5G4P Health

Legal & Ethical Compliance Report

Author: LegalMatic (LDT)

PROJECT NUMBER: C2023/1-19
PROJECT NAME: Enhanced 5G-Powered Platform for Predictive Preventive Personalized and Participatory Healthcare
PROJECT ACRONYM: 5G4PHealth

Deliverable ID	1.4
WP number	WP1
Lead Partner	LDT
Due date	31.06.2024
Date of submission	31.10.2024
Type of deliverable	R
Dissemination level	PU

Document History

Version	Person	Partner	Date
0.1	Dilara Dolunay Dursun	LegalMatic Dijital Teknolojiler (LDT)	31.10.2024
0.2	Dilara Dolunay Dursun	LegalMatic Dijital Teknolojiler (LDT)	31.04.2025
0.3			
0.4			
0.5			
0.6			

Executive Summary

The 5G4PHealth project aims to revolutionize healthcare through the integration of 5G, AI, IoMT (Internet of Medical Things), and P4-based solutions (Predictive, Preventive, Personalized, and Participatory healthcare). This report outlines the legal, regulatory, and ethical considerations governing the development and deployment of 5G4PHealth technology. The report separates the two processes: the legacy of the technology development process and the legacy of the technology itself (by design and default). It is crucial to use licensed data and consented users during the development process, while also ensuring the reservation of ethical matters. The development process requires a high level of use of health data collected across different jurisdictions. However, the primary focus of all legislation is on human rights. During the development process, 5G4PHealth technology does not pose predictable risks or harms to the (human) test subjects who will participate in this project. Nevertheless, we

recommend that parties refrain from using PHI and/or applying the technology tools or prototypes directly to real people. It may also be important to consider the accuracy of the technology's output. For this reason, it will be crucial to obtain informed consent from the participants.

The informed consent should include information about the potential risks and harms related to participation in the technology development process as a test subject, as well as a voluntary participation statement.

Attached to this report, we have shared the data license agreement template and informed consent statement templates with the project parties. Throughout the project period, we will continue to support developers in the application of these documents.

Another important matter is the use of artificial intelligence during the development process. Although artificial intelligence methodologies have been in practice for a long time, regulations are still new and subject to change. The risk categorization and classification are not yet sufficiently clarified. This uncertainty can be seen as an advantage, and parties may prefer to define their own boundaries.

Regarding the use of artificial intelligence, we recommend that parties develop their own AI software, rather than relying on third-party AI solutions**.** It is also agreed that, to comply with project rules, the steps shall be handled directly by the parties and cannot be transferred to subcontractors. Additionally, the party is responsible for the use of artificial intelligence algorithms that are accountable and can be shared if any relevant authority requests them in the context of its investigative rights. The use of "black boxes" or other undefined processes is not acceptable.

Note that this deliverable is not a fixed document. It will evolve during the lifespan of the project and will be further elaborated and updated.

Table of Contents

1 Scope and Objectives

This report aims to:

- Establish transparent management systems to prevent ethical violations.
- Safeguard physical and psychological well-being of participants in training and research activities.
- Provide informed consent management to maintain transparency in data processing operations.
- Ensure full compliance with data protection regulations.

2 The Legacy of The Technology Development Process

2.1 Ethical Considerations

2.1.1 Key Principles

- **Do No Harm:** All research activities must avoid causing physical, psychological, or moral harm to participants.
- **Informed Consent and Participation:** Participants must be fully informed about the project and allowed to withdraw at any time.
- **Transparency** in communication with all stakeholders, including patients and regulatory bodies.
- **Data minimization** to limit the collection of unnecessary information, reducing exposure to privacy risks.

- **Dual Use Risk Mitigation:** Measures must be taken to prevent the misuse of research outcomes for military or malicious purposes.

2.2 Ethics in Research

There are many ethical considerations when undertaking research. Keys amongst these are the protection of human participants, respect for intellectual property, and handling of personal data.

Protection of Human Participants: 5G4PHealth does not provide any form of medical treatment or directly intervene with human participants. During the development process, no human test subjects will be involved. Nevertheless, as a precaution and a reminder, we strongly recommend that all parties refrain from using Personal Health Information (PHI) and from applying any technological tools or prototypes directly to human subjects.

Respect for Intellectual Property: Developers should also honor patents, copyrights, and other forms of intellectual property, and should not use unpublished or unlicensed data, methods, or results without permission. During development, developers can benefit from the data license agreement template in the annex.

