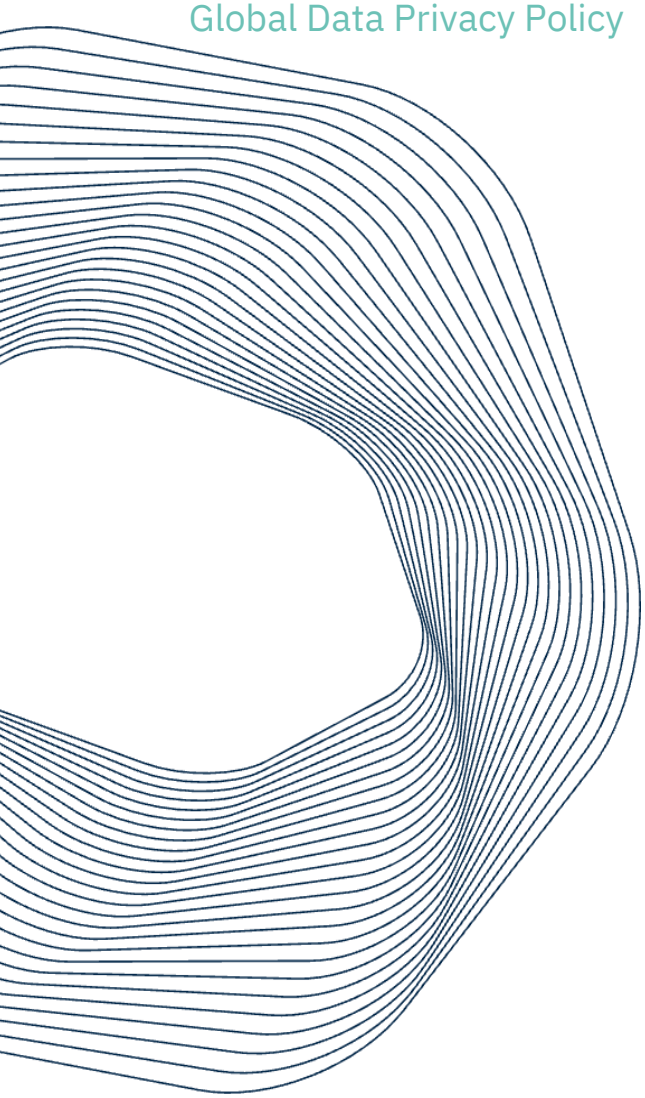
FutureLife

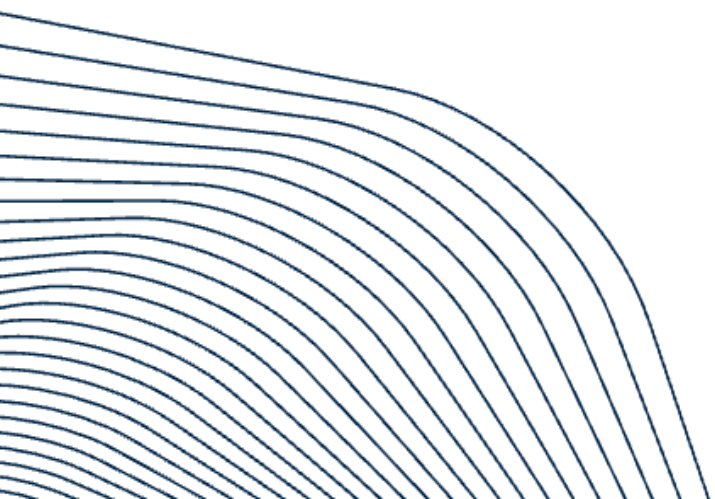
DATA PROTECTION MANAGEMENT SYSTEM

GLOBAL DATA PRIVACY POLICY

FUTURELIFE GROUP

Version: 1.0
Date: 15-09-2024
Classification: INTERNAL





FutureLife

Global Data Privacy Policy

Document Title:	Global Data Privacy Policy	FutureLife a.s.
Subtitle:	Data Protection Management System	Na Příkopě 859/22
Contact person 1:	Maros Zuba	Nové Město, 110 00 Praha 1
Department:	Digital	Czech Republic
Contact person 2:	Ilja David	
Department:	Digital	
Document ID:	FL-DP-P1	
Release date:	15-09-2025	

Document content:

The Global Data Privacy Policy outlines how FutureLife a.s. and any of its affiliates belonging to the same corporate group (the "**FutureLife Group**") process the personal data collected from internal systems, digital platforms, and other relevant sources within the organisation is processed. This policy is mandatory for the entire organisation, including all employees, collaborators, subsidiaries, and external partners who handle personal data. This policy is aligned with applicable laws and the requirements of ISO/IEC 27701, which extends the ISO/IEC 27001 standard by incorporating additional controls and guidelines for managing personal data and privacy information.

Created by:	**Verified by:**	**Approved by:**
Ilja David	Maros Zuba	Ignacio Couto
Cybersecurity Manager	Head of Legal	Chief Transformation Officer
Digital	Digital	Digital
FutureLife a.s.	FutureLife a.s.	FutureLife a.s.

Keywords:

Data Privacy Policy, Information Technologies, Operational Technologies, Data Protection, GDPR

Document Confidentiality:

☐ PUBLIC. Publicly available data relating to the organisation's day-to-day business or publicly known processes.

☒INTERNAL. Non-disclosure data about the normal course of business or internal processes of the organisation.

☐ CONFIDENTIAL. Data relating to strategic business activities, contracts, financial data, personal and healthcare data.

This document and its contents are the property of FutureLife a.s. and Iron OT s.r.o. and may not be duplicated and/or published without permission. Any use other than that for which it was intended is prohibited. Reproduction, distribution, and use of this document, as well as communication of its contents to others without express permission, is prohibited and the perpetrators will be liable for damages.

© FutureLife a.s., Iron OT s.r.o, 2024 – All rights reserved.

Version	Date	Reason for change	Created	Verified	Approved
1.0	15.09.2025	First Edition	Ilja David	Ondřej Novák	Ignacio Couto

TRACK CHANGES

TABLE OF CONTENTS

1. INTRODUCTORY INFORMATION

1.1. PURPOSE

This policy establishes a unified framework for ensuring **the protection of personal data across the entire FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group")**. Its purpose is to define principles, roles, and responsibilities related to the processing of personal data in accordance with applicable legislation, including the GDPR and other relevant national regulations.

1.2. SCOPE OF APPLICATION

The policy applies to all processes, technologies, and entities within the Group that handle personal data, ensuring a consistent approach to privacy, data security, and the rights of data subjects.

1.3. RELATED DOCUMENTS

This section lists related internal documents that support and supplement the Privacy Policy.

- **FL-CS-P1 – Cybersecurity Policy**: a framework for the management of cybersecurity of the organisation.
- **FL-CS-S1 – End User Cybersecurity**: a standard for secure behaviour and responsibilities of end users within the organisation.
- **FL-CS-S2 – Supplier Cybersecurity**: a standard for assessing and managing cybersecurity risks related to third-party suppliers.
- **FL-CS-S6 – Business Continuity Plan**: a standard to ensure operational resilience and recovery in case of disruptions.
- **FL-CS-OP2 – Cybersecurity Response Plan**: a procedure for detecting, responding to, and recovering from cybersecurity incidents.
- **FL-CS-OP3 – Secure System Development Lifecycle**: a procedure for integrating security throughout the system development process.
- **FL-CS-OP7 – Incident Communication**: a procedure for internal and external communication during cybersecurity incidents.
- **FL-CS-OP9 – New System Security Requirements**: a specification of security requirements for the design and implementation of new systems.
- **FL-CS-S7 – AI Security Standard:** a standard for security measures to protect AI tools, including organisational data and related infrastructure.
- **FL-CS-S4 – Internal Audit:** contains requirements and responsibilities for the internal audit as part of the Cybersecurity Management System.

