iPROLEPSIS

T1.4 / PRIVACY AND DATA PROTECTION POLICY OF THE iPROLEPSIS APP

Editors	Contractual delivery date	Actual delivery date
Ioannis Drivas (DBC) Sotirios Michagiannis (DBC)		

Deliverable type	Dissemination level	Version - date
R - Document, report	PU- Public	1.0 – 13/06/2024

1 Introduction

As a consortium, we consider privacy a matter of utmost importance and in this policy, the principles to which we adhere to and the measures implemented to ensure the lawful processing, security and protection of the iPROLEPSIS application (app) end users' personal data is presented. We remain committed to complying with all relevant EU and national legislation regarding the protection of personal data and the "rights and freedoms" of the data subjects, in accordance with the General Data Protection Regulation (GDPR).

To this end, we have developed and implement this Privacy and Data Protection Policy and any other necessary policies and procedures regarding the processing and protection of personal data which regulates the use of the iPROLEPSIS app. This applies to all processing operations on the personal data of the end users of the app.

Moreover, we hereby provide the end users with the necessary information regarding the collection, use, sharing, retention and general processing of their personal data. At the same time, we provide information about their rights and how to exercise them properly and in accordance with the GDPR.

We remain at the end users' disposal in order to provide them with any information within the framework of our compliance with the current European and national legislation on the protection of personal data, as applicable, and the applicable regulatory directives related to the management of personal data, guaranteeing a secure environment for the processing of end users' data.

2 Definition of personal data

2.1 Personal data includes any information in paper or digital form that may lead either directly or in combination with other information (indirectly) to the unique identification of a natural person.

2.2 For the purpose of provision of the services by the app during the study, the following personal data will be collected from the data subjects, through direct insertion of them in the app or automated collection through the use of the wearable device that will be worn by the end users and that will be connected to the app:

i. personal identification number that will be provided by the clinical personnel,
ii. photos of hands and feet,
iii. skeletal data from finger, wrist and body movements,
iv. accelerometer data
v. touchscreen typing dynamics data
vi. heart rate and beat-to-beat intervals
vii. metrics related to sleep quality and stress
viii. answers to the study questionnaires

2.3 Most of them are considered special categories of data under Article 9 of the GDPR as being health related personal data. The concept of special categories of personal data includes personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data concerning the health, sexual life or finally, sexual orientation of an individual.

2.4 The personal data collected will be stored in a pseudonymized form. No identifiers related to the personal information of the patients will be requested during the use of the app and such information will be stored only by the clinic that is conducting the study that you participate in and will not be transferred, disclosed or in any way become available to any other project partner or third party. The personal information and any identifiers of the patients will not be processed in any way throughout

the testing and implementation phase of the iPROLEPSIS application and will not be requested to be provided in the app. Each patient will receive a unique personal identification number, with the additional information that could help identify the patients being available only to the clinic conducting the study, thus ensuring anonymity of the patients in relation to the rest of the partners.

2.5 Serious games suite The iPROLEPSIS application provides the end user with the option to participate in a personalized game suite with the aim to prevent the inflammation in PsA patients by supporting key health aspects, i.e., fitness, diet, mood, motor skills, and breathing, combined (in some games) with biofeedback and sensorimotor art-based approaches for stress/fatigue/pain soothing and management. During those games, data will be collected, depending on the type of games each patient has chosen through a relevant questionnaire provided to them, prior to their participation, and their needs.

2.6 biAURA suite. The iPROLEPSIS application also provides the end user with the option to benefit from the biAURA suite, which aims to exploit the tailored-to-PsA algorithm for estimating sleep disturbances towards activation of the binaural sounds and will cease by the time the detected sleep quality indicates that the user fell in restful sleep. Through this suite, sleep quality IData (heartrate, accelerometer data and body temperature) will be collected in order for the services of the app to be provided. Moreover, metadata related to the operation of the suite will be collected (time when the user launched the app or the sound stopped, whether the connection with the end user's headphones was lost etc.) and a visual sleep diary will be created, including the aforementioned information.