2.3 Data Protection Compliance

5G4PHealth Project:

- Focuses on processing **open-source data**, without handling personal data.
- Collects no personal data; participation in training modules is voluntary.
- **Risk assessments** ensure participant safety during training and testing activities.

However, if the personal data is processed:

Each project party is responsible for its personal data processing activities separately as a 'data controller.' To ensure compliance with data protection regulations, each party is responsible for obtaining explicit consent from data subjects, notifying data breaches within 72 hours, and fulfilling other relevant requirements.

The project parties are from different jurisdictions and will work together to develop health technology. For this reason, we will focus on each party's jurisdiction separately.

In context of GDPR, personal data transfers within the Europe Union countries, and European Economic Area is permitted. Personal data transfers to United Kingdom are also permitted depending on an adequacy decision provided by European Commission. However, personal

data transfers to Türkiye can only be accepted legal if the parties act a Standard Contractual Clauses which is released by the European Commission.

In the context of GDPR-UK, personal data transfers within the European Union countries and the European Economic Area are permitted. Standard data protection clauses specified in regulations made by the Secretary of State will be used during personal data transfers abroad (to Türkiye).

The best option during development is to apply personal data only where it is strictly necessary. If the development can continue with data that is not related to an identified or identifiable person, this should be preferred first. If needed, suitable anonymization methodologies can also be applied to the datasets used. There is no single anonymity mechanism[1]; randomization or generalization models may be used.

All projects must align with the data protection principles[2]:

- **Lawfulness, fairness and transparency:** Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data is or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.
    - **Informed Consent:** Participants must be fully informed about how their data will be used, and their consent must be obtained.
    - **Access and Correction Rights:** Participants must be able to access and request corrections to their data at any time.
- **Purpose limitation:** Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.
- **Data minimization:** Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

[1] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[2] https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Lawfulness%2C%20fairness%2C%20and%20transparency%3A,are%20or%20will%20be%20processed

Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

- **Accuracy:** Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Controllers should accurately record information they collect or receive and the source of that information.
- **Storage limitation:** Personal data should only be kept in a form which permits identification of data subjects for as long as it is necessary for the purposes for which the personal data are processed. To ensure that the personal data is not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.
    - **Data Retention:** Data must be securely stored for no more than one year after the project's completion and subsequently deleted.
- **Integrity and confidentiality (security):** Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorized or unlawful access to or use of personal data and the equipment used for processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
- **Accountability**

2.4 Data Security and Risk Management

- **Access Management:** Access to data is controlled through access matrices, with all changes logged and monitored.
- **Technical Security Measures:** Antivirus software, firewalls, and encryption protocols (e.g., HTTPS, SSL) are implemented.
- **Physical Security:** Data storage facilities are protected against physical threats.
- **Data Breach Notification:** Any breaches must be reported to relevant authorities within 72 hours.

2.5 Recommendations for Effective Compliance

- **DPIA (Data Protection Impact Assessment):** Conduct DPIAs at the start of each project to proactively address potential risks.
- **Training and Awareness Programs:** Provide regular training on data protection, ethics management, and security for all project personnel.

- **Ethics Monitoring Committee:** Establish a dedicated committee to oversee compliance across all project stages.
- **Regular Audits:** Ensure projects are continuously monitored and reviewed to maintain compliance with relevant regulations.

3 The Legacy of The Technology Itself (By Design and Default)

5G4PHealth will include one main platform and a clinical environmental platform for healthcare facilities. It will include *6 AI-Driven cloud services (i.e., Posture Evaluation, Glaucoma detection, Wayfinding and Routing, Mood detection, Sensorial experience generation, and Depression Relapse Prediction), 5 Products (i.e., ePHR, Posture Evaluation platform, Glaucoma Teleconference app, Depression Management tool, and BiBo app)*.[3] The 5G4PHealth technology focuses on solutions below:

1) Address the Posture Evaluation gaps*, through the development of easy to use, objective, portable and low-cost solutions that quantify gait analysis, enabling the prescription of effective patient-tailored treatments.*

2) Address the limitations of current AI-driven glaucoma diagnosis *by developing an innovative method of early detection, supported by teleconsultation.*

3) Develop an AI-power based depression management tool for depression *that combines multisource data (mobile and wearable) to anticipate future episodes, while providing quantitative data to help with medical decision-making process.*

4) Develop a multi-modal patient emotion recognition system, *to interfere with the status of the under-treatment patient.*

5) Develop an Emotional and Empathetic AI Engine for Healthcare, *to create emotionally*
engaging and empathetic experiences.