1.4. TERMS

TERM	EXPLANATION
Data Controller	An individual or organisation that determines the purposes and means of processing personal data
Data Processor	An entity that processes personal data on behalf of the Data Controller
Sensitive Data	Confidential information that, if exposed, could cause harm, discrimination, or loss to individuals, organisations, or national security - examples include personal health information (PHI), financial details, personally identifiable information (PII), trade secrets, and potentially sensitive data
Special Categories of Data	Sensitive personal data such as health, genetic, biometric, or racial information
Consent	Freely given, specific, informed, and unambiguous indication of the data subject's wishes
Cookies	Small text files downloaded & stored on the user's device, containing limited amounts of information
Anonymisation	Process of removing or altering personal identifiers so that individuals cannot be identified
Joint Controllers	Two or more entities that jointly determine the purposes and means of processing personal data
Personal Data	Any information relating to an identified or identifiable natural person
Personal Health Information	Confidential medical data that identifies an individual and is related to their past, present, or future physical or mental health, the provision of healthcare, or the payment for healthcare services
Primary Use of Health Data	The use of collected information directly in the course of providing care to an individual
Secondary Use of Health Data	Information collected in the course of care is used for purposes beyond the direct care of the individual (e.g., research, public health, service planning, quality improvement, policy development)

1.5. ABBREVIATIONS

ABBREVIATION	EXPLANATION
EEA	European Economic Area
GDPR	General Data Protection Regulation
DPA	Data Privacy Annex
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment – a process to identify and minimise data protection risks
PHI	Personal Health Information & Sensitive Data
RACI	Responsibility Assignment Matrix – defines roles and responsibilities in a project or process
PII	Personally identifiable information
EHDS	European Health Data Space
SoHO	Substances of Human Origins Regulation
SAE	Serious Adverse Events
SAR	Serious Adverse Reactions
HDAB	Health Data Access Body
AI	Artificial Intelligence
EEHRXF	European Electronic Health Record Exchange Format
CRA	EU Cyber Resilience Act
PDE	Product with Digital Elements

2. GLOBAL DATA PRIVACY POLICY

All efforts are dedicated to respecting privacy and ensuring the security of personal data, which FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), endeavour to process in accordance with the General Data Protection Regulation (GDPR), European Health Data Space (EHDS), EU SoHO Regulation, EU Cybersecurity Action Plan 2025, EU Artificial Intelligence Act (AI Act), EU Cyber Resilience Act (CRA) and applicable national data protection laws. This Privacy Policy contains important information regarding personal data, the methods of its collection, use, and protection, and should therefore be carefully reviewed.

2.1. IDENTIFICATION OF THE DATA CONTROLLER

Personal data is processed, as appropriate in each case, by FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), and/or the relevant subsidiaries as data controllers, for the purposes described in this Privacy Policy.

2.2. FUTURELIFE AS DATA CONTROLLER

Personal data is collected and processed by FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), as the data controller, within the scope of organisational activities, for example, when subscribing to newsletters or requesting information through contact forms. The identification details of FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), as the data controller are as follows:

2.2.1. FUTURELIFE GROUP SUBSIDIARIES AS DATA CONTROLLERS.

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), are considered the data controllers of personal data processed within the scope of its own operational activities, including the provision of healthcare services, patient record management, and other legitimate business functions. The subsidiary operating the healthcare centre or clinic that initiates contact and processes personal data for the purposes above is regarded as the data controller of such data. A comprehensive list of FutureLife a.s. subsidiaries and their associated healthcare clinics, along with contact details is available upon request at the following email address: dpo@futurelifegroup.com

Medical records are processed exclusively by the relevant provider of FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"). Under no circumstances does FutureLife Group have access to identifiable medical information.

2.2.2. FUTURELIFE AND THE RELEVANT SUBSIDIARIES AS JOINT CONTROLLERS.

Depending on the specific activities involved, FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), and its subsidiaries may also act as joint controllers for the processing of users' data, particularly for marketing purposes, sending commercial communications about the FutureLife a.s., conducting market research and quality surveys, and other operational and organisational functions at the group level.

2.3. FUTURELIFE SECURITY INCIDENT MANAGEMENT

Incidents involving personal data protection are handled in accordance with Future Life Group's own **Cybersecurity Response Plan (FL-CS-OP2)**. This plan defines procedures for identifying, assessing, reporting, and resolving security events that may result in a personal data breach. The objective is to minimize the impact on data subjects, ensure appropriate remediation, and comply with legal obligations, including potential notification to supervisory authorities and affected individuals.

3. ROLES AND RESPONSIBILITIES

This section outlines the key roles within FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), and their responsibilities regarding personal data protection.

A detailed RACI matrix outlining roles and responsibilities in relation to Privacy Policy compliance is provided in Annexe B for reference.

3.1. DATA PROTECTION OFFICER

In terms of data privacy, the DPO must:

- Monitor compliance with GDPR and other applicable data protection laws.
- Serve as the contact point for supervisory authorities.
- Provide guidance and training on data protection matters.
- Conduct internal audits and assessments.
- Advise on Data Protection Impact Assessments (DPIA).
- Review and update the Personal Data Register.
- Review and update of data processing, mapping, and diagrams.
- Maintain records of processing activities.

3.2. CHIEF TRANSFORMATION OFFICER

In terms of data privacy, the CTO must:

- Approve and oversee the implementation of the Global Data Privacy Policy.
- Lead strategic initiatives related to data protection across the organisation.
- Ensure alignment of privacy practices with business transformation goals.
- Support cross-functional coordination on privacy-related matters.
- Provide training and awareness on data protection to staff.
- Support disciplinary actions related to data breaches.

3.3. HEAD OF LEGAL

In terms of data privacy, the Head of Legal must:

- Implement and maintain technical safeguards for personal data.
- Respond to and manage data breaches and cybersecurity incidents.
- Support data retention and deletion processes.
- Collaborate with the DPO on system-level compliance.
- Conduct regular security tests, penetration testing, and risk analyses.
- Provide training to employees on cybersecurity and secure data handling practices.
- Collaborate with external vendors to ensure the security of systems and data flows.
- Ensure encryption, access control, and other technical measures for data protection.

3.4. LOCAL SECURITY OFFICER

In terms of data privacy, the local Security Officer must:

- Ensure local compliance with the privacy policy and GDPR.
- Oversee secure handling of patient records and sensitive data.
- Train clinic staff on data protection procedures.

- Report data incidents to central governance.
- Serves as DPO.
- Coordinate with the DPO and IT Manager on clinic-level risks.

3.5. Cybersecurity Manager

In terms of data privacy, the Cybersecurity Manager must:

- Design, implement, and maintain security measures to protect personal data.
- Monitor cyber threats and vulnerabilities that may compromise personal data.
- Coordinate responses to security incidents and data breaches in collaboration with the DPO and Head of Legal.

3.6. Business Owner

In terms of data privacy, the Business Owner must:

- Ensure that personal data processing activities within their business domain comply with the Global Data Privacy Policy and applicable legislation (e.g. GDPR).
- Collaborate with the Data Protection Officer (DPO) to identify and mitigate privacy risks.
- Ensure that suppliers and systems selected for their business area meet privacy and security requirements.

Maintain accountability for the lawful use of personal data in applications and services under their responsibility.

3.7. Functional Owner

In terms of data privacy, the Functional Owner must:

- Maintain operational compliance with data protection requirements within their functional area.
- Lead the execution of DPIAs in collaboration with the Business Owner and DPO.
- Ensure that data processing procedures are documented and aligned with internal privacy standards.
- Support audits, reviews, and updates of systems and applications that process personal data.
- Initiate and oversee the creation of Data Protection Impact Assessments (DPIAs) for new or significantly changed processing activities.

Coordinate with IT and Legal to ensure technical and organisational measures are implemented.

3.8. Human Resources

In terms of data privacy, the HR must:

- Ensure lawful processing of employee personal data.
- Manage data protection during recruitment, onboarding, and offboarding.
- Maintain confidentiality of HR records.

3.9. All Employees

In terms of data privacy, all employees must:

- Follow internal data protection policies and procedures.
- Participate in mandatory privacy and cybersecurity training.
- Report suspected data breaches or misuse.
- Handle personal data responsibly and securely.

3.10. External Contractors and 3rd parties

In terms of data privacy, all external contractors and 3rd parties must:

- Process personal data only as instructed by FutureLife.
- Comply with contractual data protection obligations.
- Implement appropriate technical and organisational measures.
- Sign and adhere to non-disclosure agreements and DPAs.
- Cooperate during audits and assessments.

4. MANAGEMENT OF PERSONAL DATA

Some services may be accessed without providing personal data. However, for functionalities such as registration, newsletters, or tailored communication, personal data is required.

Data is collected:

- Directly via forms, calls, or emails.
- Indirectly through cookies and other tracking technologies.

Mandatory fields are marked with an asterisk (*); without them, services cannot be delivered. Details on data categories, purposes, and retention periods are provided in Annexe A: Categories of Personal Data and Purposes of the Processing.

