione della versione aggiornata di questa Politica.

Si consiglia ai soggetti interessati (utenti) di consultare regolarmente questa Politica per essere informati su eventuali modifiche. Se il soggetto non è d'accordo con questo documento, in tutto o in parte, o con eventuali modifiche successive, non deve più utilizzare i servizi e qualsiasi ulteriore utilizzo deve essere immediatamente terminato.

4.19. SUPPLEMENTO SULLA PRIVACY (DPA)

Il Data Privacy Annex (DPA) è una parte obbligatoria del quadro sulla privacy del FutureLife Group. Serve come documento formale che definisce i requisiti specifici di privacy e protezione dei dati applicabili a ciascuna applicazione, sistema o servizio che elabora dati personali, garantendo al contempo trasparenza, responsabilità e coerenza nella gestione dei dati personali all'interno del FutureLife Group.

Lo scopo della DPA è garantire che tutte le attività di trattamento siano chiaramente definite e svolte in conformità con la legislazione applicabile sulla protezione dei dati (come il GDPR) e in conformità con gli standard interni di protezione dei dati del FutureLife Group. La DPA deve includere dettagli di:

- le categorie di dati personali trattati,
- la base giuridica per l'elaborazione;
- il periodo di conservazione dei dati personali,
- le misure di sicurezza in atto;
- i ruoli e le responsabilità degli stakeholder;
- qualsiasi trasferimento di dati personali al di fuori dell'UE/SEE, nella misura in cui ciò sia rilevante per l'attività di trattamento in questione.

4.20. VIOLAZIONE DEI DATI – NOTIFICA AGLI INDIVIDUI

Oltre a notificare le autorità di supervisione, il FutureLife Group si impegna a informare senza indebito ritardo le persone fisiche (soggetti interessati) in caso di violazione della sicurezza dei dati personali qualora tale violazione comporti un alto rischio per i loro diritti e libertà.

4.20.1. CONDIZIONI PER LA NOTIFICA

- Le violazioni di dati personali riguardano categorie particolari di dati personali, in particolare dati di salute, fertilità o genetici.
- Una violazione della sicurezza dei dati personali può portare a furto d'identità, discriminazione, danni reputazionali o altre gravi conseguenze per il soggetto dei dati.

4.20.2. METODI E SCADENZE PER INFORMARE I SOGGETTI DATI

- Le persone interessate saranno informate senza ulteriori ritardi e, se possibile, entro 72 ore dalla conferma della violazione, tramite email, telefono o portale paziente sicuro.
- La notifica includerà, in particolare, una descrizione della natura della violazione, le probabili conseguenze, le misure adottate o pianificate per mitigarne l'impatto e i dettagli di contatto per ulteriori informazioni.
- Se non è possibile comunicare direttamente con i soggetti dei dati, gli annunci saranno pubblicati tramite il sito web della clinica o altri canali mediatici appropriati.

4.21. L'USO DELL'INTELLIGENZA ARTIFICIALE E DEL PROCESSO DECISIONALE AUTOMATIZZATO

Il FutureLife Group può sfruttare l'intelligenza artificiale (IA) e strumenti decisionali automatizzati per supportare i processi clinici e operativi. Questi strumenti vengono utilizzati per aumentare la precisione, l'efficienza e la qualità delle cure fornite. Tuttavia, nessuna decisione con impatto legale o

medico significativo viene presa esclusivamente sulla base di elaborazione automatica – tutte queste decisioni sono soggette a supervisione umana e revisione clinica.

Qualsiasi sistema che utilizza dati personali contenenti un modello di IA deve conformarsi:

- Qualsiasi sviluppo interno o esterno dell'IA:
  - **Nuovi requisiti di sicurezza** di sistema **FL-CS-OP09**,
  - **FL-CS-S7 Bezpečnostní standard pro AI** (AI Security Standard),
  - Ho completato una Business Impact Assessment (BIA) separata.
- Qualsiasi sistema acquistato e implementato internamente o esternamente:
  - **FL-CS-OP-03 Ciclo di Vita dello Sviluppo Sicuro del Sistema**.

Gli strumenti di IA utilizzati e i processi decisionali automatizzati possono includere:

- Selezione e smistamento degli embrioni.
- Algoritmi di abbinamento donatore-ricevitore.
- Analisi del rischio genetico.
- Modellazione predittiva degli esiti del trattamento.
- Ordinamento e programmazione automatica degli appuntamenti.

I pazienti hanno il diritto di:

- essere informati sull'uso dell'intelligenza artificiale sotto la loro cura;
- esprimono la loro opinione su tale trattamento,
- richiedere l'intervento umano nelle decisioni,
- contestare le decisioni prese esclusivamente sulla base dell'elaborazione automatica.