6) Develop a white-label Be-In-Be-Out application *that can effectively improve the endto-end patient journey in clinical environments.*

7) Develop 5G based context-aware communication *protocol which will enable (near)real-time data/video transfer, low-latency and energy-efficient communication links, required in digital healthcare.*

8) Implement an IoMT platform that can address the limitations of current platforms *regarding device compatibility and security of health information exchange.*

[3] CELTIC-NEXT PROJECT DESCRIPTION (PD)

9) Develop an electronic Personal Health Record *that can provide enhanced usability, security and trust to patients, improving their data control and sovereignty, through a highly interoperable platform that enables multisource data aggregation.*[4]

All services and products shall be analysed separately.

3.1 Ethics Management Processes

Technology alone is not sufficient for medical diagnosis and treatment. Turkish legislation dictates that medical diagnosis, and treatment must be directly performed by licensed medical doctors. We believe similar legislative rules should apply in other countries as well. This ensures that users benefit from this technology responsibly.

It is also important to uphold patients' rights in relation to the outputs of this technology. For this purpose, we advise considering the PHI Risk Assessment attached. The assessment addresses data protection, privacy, and security requirements.

Data Ownership: Unless the technology service recipient/user (e.g., health clinic) gives written permission, the ownership of data created during use belongs to the service recipient/user. The technology provider may choose to establish a different ownership structure through a data license agreement.

3.1.1 Legal and Ethical Risks Associated with Specific Technologies: AI, IoT, 5G

AI: The development process must be considered in light of both the GDPR and the AI Act. According to the AI Act, details regarding **prohibited AI practices** will be announced by the **European AI Office**. However, **Article 5** of the AI Act may prohibit the following two solutions:

4. Development of a **multi-modal patient emotion recognition system** intended to interfere with the condition of a patient under treatment.
5. Development of an **Emotional and Empathetic AI Engine for Healthcare** aimed at creating emotionally engaging and empathetic experiences.

This potential prohibition depends on whether the system utilizes **biometric authentication features** for emotion recognition. According to **Article 3**, an "emotion recognition system" is defined as *"an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data."*

Recital 44 of the AI Act highlights the **limited reliability** of AI systems in recognizing emotions, as emotional expressions may vary depending on cultural, contextual, or individual factors. Furthermore, **Recital 57** raises concerns about the possible evolution of AI systems into tools

[4] CELTIC-NEXT PROJECT DESCRIPTION (PD)

that analyze human behavior based on **gender, sexual orientation, disability status, age, or racial/ethnic origin**, especially in the workplace.

We hereby inform you that the two solutions listed above are not legally suitable for development under the current AI Act framework. Other solutions, however, are considered acceptable within the high-risk and limited risk.

IoMT: IoMT devices collect, transmit, and sometimes process PHI continuously. These devices, including wearable sensors, smart implants introduce serious **data protection** and **cybersecurity** risks. Unauthorized access to such devices may result in data breaches, manipulation of medical treatments, or denial of service.

Legally, there are challenges in ensuring **data minimization**, **purpose limitation**, and **user consent**, as per the GDPR. The complexity of device ecosystems often results in **unclear data controller/processor roles**, complicating legal responsibility. Moreover, firmware updates or third-party integrations can introduce unexpected privacy threats.

Ethically, concerns arise over the **constant monitoring** of individuals, leading to **surveillance-like environments** and possible erosion of privacy. Clear and user-friendly consent mechanisms, combined with **security-by-design** principles, are essential.

5G: There is no regulation prohibiting the use of this technology as part of Medtech. The legal and ethical risks may depend on how the data transmission speed and volume in 5G networks amplify the potential impact of breaches. Preventing data breaches is mandatory. For this reason, high-security protocols should be implemented during data transmission (details can be found in section 3.1.2, Data Transfer), and a data breach response plan should be applied.