4.1. SECURITY

The security and confidentiality of personal data is ensured by a necessary set of security and technical measures outlined in the **Cybersecurity Policy (FL-CS-P1)**, which has been implemented to prevent the loss, misuse, or unauthorised access to personal data without the data subject's consent, in accordance with the GDPR and applicable national data protection laws.

At the same time, responsibility for the protection of personal data is also placed on the data subject. Therefore, the data subject is encouraged to exercise caution when sharing information and content. The FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), do not monitor the content and information chosen to be shared with others, and the consequences of such decisions are not the responsibility of the Group.

4.2. COOKIES

Much of the information referred to in this Global Data Privacy Policy is **collected through the use of cookies**. Cookies are small text files containing limited amounts of information that are downloaded and stored on the user's device, such as a computer, smartphone, or tablet. These cookies are sometimes required for remembering account settings, language, and country. They are also used to track and analyse user behaviour on the Website and to display personalised advertisements either on the Website or on third-party websites.

Where necessary, consent to the use of cookies is requested from the user. For additional information on how cookies are used within the Services and how they can be deactivated, please refer to the Cookies Policy.

4.3. USERS' RIGHTS CONCERNING DATA PROTECTION

Data subjects may exercise their rights at any time, including access, rectification, restriction, erasure, objection, and data portability, in line with applicable legislation:

- **The Data Protection Officer (DPO):** Responsible for managing and verifying all rights requests.
- **The Head of Legal:** Ensures legal compliance and supports responses to complex cases.
- **The Local Security Officer:** Coordinates local execution and reporting.
- **The HR department:** Handles employee-related requests.
- **The Business Owner:** Ensures that requests related to their systems are properly addressed.
- **The Functional Owner:** Supports technical execution and data blocking where applicable.

Upon receiving a valid request:

- Processing of the relevant personal data must be suspended.
- Data must be blocked during the verification period.
- If an objection is raised, data must not be further processed unless legally justified.

Requests must be submitted via email to dpo@futurelifegroup.com with the subject line "Data Privacy Subject" and a clear specification of the right being exercised.

Complaints may be lodged with the relevant supervisory authority if data is believed to be processed unlawfully.

4.4. Types and Activities of Personal Data Processing

The following list outlines the main types and activities of personal data processing carried out within the FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"). These activities are conducted in accordance with the GDPR and applicable national data protection laws:

- **Patient Data Management:** Collection, storage, and processing of personal and health-related data for the purpose of providing medical services and maintaining medical records.
- **Appointment Scheduling:** Processing of contact and identification data to manage patient appointments and communications.
- **Communication and Support:** Use of personal data to respond to inquiries, provide support, and deliver requested information.
- **Marketing and Commercial Communication:** Processing of contact data for sending newsletters, promotional materials, and satisfaction surveys, subject to consent.
- **Website and Cookie Tracking:** Collection of data through cookies and similar technologies to analyse website usage and personalize content.
- **Recruitment and HR Management:** Processing of personal data of job applicants and employees for recruitment, onboarding, payroll, and performance management.
- **Legal and Regulatory Compliance:** Processing of data to comply with legal obligations, including retention, audits, and reporting to authorities.
- **Insurance and Billing:** Sharing of necessary data with insurance companies and billing entities for claim processing and payment management.
- **IT and Security Operations:** Use of personal data in system logs, access control, encryption, and cybersecurity monitoring.
- **Research and Statistical Analysis:** Anonymized or pseudonymized data used for scientific research and internal statistical purposes.
- **Data Subject Rights Management:** Processing of personal data to handle requests related to access, rectification, erasure, and other GDPR rights.
- **Vendor and Contractor Management:** Sharing of personal data with third-party service providers under contractual obligations and safeguards.
- **Cross-border Data Transfers:** – Transfer of personal data to entities outside the EEA under appropriate safeguards and legal mechanisms.

4.5. DATA REGISTER

The data register is a **central record of all personal data processing activities** carried out by FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"). It ensures transparency, accountability and compliance with GDPR. The data register documents the lawful, secure, and ethical handling of highly sensitive personal and health-related data.

4.5.1. SCOPE

All categories of personal data processed by FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), are covered in the data register, including but not limited to:

- Patient and partner medical records.
- Genetic, biometric, and laboratory data.
- Reproductive health and treatment data.
- Administrative, financial, and insurance details.
- Staff and contractor information.
- Data processed through third parties (e.g., laboratories, storage facilities, IT providers).

4.5.2. RESPONSIBILITY

- The **Data Protection Officer (DPO)** is responsible for maintaining, reviewing, and updating the data register.
- The relevant stakeholders are required to notify the DPO od any new or modified processing activities.
- The DPO ensures that the data register remains accurate, complete, and available for review by the competent Data Protection Authority (DPA) upon request.

4.5.3. CONTENTS

For each processing activity, the following information is recorded:

- **Controller details:** Name, address, and contact information of the clinic.
- **Purpose of processing:** Clinical care, diagnostics, research (where applicable), billing, or administrative functions.
- **Categories of data subjects:** Patients, partners, donors, children born as a result of treatment, staff, and contractors.
- **Categories of personal data:** Identification details, contact data, medical history, reproductive health data, genetic data, laboratory test results, billing and insurance details.
- **Special category data:** Explicitly marked, including genetic and reproductive health information.
- **Recipients of data:** Internal teams, laboratories, hospitals, storage providers, insurers, and regulatory bodies.

- **Transfers to third countries:** Where applicable, details of safeguards are in place (see section 4.9 Data transfers for details).
- **Retention periods:** Defined timelines according to medical, legal, and regulatory requirements (see section 4.10. Retention Period for details).
- **Security measures:** Technical and organizational measures applied (e.g., encryption, pseudonymisation, access control).

4.5.4. Breach Register Linkage

The data register is **linked to the breach management process**. Any personal data breaches recorded must specify the relevant processing activity entry in the register to ensure accountability and traceability.

4.5.5. Review and Updates

The data register is **reviewed at least annually** or upon significant changes in processing activities. Updates are mandatory when:

- New treatments, technologies, or diagnostic methods are introduced.
- New third-party processors are engaged.
- Legal or regulatory requirements change.

4.6. Zero Trust Architecture Principles

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), commit to adopting a Zero Trust Architecture (ZTA), a cybersecurity model aligning with NIST SP 800-207 and EU healthcare cybersecurity strategies, which assumes no user, device, or system is inherently trustworthy – a principle under which every access must be continuously verified based on identity, context, and behaviour.

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), strive to adopt following ZTA principles across all systems handling sensitive reproductive and genetic data:

- Enforce least privilege access and continuous authentication.
- Apply micro-segmentation to isolate critical systems.
- Monitor all access in real time.
- Align implementation with NIST SP 800-207.

4.7. Patient Consent Management

Due to the highly sensitive nature of fertility and medical data processed, FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), **obtain, record and respect patient consent:**

- **Consent Collection**
  - Collecting consent where required by law, particularly for the processing of special category data (e.g., fertility, genetic, medical) and for any secondary use of data.

- Consent is obtained through a patient consent form, which explains the purpose of processing, the data involved, and the patients' rights.
- Consent is always freely given, specific, informed, and unambiguous.

> **Consent Management**

- Consent preferences are securely stored.
- Only authorised staff can access or update the consent status.
- If a treatment or participation in research requires an ongoing consent, regular opportunities to confirm or update consent will be provided.

> **Withdrawal of Consent**

- The patient may withdraw their consent at any time, without affecting the legality of processing carried out before withdrawal.
- Withdrawal will not affect the care the patient receives.
- Reaction to withdrawal requests will be prompt.

> **Record Maintenance**

- Maintaining a complete record of when, how, and for what purpose the record was obtained (electronic audit logs, signed consent forms).
- Records are retained securely for as long as legally required.
- In the event of consent withdrawal, records will be updated accordingly and will restrict or cease processing relevant data.