Quando rilevante, verrà effettuata una Valutazione dell'Impatto sulla Protezione dei Dati (DPIA) per valutare i rischi associati al trattamento dei dati personali e garantire la conformità al GDPR, in particolare all'Articolo 22, e alle disposizioni correlate.

4.22. PROTEZIONE DEI DATI DEI DONATORI E DEI BAMBINI CONCEPITI DA DONATORE

Il FutureLife Group aderisce al quadro normativo UE per le Sostanze di Origine Umana (SoHO) per garantire i più alti standard di sicurezza, tracciabilità e protezione dei dati personali nella gestione di dati su donatori e bambini concepiti da donatore. Queste regole sono progettate per garantire la tracciabilità a lungo termine e le tutele della salute pubblica, proteggendo al contempo l'anonimato dei donatori, la riservatezza dei pazienti e la privacy dei bambini concepiti da donatore.

4.22.1. CODIFICA UNICA E TRACCIABILITÀ

Tutto il materiale proveniente dai donatori è contrassegnato con un codice univoco non identificativo (come il Codice Unico Europeo) che consente la piena tracciabilità dalla donazione all'uso clinico, mantenendo l'anonimato sia del donatore che del paziente. Qualsiasi dato direttamente identificativo è mantenuto separato e sicuro, con accesso solo da parte di persone autorizzate e solo per scopi consentiti dalla legge. La separazione tra codice e identità garantisce il rispetto dei requisiti normativi, facilita il monitoraggio della qualità e della sicurezza e protegge la riservatezza sia dei donatori che dei destinatari.

4.22.2. EVENTI AVVERSI GRAVI E REAZIONI

Le procedure formali per identificare, documentare e segnalare gli Eventi Avversi Gravi (SAE) e le Reazioni Avverse Gravi (SAR) sono mantenute in conformità con i requisiti normativi pertinenti dell'UE e nazionali. Tutti gli episodi vengono registrati, indagati e, dove richiesto dalla legge, riportati alle autorità competenti entro i termini stabiliti. Pazienti e donatori devono essere informati immediatamente e senza indebiti ritardi se l'evento o la reazione è rilevante per la loro cure, sicurezza o trattamento in corso.

4.22.3. DIRITTO ALLA RESTRIZIONE DEL TRATTAMENTO E ALL'ACCESSO AI DATI PERSONALI

Secondo il GDPR, pazienti e donatori hanno il diritto di limitare il trattamento dei propri dati personali e riproduttivi. Dato che i dati sulla fertilità e sulla riproduzione costituiscono una categoria speciale di dati personali, le persone fisiche (soggetti di dati) godono di diritti estesi, in particolare per quanto riguarda il consenso esplicito al trattamento e la possibilità di revocare tale consenso in qualsiasi momento.

Le misure tecniche e organizzative adottate dalla clinica per far rispettare le restrizioni sulla lavorazione e l'accesso includono, in particolare:

- **Controllo degli accessi basato sul ruolo (RBAC):** Garantisce che solo le persone autorizzate possano consultare i dati sensibili.
- **Separazione dei registri tra donatore e destinatario:** Previene il collegamento involontario o non autorizzato dei dati.
- **Registrazione completa degli accessi:** Permette di monitorare e auditare tutti gli accessi ai dati di riproduzione.

4.22.4. ANONIMATO DEI DONATORI VS. DIRITTI DEI PAZIENTI E DEI BAMBINI

In alcuni Stati membri dell'UE, la legislazione nazionale garantisce ai bambini concepiti da donatore il diritto di accedere ai dati di identificazione dei donatori non appena raggiungono l'età adulta. In tali casi, quando legalmente possibile, il FutureLife Group rispetta gli obblighi legali, mantenendo i più alti standard di sicurezza e minimizzando i dati personali.

4.22.5. MINIMIZZARE IL RISCHIO GENETICO

Minimizzare il rischio genetico è un obbligo fondamentale previsto dal Regolamento UE SoHO (che stabilisce i requisiti per la qualità e la sicurezza dei SoHO), dal GDPR (che regola il trattamento dei dati genetici) e dalla legislazione sanitaria nazionale. L'obiettivo di minimizzare il rischio genetico è ridurre la probabilità di trasmissione di malattie ereditarie o difetti genetici da gameti donatori (spermatozoi/ovociti) o embrioni ai riceventi e ai loro futuri figli.