3.1.2 Data Transfers

The lack of standardized data-sharing protocols limits seamless device communication. While this does not directly pose a legal risk, many national and international standards include specific rules on secure transmission methodologies (such as encryption, VPN, TLS, SSL, etc.) that should be used during data transfers. Additionally, these methodologies should be differentiated for on-premises tech solutions and cloud-based solutions. In written documentation about the 5G4PHealth project and during consortium meetings, it has been identified that the technology solution will be hosted on cloud platforms. For this reason, this report focuses only on cloud-based legal risks. Although not mandatory, we assume that medical corporations adopting 5G4PHealth solutions will ensure compliance with health data standards such as FHIR, HL7, DICOM, etc. Developers should take these standards into account during the development process.

Table 2: Health Data Transmission Standards

Standard	FHIR (Fast Healthcare Interoperability Resources)	HL7 (Health Level 7)	DICOM (Digital Imaging and Communications in Medicine)
Focus	Mobile and web-based applications, wearable devices	Messaging	Medical imaging
Why does the developer consider this?	Security of data transmission	Ease integration with conventional health technologies	Defining the data format for integration, definition, and transmission.

3.1.3 Assessment of Data Subjects Rights

Transparent information, communication, and modalities for the exercise of the rights of the data subject: Patients and other data subjects can be included in the 5G4PHealth platforms directly by becoming a user (through the mobile application and other interfaces) or by user identification from another authorized user (such as a medical doctor's identification of a patient on the platforms). Users who are directly included in the 5G4PHealth platforms will be informed through 5G4PHealth interfaces. However, it is the medical clinic's responsibility to provide information notices to external parties.

Automated individual decision-making, including profiling: During the development process, developers should focus on ensuring transparency in the automated decision-making process of the algorithms. As discussed in section 3.2, 5G4PHealth will not be sufficient on its own for medical diagnosis and treatment. It is designed to support medical doctors during medical services. It is uncertain whether a medical doctor's diagnosis will match the 5G4PHealth diagnosis. Any mismatch should not solely raise suspicion about the medical doctor. However, for the future and preferable use of 5G4PHealth, it is important to maintain transparency regarding decision-making details.

Developers will provide **artificial intelligence algorithms that are accountable and can be shared if any relevant authority requests them in the context of its investigative rights. The use of "black boxes" or other undefined processes will not be acceptable.**

Consent Management:

Consent is a legal basis for processing personal health information when no other legal basis under the GDPR applies. 5G4PHealth solutions do not directly fall under any other lawful basis for processing Personal Health Information (PHI), except for explicit consent.

Data subjects over the age of 16 must be fully informed about how their data will be used, and their explicit consent must be obtained. For children under the age of 16, the child's explicit consent must be supported by that of a parent or legal guardian. Informed Consent statement templates are provided below.

Explicit consent must meet the following three criteria:

- It must be **use-case specific**. A single opt-in mechanism for all types of data processing is not acceptable. Therefore, explicit consent must be obtained separately for each module.
- **Privacy notices** must be presented to the user **before** consent is obtained. This ensures that data subjects are informed about privacy risks and their rights.
- Consent must be **freely given**. Data subjects are not required to provide consent to use 5G4PHealth solutions. They must also have the right to **withdraw their consent at any time**. It is recommended to design a privacy settings interface that allows data subjects to manage their consent directly via the platform.

4 Conclusion

This report serves as a comprehensive guide to ensure **legal and ethical compliance** across various projects, including **IoMT**. Ensuring **data security, transparency, ethical management**, and **participant rights** are crucial for the success and sustainability of these projects. Collaboration between **technology providers, researchers, and regulatory bodies** is key to fostering a secure and responsible research environment.

5 ANNEX

Annex- Data License Agreement Template

Annex- PHI Risk Assessment

Annex- Privacy Notice & Consent Form

Annex- Data License Agreement Template

DATA LICENSE AGREEMENT

This Data License Agreement (the "Agreement") is made and entered into on [Date] by and between the following parties:

Licensor:
[Hospital Name]
Address: [Address]
Phone: [Phone]
Email: [Email]

Licensee:
[Company Name]
Address: [Address]
Phone: [Phone]
Email: [Email]

The parties agree as follows for the licensing of health data collected by the Licensor to the Licensee for the purpose of developing health technologies under the terms outlined below:

1. Granting of License and Usage Rights
1.1 The Licensor hereby grants the Licensee a license to use health data that includes [specified types of health data: e.g., patient information, treatment history, laboratory test results, demographic data, etc.] solely for the purposes specified in this Agreement.

1.2 The data subject to this Agreement will be anonymized in a way that prevents the identification or re-identification of any individual. The data subject to this Agreement is anonymized data.