2.7 MP Joint landmarker. Part of the iPROLEPSIS application is the MP Joint landmarker, which will collect photographic files provided by the patients. With the use of this module, the end users will be able to take photographs and insert them in the iPROLEPSIS application. By entering to this module, the camera of the end user's smartphone will be activated in order for the end user to be able to take the photograph. Permission of access shall be granted by the end user prior to the use of the module. Those files will not be stored or in any way processed by this module but they will be directly transferred, through the use of encryption, to the iPROLEPSIS application and will be processed according to the rest of the personal data collected through the app.

3 Processing operations on personal data

The envisaged processing operations on the aforementioned personal data are the following:

i. Collection of the personal data directly from the end users or automatically through the use of the app.
ii. Personal data transfers from the wearable to the smartphone app via Bluetooth connection and then through HTTPS/TLS protocols and network security ensured through Firewalls, to the iPROLEPSIS data management infrastructure.
iii. Storage of personal data on the iPROLEPSIS data management infrastructure and the premises of the clinical and technical partners of the iPROLEPSIS project.
iv. Curation and harmonization of personal data.
v. Processing for the purposes of validation of the function of the iPROLEPSIS framework. This includes automatic processing operations, especially in terms of the serious games and the biAURA suite.
vi. Publication of some of the results of the studies being conducted as a result of the iPROLEPSIS project to Open Science repositories, with the personal data being anonymized before the publications may take place.

Further information regarding the processing operations will be provided in the consent forms that will be distributed to the end users before any processing operations take place.

4 Distinct Roles and Responsibilities

4.1 According to Article 4, paragraph 7 of the GDPR, the definition of the data controller is given, stating that "a data controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the data controller or the specific criteria for its nomination may be provided for by Union or Member State law."

According to the above, the clinical and technical partners are considered the (Joint) Data Controllers, are assumed responsibility, and shall be able to demonstrate compliance with the GDPR. The purposes and means of processing are defined by the grant agreement and any other project related documentation of the iPROLEPSIS project and the project partners implement the appropriate technical and organizational measures to protect the data being processed.

4.2 Additionally, according to the definition provided in Article 4, paragraph 8, "data processor" is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller."

Mainly, the appointed personnel of the project partners, including scientists, doctors, developers and legal representatives, are the ones executing the processing on behalf of the project partners. Agreements have been concluded between the project partners and the aforementioned personnel, outlining their responsibilities as processors, with specific reference to the nature, purpose, and duration of the processing, the types of data, and the categories of data subjects.

Under certain circumstances, other natural or legal persons may also be engaged by the project partners as processors. The project partners ensure that they collaborate exclusively with processors who provide sufficient assurances for the implementation of appropriate technical and organizational measures to meet the requirements of the Regulation and ensure the protection of data subjects' rights.

4.3 The processing by the processor is governed by a contract or other legal act subject to Union or Member State law, which binds the processor in relation to the project partners and specifies the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the data controller. No third party may have access to personal data processed by the project partners without a prior signing of a cooperation and confidentiality agreement with the related project partner. Compliance with data protection legislation is the responsibility of all employees processing personal data.

The processor and any person acting under the supervision of the data controllers, processes the personal data under the defined purposes and instructions set out by the data controller, unless required to do so by Union or Member State law. The processor does not engage another processor without the prior specific or general written authorization of the project partners.

5 Lawful Processing

5.1 Data processing refers to any act or series of acts carried out, with or without the use of automated means, on personal data or sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination, or any other form of making available, alignment or combination, restriction, erasure, or destruction.

5.2 A general rule in data processing is that, in principle, it is unlawful unless the conditions set forth in Articles 6 and 9 of the Regulation are met, which provide the necessary legal framework which defines the lawfulness of the processing operations on personal data.

5.3 The legal basis for processing of the aforementioned personal data for the project related purposes through the use of the app is informed consent, according to articles 9 par 2a' and 7 of the GDPR. The end users are provided with a form, with which they will provide their consent to the processing operations on their personal data, as they are described in sections 2 and 3 of the current policy. Additionally, since the processing of the end users' personal data is based on their previously given explicit informed consent, they have the right to withdraw from it at any time by making a relevant request to our authorized legal partner of the project via an email at legalint@diadikasia.gr

5.4 During the course of the consent provision process, the end users will be thoroughly informed regarding the processing operations, the personal data that will be processed, the purpose of the personal data processing operations, the data controllers and any potential data processors, the period of storage of the personal data and their data protection related rights and the way they could exercise them.