Gli elementi della minimizzazione del rischio genetico includono:

- **Salute e storia familiare**
  - I donatori compilano questionari dettagliati riguardanti la loro storia sanitaria familiare (di solito in 2-3 generazioni).
  - In particolare, vengono monitorate le malattie del sistema cardiovascolare, le sindromi tumorali, le malattie neurologiche, i disturbi metabolici e i difetti congeniti dello sviluppo.
- **Esame fisico**

- Esame clinico per escludere fattori di rischio evidenti (ad esempio anomalie dello sviluppo).

> **Test di laboratorio**

- Screening standard per le malattie infettive (HIV, HBV, HCV, sifilide, CMV).
- Screening per i portatori di malattie genetiche (ad esempio fibrosi cistica, talassemia, malattia di Tay-Sachs, SMA).
- Analisi cromosomica (cariotipizzazione), se necessario.

> **Consulenza genetica**

- Se vengono identificati fattori di rischio, ai donatori e, se applicabile, ai futuri genitori viene offerto un supporto professionale di consulenza genetica.
- La consulenza aiuta a valutare i rischi residui e informa l'idoneità dei donatori durante le decisioni.

> **Criteri di esclusione dei donatori**

- I donatori con malattie ereditarie note o ad alto rischio di trasmettere gravi malattie genetiche sono esclusi dal programma di donazione.
- In alcune giurisdizioni, la legge può consentire eccezioni basate sul consenso esplicito informato del destinatario, ma questi casi sono eccezionali.

4.23. DATI DEI BAMBINI E CONSENSO DEI GENITORI

I servizi e le attività commerciali del FutureLife Group non sono destinati ai minorenni e i dati personali dei minorenni non vengono intenzionalmente raccolti o ulteriormente trattati. I servizi del FutureLife Group sono destinati a persone che hanno raggiunto la maggiore età.

Nei casi in cui determinati servizi siano esplicitamente rivolti ai minori, è richiesto il consenso dei genitori o dei tutori legali per la raccolta e il trattamento ulteriore dei loro dati personali, in conformità con la legge applicabile. Se il soggetto è minorenne, è necessario ottenere il consenso preventivo di un genitore o tutore legale prima di fornire qualsiasi dato personale a qualsiasi azienda del gruppo FutureLife.

4.23.1. ETÀ E VERIFICA DELL'IDENTITÀ

Le cliniche devono verificare l'età del soggetto tramite documenti di identificazione governativi prima di iniziare qualsiasi raccolta di dati personali o fornire trattamento.

Tutti i moduli di consenso devono essere firmati correttamente, datati e conservati in modo sicuro. I registri elettronici di revisione del ritiro e concessione del consenso sono conservati per tutto il periodo previsto dalla legislazione e dalle politiche interne.

4.23.2. PROCEDURE PER PRESERVARE LA FERTILITÀ NEI MINORI

In alcuni casi eccezionali, è possibile e necessario curare minorenni. Questi casi riguardano tipicamente casi di preservazione della fertilità in bambini con gravi condizioni mediche, come il cancro.

A) Criopreservazione del tessuto ovarico

La crioconservazione del tessuto ovarico è il metodo principale per preservare la fertilità nei bambini prepuberi. Questa procedura prevede la rimozione chirurgica del tessuto ovarico contenente ovuli

immaturi, che vengono poi congelati per un uso successivo. Successivamente, se il paziente desidera avere figli, il tessuto così conservato può essere trapiantato nuovamente nel corpo del paziente; Le uova immature possono anche essere lasciate maturare in condizioni di laboratorio e poi utilizzate, specialmente nelle procedure di riproduzione assistita.

B) Stimolazione delle ovaie e ottenimento di ovuli maturi

Negli adolescenti che hanno già attraversato la pubertà e che hanno sviluppato ovuli maturi (ovociti), può essere effettuata una stimolazione ovarica controllata e la successiva raccolta di ovuli maturi. Le ovaie vengono stimolate tramite trattamento ormonale e poi gli ovuli maturi ottenuti (ovociti) vengono conservati sotto forma di crioconservazione.

4.23.3. Aspetti medici e legali

- **Necessità medica:** Le procedure vengono solitamente eseguite se la condizione di salute del bambino o il trattamento può portare all'infertilità.
- **Consenso:** Il consenso è sempre richiesto sia dal paziente (se abbastanza maturo da comprendere la natura della procedura) sia dai suoi genitori/tutori legali; il consenso informato è richiesto in conformità con la legge.
- **Ricerca: Sono in corso** ricerche per trovare altre opzioni di preservazione della fertilità per bambini che non hanno ancora attraversato la pubertà.

4.23.4. Diritto di ritirare il consenso

I genitori o i tutori legali possono revocare il loro consenso in qualsiasi momento. Dopo il ritiro del consenso, il trattamento dei dati personali del minore sarà limitato o terminato, salvo che la legge applicabile richieda ulteriori trattamenti.