1.3 The Licensee shall have the right to use the data solely for the purpose of [e.g., developing health technologies officially supported by Eureka and Tübitak, training AI algorithms, developing health applications, etc.].

1.4 The ownership of the data, along with all intellectual property rights and other legal rights, remains with the Licensor. The Licensee only has the right to use the data and will not acquire any ownership rights or exclusive rights over the data.

2. Data Usage and Purposes
2.1 The Licensee shall use the licensed data only for the purposes specified in this Agreement. The Licensee will not use the data for any other purposes, nor will it transfer the data to others or provide access to third parties.

2.2 The Licensee shall use the licensed data exclusively for the development of digital health technologies supported by national and international project organizations and shall not allow third parties to access the data.

2.3 The Licensee shall not have the right to redistribute, sell, or create derivative works from the data.

3. Data Security and Confidentiality
3.1 The Licensee shall take all necessary technical and administrative measures to ensure the security of the health data received from the Licensor.

3.2 The Licensee shall ensure that only authorized personnel can access the data and shall maintain the confidentiality of the data.

3.3 The Licensee shall implement appropriate security protocols to protect the data from unauthorized access, use, or sharing.

3.4 The Licensee shall not violate data security and will take all necessary measures to prevent improper use or abuse of the data.

4. Anonymization of Data and Usage Limitations
4.1 The Licensor will take the necessary precautions to provide anonymized data to the Licensee.

4.2 The Licensee shall use the anonymized data only in accordance with the terms of this license.

4.3 The Licensee shall take all necessary measures to ensure that the data is anonymized and will not use the data in a way that reveals personal identifying information.

4.4 In the event of any conflict between this Agreement and the applicable legal regulations, the applicable legal regulations shall prevail.

5. License Term and Termination
5.1 This license shall be effective as of [start date] and shall remain valid until [end date or conditions].

5.2 The Licensee may use the license only for the specified term. Upon the expiration of the license term, the Licensee is required to destroy and/or return all data in compliance with applicable regulations.

5.3 Either party may terminate this Agreement by giving written notice. In the event of termination, the Licensee shall destroy and/or return all data in compliance with applicable regulations.

6. Payment Terms
6.1 The Licensee shall pay the Licensor a fee of [specified license fee] for the data license.

6.2 Payment shall be made via [specified payment method: bank transfer, check, etc.] by [payment date].

6.3 In the event of non-payment, the Licensee may be subject to legal proceedings for non-compliance with the terms of this Agreement.

7. Legal Obligations and Governing Law
7.1 The parties agree to comply with all applicable health regulations and personal data protection laws in the use of the data.

7.2 This Agreement shall be governed by the laws of [country name].

8. Dispute Resolution
8.1 Any disputes arising from this Agreement will be attempted to be resolved amicably through negotiation.

8.2 If the dispute cannot be resolved amicably, the parties shall submit the dispute to the courts of [specified jurisdiction].

(If any) Annexes:

Licensor's Ethical Policies
Licensor's ISMS Policies
Licensor's Access Control Procedures
Licensor's Data Transfer Protocols, etc.

Annex - PHI Risk Assessment

Requirement	Indicator	Status
Application of Destruction Rules		
Employee Training		
Service Agreements		
Obtain Patient Consent for Disclosure		
Appointment of Privacy Officer		
Privacy Practices Notification (NPP)		
Cooperation in Investigation / Responding to Authorities		
Access Rights - Fulfillment of Record Request - In Requested Format		
Access Rights - Fulfillment of Record Request - Within 30 Days		
Access Rights - Fulfillment of Record Request – Complete		
Access Rights - Fulfillment of Record Request - Without Requesting Fees and Conditions		
Risk Analysis		
Breach Response Plan - Incident Response		
Breach Response Plan - Breach Notification		
Auditing		
Monitoring / Evaluating Environmental / Operational Changes		
Keeping System Activity Logs		
Monitoring System Activity Logs		
Security Policies/Procedures		
Prevention of Unauthorized Access - Encryption		
Prevention of Unauthorized Access - Access Policies/Procedures		
Prevention of Unauthorized Access - Access Authentication		
Prevention of Unauthorized Access - Removal of Access Rights at Employment End		