4.8. Sharing Personal Data

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), have safeguards in place in cases personal data must be shared with third parties or external service providers:

a) **Insurance companies and mutual insurance entities (including those of third parties in cases involving civil liability insurance):**
   > Personal data may be shared to verify coverage and manage payment of expenses.
   > Only strictly necessary data is shared – no medical or sensitive health data disclosed.
   > If the insurer is outside the EEA without equivalent data protection:
      - Data transfer may be required for claim processing.
      - Transfer occurs only with explicit informed consent.
      - Only the minimum necessary data is transferred.
      - If consent is withheld, the insurer may refuse coverage, and the patient may bear full costs.

b) **Subsidiaries of FutureLife a.s.:**
   > Minimal necessary personal data may be shared for referrals with other clinics of FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group").
   > Ensure continuity and quality of care.

c) **External contractors and service providers:**

- Data may be shared with partners providing medical care, diagnostics, clinical analysis, auditing, security, IT support, legal advice, and other administrative functions.
- Contractors may also manage and maintain digital platforms and applications.
- Data is shared only to the extent necessary for the provision of services.

d) Legal professionals, advisors, and authorities:

- Data may be shared to exercise rights, handle complaints, or obtain legal advice.
- Recipients may be within or outside the EEA – for transfers outside the EEA, Standard Contractual Clauses ensure adequate protection.
- Data may be shared to exercise rights, handle complaints, or obtain legal advice.
- Recipients may be within or outside the EEA – for transfers outside the EEA, Standard Contractual Clauses ensure adequate protection.
- All providers must safeguard confidentiality and security in line with GDPR.

4.9. DATA TRANSFERS

Under the GDPR, medical and fertility data **may flow freely within the EU/EEA but must be processed with strict safeguards**. Secondary uses such as research or registries require explicit consent and strong protections. **From 2025, the European Health Sata Space (EHDS) will further strengthen cross-border patient rights** and set new rules for secondary use of sensitive health data.

4.9.1. FLOW OF DATA & COMPLIANCE

The transfer of personal data within the EU/EEA is not subject to additional restrictions for data protection reasons, therefore there is no need for Standard Contractual Clauses (SCCs) or adequacy checks, however **compliance with GDPR is still required when transferring data:**

- **Data minimisation:** Only share necessary information.
- **Purpose limitation:** Only process data for defined medical purposes.
- **Integrity & confidentiality:** Protect against unauthorised access or loss.
- **Transparency:** Patients must be informed if their data is shared against borders.
- **Data subject rights:** Patients can access, correct, restrict, or request deletion.
- **Security:** Encryption, access controls, audit logs.

4.9.2. SECONDARY USE OF FERTILITY DATA

When data is used beyond direct treatment, rules are much stricter. **Secondary use (e.g. research, quality improvement, training, registry, product development, marketing) of patient fertility data requires:**

- **Explicit consent:** Data will only be processed if the patient has provided their explicit consent.
- **Safeguards:** Pseudonymisation or anonymisation.
- **Transparency:** Patients must know what research their data supports and be able to withdraw consent.

4.9.3. INTERNATIONAL TRANSFERS

The transfer of medical or fertility data outside the EU/EEA will only take place in compliance with GDPR. Where the European Commission has issued an **adequacy decision**, the data may be transferred to those countries (e.g., Switzerland, Japan). For other destinations, **Standard Contractual Clauses (SCCs)** are used, and **transfer risk assessments** are conducted in line with post-Schrems II requirements. In exceptional, case-specific situations, derogations may be used (e.g., an explicit consent for a one-off laboratory test abroad).

4.10. RETENTION PERIOD

Personal data is **retained for as long as necessary** to fulfil the purpose for which it was collected. In some instances, data may continue to be processed after the original purpose has been fulfilled, for example, if the data subject becomes a client.

Retention periods are determined as follows:

- **Medical records:** Are retained for the period required by law, typically 10 years from the end of treatment or discharge, in accordance with healthcare regulations. The exception is the traceability of reproductive substances which must be retained for up to 30 years.
- **Genetic Data:** In line with the applicable legislation must be retained for a period of at least 30 years from the end of treatment or discharge.
- **Data for legal and administrative purposes:** After the initial retention period, personal data may be stored for up to 3 years, corresponding to the statutory limitation period, to ensure legal protection and compliance.
- **Data for research purposes:** May be retained in anonymised form for the duration of the research project, usually 5–10 years, in accordance with applicable laws. Data may be shared with accredited research institutions for legitimate research purposes.
- **Data related to inquiries, complaints, or rights requests:** Is retained for the time necessary to process the request, typically 1–2 years and may be stored longer if required for legal or regulatory reasons or to protect the organisation's interests in case of disputes.
- **Data related to contractual relationships:** Is retained for the duration of the contract and subsequently for 5 years after its termination, to manage potential claims or disputes.
- **Newsletter subscription data**: Is retained until consent is withdrawn or the subscription is cancelled.

4.11. DATA DELETION

The security of data deletion procedures is guaranteed through appropriate technical and organisational measures. Documented, verifiable, and secure methods for erasing data are established by FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), in accordance with the General Data Protection Regulation (GDPR) and the Substances of Human Origin Regulation (SoHO).

4.11.1. RIGHT TO ERASURE

Individuals have the **right to request erasure of their personal data without undue delay**. This includes situations where the data is no longer necessary for its original purpose, consent is withdrawn, or the data was unlawfully processed.

4.11.2. Limitations in healthcare context

The Right to Erasure **in healthcare is limited by legal retention obligations and/or public health and research exemptions**. Under GDPR, medical and fertility data fall under special category data (sometimes called "sensitive personal data"). Consequently, their processing requires explicit consent or another lawful basis, and additional safeguards. The EU SoHO Regulation mandates long-term traceability (unique non-identifying codes, e.g. Single European Code) of reproductive substances such as gametes and embryos, often up to 30 years. Therefore, clinics may not be able to fully erase certain health records even upon request.

4.11.3. Secure deletion techniques

All deletion activities must be logged and verifiable.

- **Digital Data**
  - **Cryptographic erasure:** destroying encryption keys to render data unreadable.
  - **Data Wiping:** use certified tools to overwrite storage with random patterns.
  - **Certified deletion tools:** using EU-approved software for secure erasure.
- **Backups & Archives**
  - **Retention schedules:** automatically delete or overwrite expired backup data.
  - **Separation of duties:** Only authorised staff can delete sensitive data.
  - **Immutable logging:** Ensure deletions in backups are tracked.
- **Paper & Physical media:** Shedding, pulping or incineration, shredding, pulverising.

4.11.4. Documentation and auditing

All data deletion procedures must be documented. This includes specifying retention periods, deletion triggers, and exceptions. Regular audits are required to verify compliance with GDPR and SoHO obligations. Audit trails must be maintained for all deletion actions.

4.12. Notification of data protection authorities

In the event of a personal data breach, the relevant supervisory authority must be notified without undue delay, and where feasible, within 72 hours of becoming aware of the incident. All FutureLife entities must follow internal procedures for incident reporting. Documentation of the breach and notification process must be maintained for audit and compliance purposes.

The Data Protection Officer (DPO) is responsible for:

- Coordinating the notification process.
- Maintaining and updating the data register, ensuring that records of processing activities are accurate, complete, and up to date.
- Preparing the breach report, including:
  - Nature and scope of the breach.
  - Categories and number of affected data subjects and records.
  - Contact details for follow-up.
  - Likely consequences and mitigation measures.

The Local Security Officer must:

- Ensure timely escalation from local entities to the DPO.

The Head of Legal must:

- Review the legal implications and supports communication with authorities.

4.13. Third-party risk management

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), ensure that all third-party service providers and contractors who process personal data on their behalf are subject to rigorous privacy and security standards aligning with FutureLife's own internal policies. FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), maintain a **Vendor Risk Register and follow the internal Supplier Cybersecurity Standard (FL-CS-S2)**.

4.13.1. Due diligence before onboarding

- All 3rd parties must complete a Data Protection and Security Questionnaire.
- **Risk assessments are conducted** to evaluate data handling practices, certifications (e.g., ISO 27001), and regulatory compliance.
- Data Processing Agreements (DPAs) are signed before any data is shared.

4.13.2. Monitoring

- Annual audits or assessments are conducted for high-risk 3rd party providers.
- Breach history, incident response capabilities, and subcontractor use are reviewed.
- 3rd parties must notify FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), of any data breaches or changes in processing activities.

4.14. Personal Data Processing Mappings and Diagrams

To support clarity and compliance, visual mappings and flow diagrams of personal data processing activities must be developed and maintained. **These diagrams must illustrate:**

- Data flows across systems and departments.
- Points of data collection, storage, and transfer.
- Interfaces with third-party processors.
- Locations of data storage (including cloud services and cross-border transfers).

These mappings must be used to:

- Identify risks and gaps in data protection.
- Support Data Protection Impact Assessments (DPIAs).
- Facilitate internal audits and training.

All diagrams must be reviewed by the DPO every two years or upon significant changes to processing activities.