4.23.5. Conformità alle normative nazionali

Il FutureLife Group deve garantire il rispetto della legislazione nazionale di ciascun paese in cui opera, in particolare della legislazione sull'età di idoneità al trattamento medico e sull'idoneità al trattamento di fertilità.

5. CONFORMITÀ AD ALTRI QUADRI NORMATIVI

5.1. EU CYBER RESILIENCE ACT (CRA)

Il Cyber Resilience Act (CRA), entrato in vigore nel 2024 e i cui principali obblighi saranno pienamente applicabili a partire da dicembre 2027, stabilisce i requisiti di cybersicurezza per i "Prodotti con Elementi Digitali" (PDE), inclusi hardware e software immessi sul mercato nell'Unione Europea. I produttori, importatori e distributori di questi prodotti avranno responsabilità di cybersecurity, inclusa la conduzione di valutazioni dei rischi informatici e la documentazione degli sforzi di conformità.

Il FutureLife Group deve prepararsi a soddisfare i requisiti del Cyber Resilience Regulation (CRA) attraverso:

- Identifica tutti i prodotti con elementi digitali (EDP), ad esempio sistemi di cartelle cliniche elettroniche (EHR), strumenti che utilizzano intelligenza artificiale, ecc.
- Garantirà il principio di "security by design" (sviluppo basato sulla security by design).
- Implementa procedure formalizzate per la gestione delle vulnerabilità.
- Coordina il processo di certificazione CRA tramite un responsabile della cybersecurity.

5.2. SPAZIO EUROPEO DEI DATI SANITARI (EHDS)

Il FutureLife Group deve impegnarsi a implementare lo Spazio Europeo dei Dati Sanitari (EHDS), un quadro normativo che entrerà in vigore nel 2025 e mira a facilitare l'accesso, la condivisione e l'uso sicuri ed efficienti dei dati sanitari, inclusi quelli sulla salute riproduttiva, in tutti gli Stati membri dell'UE.

5.2.1. USO PRIMARIO DEI DATI SANITARI

Il FutureLife Group garantirà la conformità alle normative EHDS riguardanti il trattamento di tutti i dati sanitari personali ai fini dell'assistenza diretta al paziente, e in particolare si applicheranno i seguenti principi:

- **Interoperabilità:** I sistemi devono essere aggiornati per supportare gli standard tecnici EHDS per formati dati, protocolli di comunicazione/scambio e coerenza semantica.
- **Diritti di accesso:** I pazienti devono poter accedere ai propri dati sanitari oltre confine, inclusi i dati riproduttivi e legati alla fertilità, in modo sicuro e facile da usare.
- **Portabilità dei dati:** Devono essere sviluppati meccanismi che permettano ai pazienti di trasferire i propri dati sanitari tra le cliniche FutureLife e altri fornitori sanitari autorizzati all'interno dell'UE, in conformità con il diritto GDPR alla portabilità dei dati.

5.2.2. USO SECONDARIO DEI DATI SANITARI

Il FutureLife Group sostiene l'uso secondario etico e legale dei dati sanitari per scopi di ricerca, innovazione e salute pubblica ai sensi dell'EHDS, soggetto alle seguenti condizioni:

- **Consenso esplicito:** L'uso secondario di dati sulla fertilità e dati genetici richiede il consenso documentato, informato ed esplicito del soggetto dei dati, a meno che l'uso secondario non sia consentito su un altro basamento legale previsto dal GDPR e dall'EHDS.

- **Minimizzazione dei dati e pseudonimizzazione:** Viene utilizzata solo la quantità minima di dati necessari e gli identificatori vengono rimossi o pseudonimatizzati per garantire la protezione della privacy dei soggetti in dato.
- **Trasparenza:** I pazienti sono informati in modo chiaro sulla natura, lo scopo e i destinatari dell'uso secondario dei loro dati sanitari e possono revocare il loro consenso in qualsiasi momento. Meccanismi chiari e reversibili di esclusione saranno offerti ai pazienti, ove possibile secondo la legislazione pertinente.

5.2.3. Formato europeo di scambio elettronico delle cartelle cliniche (EEHRXF)

Il FutureLife Group sta attivamente implementando il Formato Europeo di Scambio Elettronico delle Cartelle Cliniche (EEHRXF). L'EEHRXF è la base tecnica dell'EHDS, che garantisce l'uso primario dei dati sanitari per scopi di assistenza diretta ai pazienti e garantisce l'interoperabilità tra gli Stati membri. Si tratta di uno standard che consente lo scambio transfrontaliero di dati controllato dai pazienti all'interno dell'EHDS. Copre la strutturazione e lo scambio di categorie chiave di dati sanitari elettronici, come riepiloghi dei pazienti, prescrizioni elettroniche, risultati di laboratorio, immagini e rapporti medici, rapporti di dimissione ospedaliera e dati sulle malattie rare.