Network and Server Security - Identifying Suspicious Network Activity - Network Monitoring		
Network and Server Security - Identifying Suspicious Network Activity - Limiting / Blocking Network Access		
Network and Server Security - Unauthorized Access Controls		
Network and Server Security - Up-to-date Software and Security Patches		
Network and Server Security - Strong Passwords and Authentication		
Network and Server Security - Backup		
Network and Server Security - Network Firewall		
Network and Server Security - Penetration Testing		
Network and Server Security - VPN		
Network and Server Security - Emergency Plan		
Network and Server Security – Encryption		

Annex- Privacy Notice

Privacy Notice - 5G4PHealth Solutions

Effective Date: [DD/MM/YYYY]

Version: 1.0

Data Controller: [Organization Name & Contact Info]

Data Protection Officer (DPO): [DPO Name & Email]

1. Introduction

This Privacy Notice explains how your personal data will be collected, used, stored, and protected as part of the 5G4PHealth solutions, in accordance with the **General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679**.

2. What Personal Data Will Be Collected?

Depending on the module(s) you participate in, we may collect the following categories of data:

- **Health-related data:** vital signs, symptoms, mental health indicators, retinal images, gait analysis, etc.
- **Behavioral data:** sleep patterns, physical activity, mood logs, interaction history.
- **Location data:** within clinical environments (for Be-In-Be-Out module).
- **Device metadata:** usage logs, communication patterns, and signal information.
- **Identifiers:** pseudonymized participant ID; no directly identifying data (e.g., name, national ID) will be processed unless explicitly required and agreed upon.

3. Purpose of Data Processing

Your data will be processed strictly for the following purposes:

- Development and testing of healthcare technologies under the 5G4PHealth solutions
- Enhancing diagnostic and therapeutic tools (e.g., AI-based systems)
- Improving usability, safety, and security of digital health services
- Scientific analysis and project reporting in anonymized or aggregated form

4. Legal Basis for Processing

In compliance with **Article 6(1)(a)** and **Article 9(2)(a)** of the GDPR, **your explicit consent** is the primary legal basis for processing your personal health data. You are not obligated to provide consent and may **withdraw your consent at any time** without consequences.

5. Data Sharing and Recipients

- Your data will be accessed only by authorized personnel.
- Pseudonymized data may be shared with research partners, subject to contractual data protection safeguards.
- Data will **not be used for commercial purposes** or shared with third parties outside the research consortium unless legally required.

6. International Data Transfers

All data will be stored and processed within the European Economic Area (EEA) and the data controller's local servers. If international transfers are necessary, appropriate safeguards under **Chapter V of the GDPR** will be applied (e.g., Standard Contractual Clauses).

7. Data Retention

Your data will be stored only as long as necessary for the project goals and in compliance with ethical and legal requirements. Anonymized or aggregated data may be retained for scientific purposes indefinitely.

8. Your Rights Under GDPR

You have the following rights:

- Right to **access** your data
- Right to **rectification** of incorrect or outdated information
- Right to **erasure** ("right to be forgotten")
- Right to **restrict processing**
- Right to **data portability**
- Right to **withdraw consent** at any time
- Right to **lodge a complaint** with a supervisory authority

To exercise your rights, contact our **DPO** at [DPO Email].

9. Security Measures

We implement strong technical and organizational measures to protect your data, including:

- End-to-end encryption
- Secure storage and access control
- Pseudonymization of sensitive data
- Regular audits and compliance checks

10. Contact

If you have questions or concerns about this Privacy Notice or how your data is handled:

Email:
Address:

Annex- Explicit Consent

Consent to Data Processing for Specific Modules

Please indicate your **explicit consent** by ticking the relevant boxes:

No.	Module Description	Consent Given
1	Posture and gait analysis using wearable and mobile data for patient-specific treatment suggestions.	☐ Yes ☐ No
2	Early glaucoma detection through AI-enhanced retinal scan evaluation and teleconsultation.	☐ Yes ☐ No
3	Depression monitoring system using multisource (wearable and mobile) data to support medical decisions.	☐ Yes ☐ No
4	Indoor navigation via Be-In-Be-Out system to enhance clinical journey efficiency.	☐ Yes ☐ No
5	5G-based low-latency communication for healthcare data and video transmission.	☐ Yes ☐ No
6	Secure and interoperable IoMT platform for connected medical devices.	☐ Yes ☐ No
7	Personalized electronic Health Record system to enhance patient data sovereignty.	☐ Yes ☐ No