4.15. Data Protection Impact Assessments (DPIA)

DPIAs must be conducted before initiating any processing activity that is likely to result in a high risk to the rights and freedoms of individuals. This includes, but is not limited to:

- Large-scale processing of sensitive data.
- Systematic monitoring of publicly accessible areas.
- Use of new technologies or profiling techniques.

Each DPIA must include:

- A description of the processing and its purpose.
- An assessment of necessity and proportionality.
- Identification of risks to data subjects.
- Measures to mitigate identified risks.

DPIAs must be documented and retained by the DPO. Where necessary, consultation with supervisory authorities must be initiated before processing.

4.16. STAFF TRAINING AND AWARENESS

All staff with access to personal or reproductive data complete mandatory annual training on GDPR, the European Health Data Space (EHDS), and cybersecurity, with specialized modules for lab technicians (secure handling of donor and embryology data), clinicians (confidentiality and consent management), and IT staff (system security and access controls). To reinforce awareness, the clinic runs phishing simulations and cyber hygiene campaigns, and completion of training is monitored to ensure ongoing compliance and protection of sensitive fertility and donor data.

4.17. PRIVACY POLICY REVIEW AND GOVERNANCE

The Future Life Group Global Data Privacy Policy shall be reviewed annually, or immediately upon significant regulatory changes. The review process is coordinated by the Data Protection Officer (DPO) in collaboration with the Head of Legal, Cybersecurity Manager, and Chief Transformation Officer. Clinic leadership and local legal counsel are responsible for validating the applicability of the policy at the subsidiary level and ensuring alignment with local regulations. All updates must be documented in the version control table and communicated to relevant stakeholders. A summary of the changes shall be included in the policy update notice.

4.18. POLICY ACCESSIBILITY

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the “FutureLife Group”), are committed to ensuring that this Global Data Privacy Policy is accessible to all individuals. Requests for alternative formats may be submitted to the Data Protection Officer (DPO).

Accessibility measures:

- The policy is available in all official languages of the countries where FutureLife operates.
- Accessible formats (e.g., large print, screen-reader compatible PDFs) are available upon request.
- Clinics display printed copies of the policy in reception areas and provide digital access via websites and/or patient portals.
- Staff are trained to assist patients in understanding the policy and exercising their rights.

4.19. PRIVACY POLICY UPDATES

The right to modify or replace this Global Data Privacy Policy is reserved at the sole discretion of FutureLife a.s., and any of its affiliates belonging to the same corporate group (the “FutureLife Group”).

Continued use of the services following any such changes must be considered as acceptance of the updated Privacy Policy.

Users are advised to review this agreement periodically to remain informed of any potential modifications. If this document, in whole or in part, or any subsequent changes are not accepted by the data subject, the services should no longer be accessed or used, and any ongoing use must be discontinued immediately.

4.20. Data Privacy Annex (DPA)

The Data Privacy Annex (DPA) is a mandatory component of the group's data protection framework. It serves as a formal document that outlines the specific privacy and data protection requirements applicable to each application, system, or service that processes personal data, which ensures transparency, accountability, and consistency in managing data across the FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group").

The purpose of the DPA is to ensure that all processing activities are clearly defined, compliant with applicable data protection laws (such as the GDPR) and aligned with the group's internal privacy standards. DPA must includes details:

- The categories of personal data being processed
- The legal basis for processing
- Data retention periods
- Security measures in place
- Roles and responsibilities of involved parties
- Any data transfers outside the EU/EEA, if applicable

4.21. Data breach Notification to individuals

In addition to notifying supervisory authorities, FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), are committed to informing the affected individuals without undue delay in the event of a personal data breach, when such a breach is likely to result in a high risk to their rights and freedoms.

4.21.1. Criteria

- The breach involves sensitive health, fertility, or genetic data.
- The breach may lead to identity theft, discrimination, reputational harm, or other significant consequences.

4.21.2. Communication channels & timelines

- Without undue delay and where feasible, affected individuals will be notified via email, phone, or secure patient portal within 72 hours of breach confirmation.
- The nature of the breach, likely consequences, mitigation measures, and contact details for further information will be included in the notification.
- Where direct communication is not possible, public announcements will be made via the clinic's website or media channels.

4.22. USE OF ARTIFICIAL INTELLIGENCE AND AUTOMATED DECISION-MAKING

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), may use Artificial Intelligence (AI) and automated decision-making tools in order to support clinical and operational processes. These tools are used to enhance accuracy, efficiency, and quality of care. Nonetheless, no decisions with significant legal or medical impact are made solely by automated systems – all such decisions are subject to human oversight and clinical review.

Any system incorporating an AI model must comply with:

- **Any internal or external AI development:**
  - FL-CS-OP-09 New System Security Requirements.
  - Have a dedicated Business Impact Assessment (BIA) completed.
- **Any internally or externally purchased and implemented system:**
  - FL-CS-OP-03 Secure System Development Life Cycle.

The AI and automated decision-making processes employed might include:

- Embryo grading and selection
- Donor-recipient matching algorithms
- Genetic risk analysis
- Predictive modelling for treatment outcomes
- Automated triage and appointment scheduling

Patients have the right to:

- Be informed about the use of AI in their care
- Express their point of view
- Request human intervention
- Contest decisions made through automated processing

Where applicable, Data Protection Impact Assessments (DPIAs) are conducted in order to estimate the risks and to ensure compliance with GDPR (Article 22) and related provisions.

4.22.1. EU ARTIFICIAL INTELLIGENCE ACT (AI ACT)

IVF clinics are increasingly using **AI-driven tools, which are now regulated under the EU AI Act**. FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), will strive to implement a structured AI Conformity Assessment Framework for all AI systems used in clinical decision-making (e.g., embryo grading, donor matching).

This includes:

- Pre-deployment conformity assessments (Annex VI/VII of the AI Act).
- Establishing a Post-Market Monitoring System (PMMS).
- Assigning oversight to the DPO and Cybersecurity Manager.
- Maintaining technical documentation and risk logs.

4.23. Donor and Offspring Data Protection

Future Life Group complies with the EU regulatory framework on Substances of Human Origin (SoHO) to ensure the highest standards of safety, traceability, and privacy in the handling of donor and offspring data. These rules are designed to ensure the need for long-term traceability and public health protections while also safeguarding donor anonymity, patient confidentiality, and the privacy of children conceived through donation.

4.23.1. Unique coding & traceability

All donor materials are assigned a unique, non-identifying code (such as the Single European Code), to ensure full traceability from donation through clinical application, while preserving donor and patient anonymity. Any directly identifiable information is stored separately and securely, accessible only to authorised staff for purposes permitted by law. The separation of coding and identity ensures compliance with regulatory requirements, facilitates quality and safety monitoring, and protects the confidentiality of both donors and recipients.

4.23.2. Serious adverse events and reactions

Formal procedures for the identification, documentation, and reporting of **Serious Adverse Events (SAEs) and Serious Adverse Reactions (SARs)** are maintained in line with applicable EU and national regulatory requirements. All incidents are recorded, investigated, and, where required, reported to the competent authorities within the prescribed timeframes. Patients and donors will be informed without undue delay where the event or reaction is relevant to their care, safety, or ongoing treatment.

4.23.3. Right to restrict access

Under GDPR, patients and donors have the right to request a **restriction of processing of their personal and reproductive data**. Because fertility and reproduction data constitute special category data, individuals have enhanced rights to explicitly consent to its use and to withdraw consent at any time.

Technical and organisational measures implemented by the clinic **to enforce data restriction** include:

- **Role-based access controls:** Ensure only authorised personnel can view sensitive files.
- **Segregation of donor and recipient records:** Prevention of undesired linkage.
- **Comprehensive access logs:** Monitoring and auditing all access to reproductive data.

4.23.4. Donor anonymity vs. Patient rights

In some EU Member States, national law grants **donor-conceived children the right to access identifying donor data** once they reach maturity. In such cases, where legally applicable, Future Life Group complies with legal obligations while maintaining the highest standards of data security and minimisation.

4.23.5. Genetic risk minimisation

A fundamental obligation under EU SoHO Regulation (requires quality and safety standards for substance of human origin), GDPR (regulates the processing of genetic data) and national health laws. The objective of genetic risk minimisation is to **reduce the probability of transmitting inheritable diseases or genetic conditions** from donor gametes (sperm/eggs) or embryos to recipients and their future children.