5.2.4. Meccanismo di portabilità dei dati

Il FutureLife Group consentirà ai pazienti di ricevere e trasmettere i propri dati sanitari personali in un formato strutturato, comunemente utilizzato e leggibile da macchina, in conformità con il diritto GDPR alla portabilità dei dati.

Meccanismi di portabilità:

- I pazienti potranno richiedere i propri dati tramite portali sicuri o inviando una richiesta scritta al Data Protection Officer (DPO).
- I dati sanitari personali saranno forniti in formati conformi all'EHDS come HL7 FHIR, CDA o EEHRXF XML.
- I trasferimenti ad altri fornitori di servizi sanitari saranno effettuati tramite API sicure o protocolli di trasferimento file criptati.

5.2.5. Centri nazionali EHDS

Il FutureLife Group osserva che ogni Stato membro dell'UE è tenuto a istituire un centro nazionale EHDS per coordinare lo scambio di dati sanitari. In particolare, il FutureLife Group avrà l'obiettivo di:

- Collaborare con i centri nazionali EHDS nei paesi in cui opera.
- Registrare i dataset idonei presso i centri nazionali per l'uso secondario dove è richiesto il consenso del paziente e l'approvazione da parte delle autorità regolatorie competenti.
- Ha partecipato a programmi pilota e a unboarding tecnico guidati dalle autorità nazionali per testare e convalidare sistemi compatibili con EHDS.

5.2.6. Condivisione transfrontaliera dei dati

- I dati sanitari transfrontalieri possono essere riutilizzati solo a scopo di ricerca in un ambiente di elaborazione dati sicuro approvato dal National Health Data Access Body (HDAB).
- Le strutture sanitarie devono catalogare i dataset e contrassegnare tutti i diritti di proprietà intellettuale e i segreti commerciali ad essi relativi all'HDAB.
- L'uso secondario per marketing o qualsiasi profilazione discriminatoria è severamente vietato.

5.2.7. Implementazione della sicurezza EHDS

Lo scopo dell'EHDS è consentire la condivisione transfrontaliera e l'uso secondario dei dati sanitari a scopo di ricerca, il che significa coinvolgere più attori e più dati, aumentando così potenzialmente il numero di punti di ingresso per attori malevoli. Data la sensibilità dei dati sulla salute riproduttiva, un quadro di cybersecurity adattivo e solido è essenziale per l'implementazione sicura dello Spazio Europeo dei Dati Sanitari (EHDS) all'interno del FutureLife Group.

Oltre alla conformità ai documenti interni, saranno implementate le seguenti misure organizzative:

- **Prevenire violazioni di dati personali:** Allineare le procedure al **Piano di Risposta agli Incidenti Informatici (FL-CS-OP2)** e garantire la tempestiva rilevazione, notifica e mitigazione degli incidenti di violazione dei dati correlati all'EHDS.
- **Implementare sistemi EHR certificati:** Assicurarsi che tutti i sistemi di Cartelle Cliniche Elettroniche (EHR) utilizzati nelle cliniche siano certificati secondo l'EHDS per interoperabilità, sicurezza e privacy prima di utilizzarli negli scambi transfrontalieri.
- **Scambio di dati sicuro:** Utilizzare canali di comunicazione criptati e API sicure per condividere dati con i centri nazionali EHDS e le infrastrutture HealthData@EU (un hub centrale che riunisce set di dati sanitari da tutta Europa).
- **Cooperazione con l'EHDS Nazionale:** Collaborare attivamente con le Autorità Nazionali di Accesso ai Dati Sanitari (HDAB) per integrarsi in modo sicuro e garantire la conformità ai requisiti legali.

5.2.8. Governance e conformità

- Sarà **istituito un ruolo di coordinatore EHDS** (all'interno del team DPO) per supervisionare l'implementazione, cooperare con i centri nazionali EHDS e garantire la prontezza al graduale adempimento dei requisiti.
- Il Capo **del Dipartimento Legale** monitorerà regolarmente lo sviluppo della legislazione e garantirà la conformità con le normative GDPR, SoHO ed EHDS.
- Tutte le attività di elaborazione dei dati relative all'EHDS **saranno documentate** nel registro dei dati personali e saranno **soggette a revisione.**

ALLEGATO A – CATEGORIE DI DATI PERSONALI E SCOPI DI TRATTAMENTO

Di seguito sono riportate le categorie di dati personali raccolti, gli scopi per cui tali dati sono utilizzati e il periodo per cui sono conservati.

Tabella 1: Categorie di dati personali e scopi del trattamento

SCOPO DEL TRATTAMENTO DEI DATI PERSONALI	CATEGORIE DI DATI PERSONALI	BASE GIURIDICA PER L'ELABORAZIONE	AMMINISTRATORE/I
1. Gestione di richieste di informazioni, reclami o suggerimenti			
Le richieste di informazioni, reclami o suggerimenti vengono elaborate per rispondere a domande, affrontare le preoccupazioni sollevate e gestire le richieste ricevute.	– Dettagli di contatto: nome, indirizzo email, numero di telefono. - Dati di contenuto: informazioni fornite nella richiesta o comunicazione.	Consenso del soggetto dati (Art. 6(1) (a) GDPR). L'interesse legittimo del controller nel controllo qualità, nella risoluzione delle controversie e nel miglioramento del servizio (Articolo 6(1)(f) del GDPR).	Il FutureLife Group insieme alla clinica competente del gruppo a cui è indirizzata la richiesta.
2. Fornitura di servizi sanitari			
I dati personali vengono trattati con lo scopo di garantire la corretta erogazione dei servizi sanitari. Ciò include la gestione delle cartelle cliniche dei pazienti e l'elaborazione dei dati e dei documenti generati nel contesto dell'assistenza medica.	– Contatti: nome, indirizzo email, numero di telefono, indirizzo postale. – Dati di identificazione: numero di carta d'identità o altro numero di carta d'identità, numero di passaporto, sesso, data di nascita. - Dati immagine: foto, scansioni o altri documenti fotografici. - Dati sulla salute e sulla salute riproduttiva (categorie speciali di dati personali): storia clinica, referti medici, risultati diagnostici, informazioni sui trattamenti, campioni biologici, test di laboratorio, dati sulla fertilità e altre informazioni sanitarie rilevanti, ecc.	Esecuzione di un contratto con il soggetto dati (art. 6(1) (b) GDPR). Rispetto degli obblighi legali del responsabile (articolo 6(1)(c) del GDPR).	La relativa clinica FutureLife che fornisce servizi sanitari e agisce come responsabile dei dati personali in questo contesto (o un responsabile congiunto insieme al FutureLife Group, se tale è fornito).

Scopo del trattamento dei dati personali	Categorie di dati personali	Base giuridica per l'elaborazione	Amministratore/i
3. Gestione dei Registri dei Pazienti			
I dati personali vengono trattati con lo scopo di conservare le cartelle cliniche dei pazienti e garantire una corretta gestione amministrativa e organizzativa dei centri sanitari.	- Dettagli di contatto: nome, indirizzo email, numero di telefono, indirizzo postale, ecc. – Dati sanitari: storia clinica, diagnosi, trattamenti, allergie, farmaci, segni vitali e altre informazioni sanitarie rilevanti provenienti dal paziente e dal suo partner. – Dati di identificazione: numero di nascita, numero di paziente, numero di passaporto, sesso, data di nascita. - Dati amministrativi: dettagli degli appuntamenti, dati di fatturazione, dati assicurativi, moduli di consenso e registri di comunicazione.	Esecuzione di un contratto con il soggetto dati (art. 6(1) (b) GDPR). Rispetto degli obblighi legali del responsabile (articolo 6(1)(c) del GDPR). Per categorie particolari di dati personali, il trattamento si basa sulla fornitura di assistenza sanitaria in conformità con la normativa UE o degli Stati membri (articolo 9(2)(h) del GDPR).	Cliniche del FutureLife Group.
4. Gestione delle relazioni con i donatori			