The elements of genetic risk minimisation are:

- **Medical and Family History**
  - Donors complete detailed questionnaires covering family health history (up to 2–3 generations).
  - Conditions screened for: cardiovascular disease, cancer syndromes, neurological disorders, metabolic conditions, congenital anomalies.
- **Physical Examination**
  - Clinical assessment to exclude obvious risk factors (e.g., developmental anomalies).
- **Laboratory testing**
  - Standard infectious disease screening (HIV, HBV, HCV, syphilis, CMV).
  - Genetic disease carrier screening (e.g., cystic fibrosis, thalassemia, Tay-Sachs, SMA).
  - Chromosomal analysis (karyotyping) where required.
- **Genetic Counselling**
  - Where risk factors are identified, professional counselling is offered to donors and, where relevant, to intended parents.
  - Counselling helps assess residual risks and informs decisions about donor eligibility.
- **Donor Exclusion Criteria**
  - Donors with known inheritable diseases or high-risk carrier status for serious conditions are excluded.
  - Some jurisdictions allow exceptions with explicit informed consent of the recipient, but this is rare.

4.24. CHILDREN'S DATA AND PARENTAL CONSENT

The services and business activities of FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), are not intended to be used by individuals under the legal age nor is personal data of such persons intentionally collected or processed. The services of FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), are designed for persons who have reached the age of majority.

In cases where certain services are specifically directed at minors, the consent of parents or legal guardians is required for the collection of personal data, in accordance with applicable legislation. If a data subject is a minor, prior consent from a parent or legal guardian must be obtained before any personal data is provided to FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group").

4.24.1. VERIFICATION OF AGE & DOCUMENTATION

Clinics must verify the age of the data subject through official identification documents before initiating any data collection or treatment.

All consent forms must be signed, dated, and securely stored. Electronic audit trails are maintained.

4.24.2. Fertility preservation procedures for minors

In certain exceptional cases, it is possible and necessary to treat individuals under the age of majority. These cases typically include cases of fertility preservation in children with serious medical conditions like cancer.

A) Ovarian Tissue Cryopreservation

Ovarian tissue cryopreservation is the most common and primary method for preserving fertility in pre-pubescent children. This procedure involves surgically removing ovarian tissue that contains immature eggs, which are then frozen for later use. Later, if the individual desires to have children, the tissue can be transplanted back into the body, or the immature eggs can be matured in a lab and then used.

B) Ovarian Stimulation & Mature Egg Retrieval

For adolescents who have started puberty and developed mature eggs, there is the option of ovarian stimulation & mature egg retrieval. The ovaries can be stimulated using hormones, followed by the retrieval of mature eggs for freezing.

4.24.3. Considerations

- **Medical necessity:** Procedures are usually performed when a child's medical condition or the treatment of that condition could lead to infertility.
- **Consent:** Consent is always required from both the patient (if mature enough) and their parents/legal guardians.
- **Research:** Currently, research is ongoing to find other fertility preservation options for children who have not yet gone through puberty.

4.24.4. Right to withdraw consent

Parents or guardians may withdraw consent at any time. Upon withdrawal, processing of the minor's data will be restricted or ceased, unless required by law.

4.24.5. Jurisdictional compliance

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the “FutureLife Group”) must ensure compliance with national laws regarding the age of medical consent and fertility treatment eligibility.

5. EU RESILIENCE ACT CERTIFICATION (CRA)

The Cyber Resilience Act Certification (CRA), which entered into effect in 2024, but its primary obligations will become fully applicable by December 2027, regulates the cybersecurity of "products with digital elements" (PDEs), including hardware and software, sold in EU market. Manufacturers, importers, and distributors will have cybersecurity-related responsibilities, such as cybersecurity risk assessments and the documentation of compliance efforts.

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") shall prepare for the Cyber Resilience Act Certification (CRA) compliance by:

- Identifying all products with digital elements (PDEs) - e.g., EHRs, AI tools.
- Ensuring secure-by-design development.
- Implementing vulnerability handling procedures.
- Coordinating CRA certification through the Cybersecurity Mananager.

5.1.1. TIMELINE OF IMPLEMENTATION & READINESS

2025 – 2026: Preparation & Gap Analysis

- **Identify all products with digital elements (PDEs):**
  - EHR systems
  - AI embryo grading tools
  - Donor databases
  - Cryo-storage monitoring systems
- **Conduct CRA gap Assessment**
  - Compare current cybersecurity controls against CRA Annex I & II requirements
  - Include secure system development lifecycle, vulnerability disclosure, and incident response
- **Assign CRA Compliance Roles**
  - Appoint a CRA Compliance Officer or integrate the role into the Cybersecurity Manager's role
  - Define responsibilities for CE marking, documentation, and vendor coordination.

2026 – 2027: Secure-by-Design Implementation

- **Integrate Secure-by-Design Principles**
  - Apply threat modeling during system design
  - Enforce least privilege, data minimisation, and access control
- **Update Procurement Procedures**
  - Require CRA compliance from all vendors

- Include security clauses in contracts (e.g., vulnerability handling, patch timelines)

> **Implement Technical Controls**

- Encryption (AES-256)
- Multi-factor authentication (MFA) and Zero Trust Architecture (ZTA)
- Immutable logging (WORM or blockchain)

2027 – 2028: CE Marking & Documentation

> **Prepare Technical Documentation**

- Risk assessment
- Security architecture
- Vulnerability management procedures
- Incident response plans

> **Conduct Conformity Assessment**

- For non-critical PDEs: self-assessment under Annex III
- For critical PDEs (e.g., AI tools): third-party assessment under Annex IV

> **Apply CE marking**

- Submit documentation to national authority or notified body
- Affix CE mark to compliant systems

2028 and onwards: Post-market Surveillance & Continuous Improvement

> **Establish Post-Market Monitoring System**

- Track performance, vulnerabilities, and incidents
- Maintain logs and audit trails

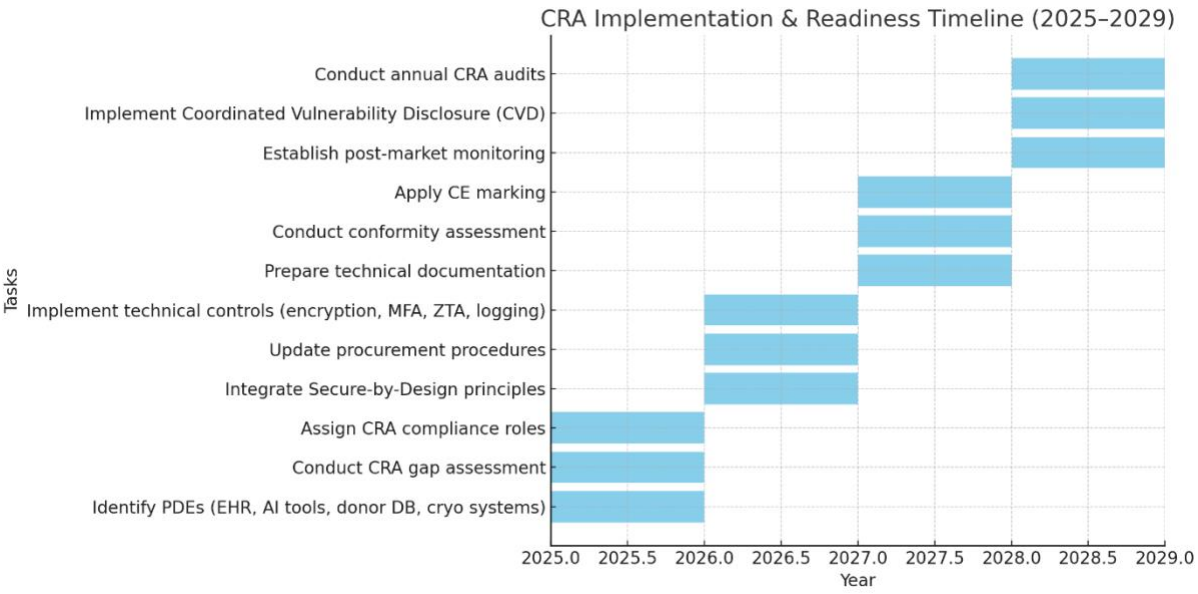
> **Implement Coordinated Vulnerability Disclosure (CVD)**

- Create a public-facing vulnerability reporting channel
- Respond within CRA-defined timelines

> **Conduct Annual CRA Audits**

- Internal or external review of compliance
- Update documentation and CE marking as needed

FutureLife Planned CRA Implementation Timeline:



6. EUROPEAN HEALTH DATA SPACE (EHDS)

The FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), **shall commit to implementing the European Health Data Space (EHDS)** - a regulatory framework **coming into effect in 2025** designed to facilitate secure and efficient access, sharing, and use of health data across EU Member States.