SCOPO DEL TRATTAMENTO DEI DATI PERSONALI	CATEGORIE DI DATI PERSONALI	BASE GIURIDICA PER L'ELABORAZIONE	AMMINISTRATORE/I
I dati personali vengono trattati con lo scopo di creare profili dei donatori e gestire il rapporto contrattuale tra il donatore e la clinica. Ciò include la fornitura delle cure sanitarie necessarie e il pagamento di un risarcimento concordato.	– Dati di contatto: nome, indirizzo e-mail, numero di telefono, indirizzo postale.– Dati identificativi: numero di previdenza sociale o altro numero di identificazione, numero di passaporto, sesso, data di nascita.– Dati sanitari e genetici (categorie speciali di dati personali): storia sanitaria e familiare, risultati dei test, informazioni sulla fertilità, test genetici e altre informazioni sanitarie rilevanti.– Dati amministrativi e finanziari: dati sul rapporto contrattuale, sulla programmazione delle visite, Dati su remunerazioni/compensi, dati di pagamento e contabilità, moduli di consenso e registri di comunicazione.	Esecuzione di un contratto con il soggetto dati (art. 6(1) (b) GDPR). Rispetto degli obblighi legali del responsabile (articolo 6(1)(c) del GDPR). Per categorie particolari di dati personali, il trattamento si basa sulla fornitura di assistenza sanitaria in conformità con la normativa UE o degli Stati membri (articolo 9(2)(h) del GDPR).	Cliniche del FutureLife Group.
5. Rincorso Paziente			
I dati personali vengono trattati e inoltrati alla clinica raccomandata per garantire che il trattamento necessario possa essere fornito in un luogo di lavoro alternativo su richiesta del paziente.	– Contatti: nome, indirizzo email, numero di telefono, indirizzo postale. – Dati di identificazione: numero di carta d'identità o altro numero di carta d'identità, numero di passaporto, sesso, data di nascita.	Consenso dei dati soggetti al trasferimento di dati personali ad altre cliniche FutureLife (Articolo 6(1)(a) del GDPR).	Cliniche del FutureLife Group.
6. Scopi interni amministrativi e manageriali			
I dati personali vengono trattati allo scopo di garantire una corretta gestione amministrativa e organizzativa delle cliniche, nonché per scopi statistici interni.	– Dettagli di contatto: nome, indirizzo email, numero di telefono.	L'interesse legittimo del controller nella gestione e nel controllo delle attività organizzative e delle relazioni commerciali (articolo 6(1)(f) del GDPR).	Il gruppo FutureLife insieme alla clinica pertinente del gruppo coinvolto nell'attività di

SCOPO DEL TRATTAMENTO DEI DATI PERSONALI	CATEGORIE DI DATI PERSONALI	BASE GIURIDICA PER L'ELABORAZIONE	AMMINISTRATORE/I
	- Dati amministrativi: dettagli delle riunioni, dati di fatturazione, dati assicurativi e registri di comunicazione. –Statistiche.		trattamento (controllori congiunti).
7. Scopi del rilevamento			
I dati personali vengono trattati con lo scopo di inviare sondaggi di qualità e soddisfazione relativi ai servizi e alle cure fornite.	– Dettagli di contatto: nome, indirizzo email, numero di telefono. –Statistiche.	Legittimo interesse nel controllo qualità, nell'adattamento delle attività e nello sviluppo di prodotti e servizi migliorati (Art. 6(1) (f) GDPR).	Il FutureLife Group insieme alla clinica competente del gruppo a cui è indirizzata la richiesta.
8. Scopi di marketing. Invio di messaggi commerciali e newsletter			
I dati personali vengono trattati con lo scopo di gestire gli abbonamenti ai servizi di notifica e comunicazione (ad esempio newsletter) e fornire informazioni su servizi o offerte speciali.	– Dettagli di contatto: nome, indirizzo email, numero di telefono.	Il consenso del soggetto fornito tramite abbonamento (Art. 6(1) (a) GDPR). Nel caso di una relazione contrattuale esistente, l'interesse legittimo del responsabile nel trasmettere informazioni su prodotti e servizi simili (Articolo 6(1)(f) del GDPR).	Il FutureLife Group, insieme alla clinica pertinente del gruppo a cui si riferisce l'invio di comunicazioni commerciali.
9. Indagini scientifiche e di ricerca			
I dati personali vengono trattati a scopo scientifico e di ricerca al fine di approfondire la conoscenza della fertilità e delle condizioni di salute riproduttiva, migliorare i metodi di trattamento riproduttivo assistito e sostenere la formazione professionale in questo ambito.	- Dati medici e sanitari: storia clinica, risultati diagnostici, informazioni sui trattamenti, segni vitali, dati sulla salute mentale/comportamentale, dati sulla salute riproduttiva, ecc.	Legittimo interesse a condurre attività di ricerca e scientifiche nel campo della fertilità e della salute riproduttiva (Articolo 6(1)(f) del GDPR). Se i dati non sono anonimizzati, è richiesto il consenso esplicito dei soggetti interessati (art. 6(1) (a) GDPR).	Il FutureLife Group insieme alla clinica pertinente del gruppo a cui si riferisce la ricerca.

Scopo del trattamento dei dati personali	Categorie di dati personali	Base giuridica per l'elaborazione	Amministratore/i
10. Manutenzione e analisi del sito web			
I dati personali vengono trattati con lo scopo di garantire e ottimizzare le prestazioni del sistema, valutare sicurezza e stabilità, e fornire pubblicità personalizzata basata sul comportamento degli utenti. Questo si ottiene tramite l'uso della tecnologia dei cookie. Per informazioni più dettagliate, si prega di consultare la Cookie Policy.	- L'indirizzo IP del dispositivo connesso a Internet. – Data e ora di accesso. - L'URL del referer, il tipo di browser e il sistema operativo. - Il nome del fornitore di accesso.	Per i cookie non necessari: consenso fornito tramite impostazioni/preferenze sui cookie (Art. 6 (1) (a) GDPR). Per i cookie tecnici e necessari: legittimo interesse a garantire la sicurezza, la stabilità e l'usabilità del sito web (Art. 6(1) (f) GDPR).	FutureLife Group.
11. Rispetto degli obblighi legali			
I dati personali sono trattati ai fini di rispettare gli obblighi legali, inclusi quelli relativi alla protezione dei dati personali, agli obblighi fiscali e contabili, all'assistenza sanitaria e ad altre normative legali applicabili. I dati possono inoltre essere messi a disposizione delle autorità di polizia, dei tribunali, delle autorità amministrative o di altre autorità pubbliche se richiesto dalla legge.	– Dettagli di contatto: nome, indirizzo email, numero di telefono. - Dati di contenuto: informazioni contenute in documenti e comunicazioni relative alla conformità ai requisiti legali o normativi.	Rispetto degli obblighi legali (art. 6(1) (c) GDPR).	Il FutureLife Group, insieme alla clinica competente del gruppo a cui si riferiscono l'obbligo e il trattamento dei dati personali.

ALLEGATO B – MATRICE RACI

Questa matrice RACI descrive i ruoli e le responsabilità legati alla conformità alla Politica di Protezione dei Dati Personali tra le principali parti interessate.

Segue la legenda che spiega il significato delle sigle utilizzate nella matrice RACI:

- **R (Responsible):** La persona che effettivamente svolge il compito o l'attività.
- **A (Accountable):** La persona che assume la responsabilità ultima per il corretto e completo completamento del compito.
- **C (Consulted):** Una persona che fornisce documenti, opinioni o competenze prima di completare un compito.
- **I (Informed):** Una persona che è costantemente informata sui progressi e sulle decisioni prese, ma che non partecipa attivamente all'esecuzione del compito.

Tabella 2: Matrice RACI

Attività / Ruolo	DPO	CTO	Capo del Dipartimento Legale	Security Officer Locale	Dipartimento Risorse Umane	Personale	Fornitori	Responsabile della Sicurezza Informatica	Business Owner	Functional Owner
Monitorare la conformità al GDPR	R	A	A	C	I	I	I	C	A	C
Punto di contatto per le autorità di controllo	R	I	I	I	I	I	I	I	I	I
Formazione e consulenza nel campo della protezione dei dati personali	R	C	C	C	C	I	I	C	I	C
Audit interni e valutazioni	R	A	C	C	I	I	C	C	C	C
Valutazione dell'Impatto sulla Privacy (DPIA)	A	I	C	C	I	I	C	C	R	R

Registrazioni delle attività di elaborazione	R	I	C	C	I	I	C	I	C	R
Approvazione dell 'Politica di Protezione dei Dati Personalie successiva supervisione	I	A	R	I	I	I	I	C	C	I
Salvaguardie tecniche per i dati personali	C	I	R	C	I	I	R	A	C	C
Rispondere a incidenti e violazioni di dati personali	C	I	R	C	C	I	C	A	I	I
Conformità locale GDPR	I	I	C	R	I	I	I	C	R	R
Trattamento dei dati personali dei dipendenti	I	I	I	I	R	I	I	I	R	R
Formazione dello staff	C	I	C	R	R	R	I	C	I	C
Gestione responsabile dei dati personali	I	I	I	I	I	R	R	C	R	R
Trattamento contrattuale dei dati personali	I	I	I	I	I	I	R	C	R	C
Test di penetrazione e analisi del rischio	I	C	C	I	I	I	I	R	C	C
Crittografia e controllo degli accessi	I	I	C	I	I	I	I	R	C	C

FutureLife

Politica di Protezione dei Dati Personali

INFORMAZIONI SU FUTURELIFE

Dalla fondazione del FutureLife Group nel 2014, abbiamo continuato a crescere ogni anno. Oggi abbiamo più di 50 cliniche in 16 paesi europei, gestite da più di 1.500 membri qualificati e 600 medici. Le nostre cliniche offrono un trattamento completo di sterilità, inclusi test genetici, immunologici e altri controlli.

Il nostro obiettivo principale è fornire cure di qualità e trattamenti efficaci per creare bambini sani e famiglie felici. Investiamo continuamente nelle nostre cliniche, nella ricerca e nella formazione. Questo ci aiuta a offrire ai nostri team competenza, stabilità finanziaria, buone condizioni di lavoro e stipendi competitivi.