6.1.1. PRIMARY USE OF HEALTH DATA

The compliance with EHDS regulations in regards with the processing of all personal health data for direct patient care will be warranted and **the following principles will be applied**:

- **Interoperability:** Systems shall be upgraded to support EHDS technical standards for data formats, exchange protocols, and semantic consistency.
- **Access Rights:** Patients shall be able to access their health data across borders, including reproductive and fertility records, in a secure and user-friendly manner.
- **Data Portability:** Mechanisms shall be developed to allow patients to transfer their health data between FutureLife clinics and other authorised healthcare providers within the EU.

6.1.2. SECONDARY USE OF HEALTH DATA

FutureLife supports the **ethical and lawful** secondary use of health data for research, innovation, and public health purposes under EHDS:

- **Explicit Consent:** Secondary use of fertility and genetic data requires documented, informed, and explicit consent from the data subject.

- **Data Minimisation & Pseudonymisation:** Only the minimum necessary data is used, and identifiers are removed or masked to protect privacy.
- **Transparency:** Patients are informed about the nature, purpose, and recipients of secondary data use, and may withdraw consent at any time. Opt-out mechanisms will be offered to patients with clear and reversible procedures.

6.1.3. European Electronic Health Record Exchange Format (EEHRXF)

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), are actively implementing the European Electronic Health Record Exchange Format (EEHRXF). The EEHRXF is the **technical foundation** of the EHDS for primary use of health data - it ensures interoperability across Member States. It is the standard that makes cross-border, patient-controlled data exchange possible within the EHDS. It applies to structuring and **exchanging key categories of electronic health** data such as **patient summaries, E-prescriptions, laboratory results, medical images & reports, hospital discharge reports and rare disease data**.

6.1.4. Data Portability Mechanism

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), will enable patients to receive and transmit their personal health data in a structured, commonly used, and machine-readable format.

Portability mechanisms:

- Patients will be able to request their data via secure patient portals or by submitting a written request to the Data Protection Officer (DPO).
- Data will be provided in EHDS- compliant formats such as HL7 FHIR, CDA, or EEHRXF XML.
- Transfers to other healthcare providers will be conducted via secure APIs or encrypted file transfer protocols.

6.1.5. National EHDS Hubs

FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group"), acknowledge that each EU Member state is required to **establish a national EHDS hub** (more information can be found at MyHealth@MyHands, a project supporting EHDS implementation, which currently lists 18 Member States as participating in the deployment of interoperable health data systems) in order to coordinate data exchange and integration with HealthData@EU. FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") will strive to:

- Collaborate with national EHDS hubs in countries where it operates.
- Register eligible datasets with national hubs for secondary use, subject to patient consent and regulatory approval.
- **Participate in pilot programs and technical onboarding** led by national authorities to test and validate EHDS-compatible systems.

6.1.6. Cross-Border Data Sharing

- Cross-border data may be reused for research only within secure processing environments, which are subject to approval by national Health Data Access Bodies (HDABs).

- Clinics must catalogue datasets and flag any intellectual property or trade secrets to HDABs.
- Secondary use for marketing or any discriminatory profiling is strictly prohibited.

6.1.7. EHDS Cybersecurity implementation

The EHDS's purpose of enabling cross-border data sharing and reuse for research means more entities and more data are involved, potentially increasing the number of entry points for malicious actors. Due to the sensitivity of reproductive health data, **adaptive and robust cybersecurity framework is the crux of supporting the secure implementation of the European Health Data Space (EHDS)** within FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group").

Apart from the compliance with internal documents, **organisational measures** will be implemented:

- **Prevent data breaches:** Align with the Cybersecurity Response Plan (FL-CS-OP2) to detect, report and mitigate EHDS-related data breaches.
- **Implement certified EHR Systems:** Ensure all electronic health record (EHR) systems used in clinics are EHDS-certified (for interoperability, security, and privacy) before use in cross-border exchanges.
- **Secure Data Exchange:** Use encrypted channels and secure APIs for data sharing with national EHDS hubs and HealthData@EU (central hub which brings together health datasets from across Europe) infrastrucure.
- **Collaboration with National EHDS Hubs:** Engage with national health data access bodies (HDABs) to ensure secure integration and compliance.

6.1.8. Governance and compliance

- An **EHDS Coordinator** (within the DPO team) will be established, who will oversee implementation, liaise with national hubs, and ensure readiness for phased compliance.
- The **Head of Legal** will regularly monitor regulatory developments and ensure the alignment with GDPR, SoHO, and EHDS acts.
- All EHDS related data processing activities **will be documented** in the Data Register and will be **subject to audit**.

6.1.9. Timeline of implementation & readiness

FutureLife will strive to adhere to the EHDS phased implementation:

2025 – 2027 Secondary legislation phase (preparation):

- Preparation of policies.
- System upgrades.
- Staff training.
- Engagement with national EHDS hubs.

2027 – 2029 Member States establish national EHDS hubs (integration):

- Clinics begin integration with national hubs and HealthData@EU for primary and secondary use.

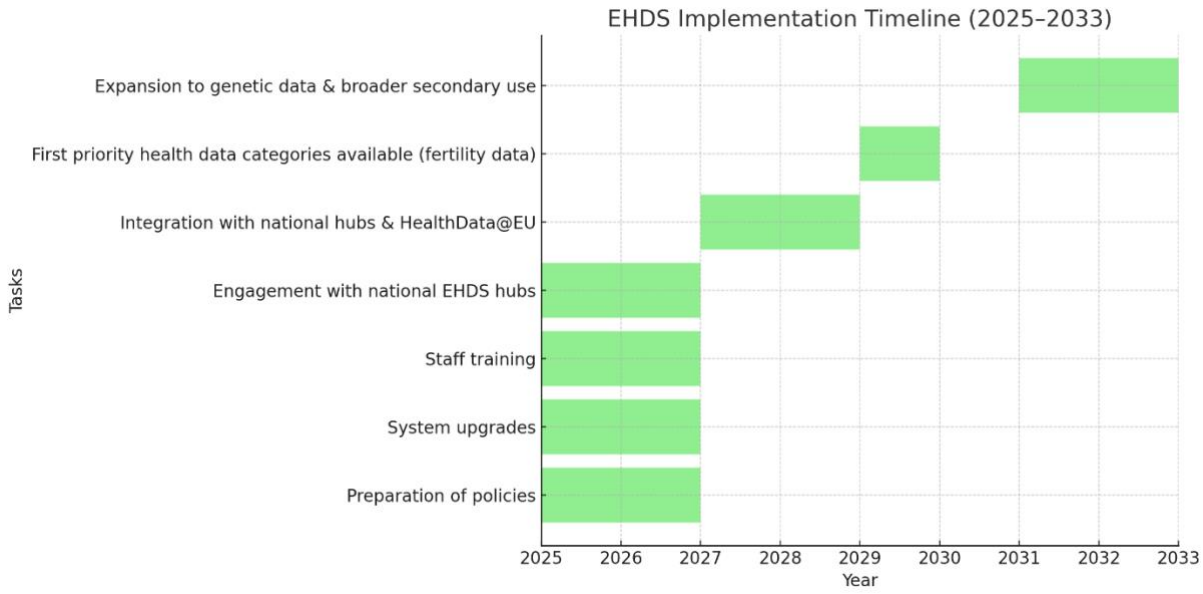
2029:

> First priority health data categories (including fertility data) available for cross-border primary use.

2031 and onwards:

> Expansion to genetic data and broader secondary use.

FutureLife EHDS Planned Implementation Timeline:



ANNEXE A - CATEGORIES OF PERSONAL DATA AND PURPOSES OF THE PROCESSING

Below, the categories of personal data collected, the purposes for which such data is used, and the duration of its retention are specified.

Table 1: Categories of personal data and purposes of the processing

PURPOSES OF PROCESSING PERSONAL DATA	CATEGORIES OF PERSONAL DATA	LEGAL BASIS FOR PROCESSING	PURPOSES OF PROCESSING PERSONAL DATA
1. Attention to Request for Information, Complaints or Suggestions			
Requests for information, complaints, or suggestions are processed to respond to inquiries, address concerns, and resolve submitted requests.	-Contact data: name, e-mail address, phone number. - Content data: information provided in the request or communication.	Consent (Article 6(1)(a) GDPR). Legitimate interest in quality control, dispute resolution, and service improvement (Article 6(1)(f) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") jointly with the relevant Group clinic to which the request is addressed.
2. Provision of Healthcare Services			
Personal data is processed to ensure the proper provision of medical services. This includes managing patient files and processing data and documents generated in connection with medical treatment.	- Contact data: name, e-mail address, phone number, postal address. - Identification data: national ID number, passport number, gender, date of birth. - Image data: photographs, scans, or other visual documents. - Medical data: medical history, medical reports, diagnostic results, treatment information, biological samples, tests, reproductive health details, etc.	Execution and performance of a contract (Article 6(1)(b) GDPR). Compliance with legal obligations (Article 6(1)(c) GDPR).	The relevant FutureLife clinic provides the healthcare services.

PURPOSES OF PROCESSING PERSONAL DATA	CATEGORIES OF PERSONAL DATA	LEGAL BASIS FOR PROCESSING	PURPOSES OF PROCESSING PERSONAL DATA
3. Management of Patient's files			
Personal data is processed to manage patient files and to ensure proper administrative and organisational management of healthcare centres.	- Contact information: name, e-mail address, phone number, postal address, etc. - Health data: medical history, diagnoses, treatments, allergies, medications, vital signs, and other relevant health information from the patient and their partner. - Identification data: national ID number, patient ID number, passport number, gender, date of birth. - Administrative data: appointment details, billing information, insurance data, consent forms, and communication records.	Execution and performance of a contract (Article 6(1)(b) GDPR). Compliance with legal obligations (Article 6(1)(c) GDPR). For special categories of data, processing is based on the provision of healthcare treatment in accordance with EU or Member State law (Article 9(2)(h) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") clinics.
4. Management of the relationship with donors			
Personal data is processed to create donor profiles and to manage the contractual relationship between the donor and the clinic. This includes the provision of necessary medical assistance and the payment of agreed compensation.	Personal data is processed to create donor profiles and to manage the contractual relationship between the donor and the clinic. This includes the provision of necessary medical assistance and the payment of agreed compensation.	Execution and performance of a contract (Article 6(1)(b) GDPR). Compliance with legal obligations (Article 6(1)(c) GDPR). For special categories of data, processing is based on the provision of healthcare treatment in accordance with EU or Member State law (Article 9(2)(h) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") clinics.
5. Patient Referral			
Personal data is processed and communicated to the referred clinic to ensure that the requested treatment can	- Contact data: name, e-mail address, phone number, postal address.	Consent to the referral of personal data to other FutureLife clinics (Article 6(1)(a) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group

PURPOSES OF PROCESSING PERSONAL DATA	CATEGORIES OF PERSONAL DATA	LEGAL BASIS FOR PROCESSING	PURPOSES OF PROCESSING PERSONAL DATA
be provided at an alternative location, upon request.	- Identification data: national ID number, passport number, gender, date of birth.		(the "FutureLife Group") clinics.
6. Administrative and Management Internal Purposes			
Personal data is processed to ensure proper administrative and organisational management of clinics, as well as for internal statistical purposes.	- Contact data: name, e-mail address, phone number. - Administrative data: appointment details, billing information, insurance data, and communication records. - Statistical data.	Legitimate interest in managing and controlling organisational activities and business relationships (Article 6(1)(f) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") jointly with the relevant Group clinic to which the request is addressed.
7. Survey Purposes			
Personal data is processed for the purpose of sending quality and satisfaction surveys related to services provided and care received.	- Contact data: name, e-mail address, phone number. - Statistical data.	Legitimate interest in quality control, adapting activities, and developing improved products and services (Article 6(1)(f) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") jointly with the relevant Group clinic to which the request is addressed.
8. Marketing Purposes. Sending Commercial Communications and Newsletter			
Personal data is processed to manage subscriptions to notification or messaging services, such as newsletters, and to provide information about services or special offers.	- Contact data: name, e-mail address, phone number.	Consent provided through subscription (Article 6(1)(a) GDPR). In the case of an existing contractual relationship, legitimate interest in sending information about similar products and services (Article 6(1)(f) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") jointly with the relevant Group clinic to which the request is addressed.

PURPOSES OF PROCESSING PERSONAL DATA	CATEGORIES OF PERSONAL DATA	LEGAL BASIS FOR PROCESSING	PURPOSES OF PROCESSING PERSONAL DATA
9. Scientific and Research Investigation			
Personal data is processed for scientific and research purposes to improve understanding of fertility and reproductive health conditions, enhance assisted reproductive treatments, and support the training of professionals in the field.	- Medical and health data: medical history, diagnostic results, treatment information, vital signs, behavioural health details, reproductive health details, etc.	Legitimate interest in conducting research and scientific activities in the field of fertility and reproductive health (Article 6(1)(f) GDPR). Where data is not anonymised, express consent is required (Article 6(1)(a) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") jointly with the relevant Group clinic to which the request is addressed.
10. Website Maintenance and Analysis			
Personal data is processed to ensure and optimise system performance, evaluate security and stability, and deliver personalised advertising based on user behaviour. This is achieved through the use of cookie technology. For more details, please consult the Cookie Policy.	- IP address of the internet-connected device. - Date and time of access. - Referrer URL, browser type, and operating system. - Name of the access provider.	For non-essential cookies: consent provided through cookie preferences (Article 6(1)(a) GDPR). For technical and essential cookies: legitimate interest in ensuring security, stability, and usability (Article 6(1)(f) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group").
11. Compliance with Legal Obligations			
Personal data is processed to comply with legal obligations, including those related to data protection, taxation, healthcare, and other applicable regulations. Data may also be disclosed to law enforcement agencies, courts, tribunals, or other government authorities as required by law.	- Contact data: name, e-mail address, phone number. - Content data: information shared and/or included in legal or regulatory requirements.	Compliance with legal obligations (Article 6(1)(c) GDPR).	FutureLife a.s., and any of its affiliates belonging to the same corporate group (the "FutureLife Group") jointly with the relevant Group clinic to which the request is addressed.

ANNEXE B – RACI MATRIX

This RACI matrix outlines the roles and responsibilities related to Global Data Privacy Policy compliance across key stakeholders. The following is a legend that explains the meaning of each role designation used in the RACI matrix.

- **R (Responsible):** The person who performs the task or activity.
- **A (Accountable):** The person ultimately answerable for the correct and thorough completion of the task.
- **C (Consulted):** The person who provides input or expertise before the task is completed.
- **I (Informed):** The person who is kept up to date on progress or decisions, but does not actively contribute.

Table 2 : RACI matrix

Activity / Role	DPO	CTO	Head of Legal	Local Security Officer	HR	Employees	Contractors	Cybersecurity Manager	Business Owner	Functional Owner
Monitoring GDPR compliance	R	A	A	C	I	I	I	C	A	C
Contact point for supervisory authorities	R	I	I	I	I	I	I	I	I	I
Training and guidance on data protection	R	C	C	C	C	I	I	C	I	C
Internal audits and assessments	R	A	C	C	I	I	C	C	C	C
Data Protection Impact Assessments (DPIA)	A	I	C	C	I	I	C	C	R	R
Records of processing activities	R	I	C	C	I	I	C	I	C	R
Approval and oversight of the global privacy policy	I	A	R	I	I	I	I	C	C	I

Technical safeguards for personal data	C	I	R	C	I	I	R	A	C	C
Incident and data breach response	C	I	R	C	C	I	C	A	I	I
Local GDPR compliance	I	I	C	R	I	I	I	C	R	R
Processing of employee personal data	I	I	I	I	R	I	I	I	R	R
Staff training	C	I	C	R	R	R	I	C	I	C
Responsible data handling	I	I	I	I	I	R	R	C	R	R
Contractual data processing	I	I	I	I	I	I	R	C	R	C
Penetration testing and risk analysis	I	C	C	I	I	I	I	R	C	C
Encryption and access control	I	I	C	I	I	I	I	R	C	C

FutureLife

Global Data Privacy Policy

ABOUT FUTURELIFE GROUP

Since the FutureLife group was founded in 2014, we continue to grow each year. Today, we have over 38 clinics across 8 European countries, run by more than 1,000 skilled team members and 450 doctors. Our clinics offer comprehensive sterility treatment, including genetic, immunological, and other follow-up tests.

Our main aim is to provide quality care and effective treatments to create healthy babies and happy families. We are continuously investing in our clinics, research, and training. This helps us offer expertise, financial stability, good working conditions, and competitive pay for our teams.