6 Collection of personal data

During the use of the app and depending on the personal data, the project partners collect the personal data through the following means:

i. Automatically through the use of the wearable to be worn by the end user, which will transfer the collected personal data via Bluetooth collection to the iPROLEPSIS app or
ii. Through direct insertion of the personal data from the end users themselves in the iPROLEPSIS app. This included direct upload of information or photos, for instance in the case of providing any information requested, taking photographs or performing the touchscreen typing dynamics test.

7 Principles of Data Collection and Processing

7.1 With this Privacy Policy, our aim is to provide the necessary information to the end users of the app about the terms of collection, processing, and transmission of their personal data by our project partners as the Data Controller or Processor. The project partners and their appropriately trained personnel adhere fully to the principles governing the processing of personal data as provided in the GDPR, namely the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.

7.2 Additionally, the project partners respect, protect, and ensure the exercise of the data subjects' rights provided in the GDPR, including:

I. **"Right to be informed"** regarding anything that is related to the processing of personal data (arts. 12-14 GDPR),
II. **"Right of access" to** the personal data and any other information related to the data processing activities (art. 15 GDPR),
III. **"Right to rectification"** of inaccurate personal data or completion of incomplete personal data (art. 16 GDPR),
IV. **"Right to erasure" ("right to be forgotten"),** according to which the data subject could achieve the deletion of his/her personal data under certain conditions (article 17 GDPR),

V. **“Right to restriction of processing”** of the personal data under certain conditions (art.18 GDPR),
VI. **“Right to data portability”,** according to which the data subject can receive the personal data concerning him/her, which had been provided to a controller, in a structured, commonly used and machine-readable format and transmit them to another controller without hindrance from the controller to which the personal data had been previously provided (art. 20 GDPR),
VII. **“Right to object”** at any time to processing of personal data concerning him/her (art. 21 GDPR),
VIII. **“Right to object to the automated individual decision-making, including profiling”** (art. 22 GDPR),
IX. **“Right to withdraw from the provided consent”** freely, at any time and
X. **“Right to appeal against the competent supervisory authority”.**

7.3 The project partners remain at the disposal of the data subjects – end users to respond to any of their requests regarding the above and to ensure the substantial and effective protection of personal data throughout the use of the iPROLEPSIS application, in compliance with the applicable European and national legislation for data protection, as well as applicable regulatory directives related to data management.

For this purpose, the end users can submit a request or exercise their rights by contacting the project partner in charge of the study that they are participating, and, as a consortium, we will make all reasonable and practical efforts to comply with their request. They may file a relevant request to the email address or the mean of communication provided to them by the project partner in charge of the study that they participate in, according to the information provided in the consent form.

8 Minimization, Storage, and Deletion of Personal Data

8.1 The project partners request from the end users the minimum necessary personal data, according to the data minimization principle and as required by law, to fulfill the project related tasks. The selection of the personal data to be collected and processed is based on a selection process that was based on scientifically proven factors that affect the inflammation of the Psoriatic Arthritis disease.

8.2 Our project partners will store the personal data for as long as required by current legislation, based on the respective purpose of processing. Following this, the personal data will be anonymized or deleted.

9 Data Transfer to Third Parties

9.1 As a rule, our project partners do not transfer personal data to any third parties without the need of such processing operation to take place and additionally, the explicit consent of the data subjects. Respecting the principle of confidentiality, they ensure that the personal data processed is not disclosed to unauthorized individuals, taking necessary measures accordingly.

9.2 In the context of processing of the end users’ personal data, it may be necessary to transfer the personal data to the project partner of iPROLEPSIS located in the United Kingdom. In this case, we inform the end users that such transfer is considered secure since the United Kingdom’s legal framework for data protection has been deemed adequate by the issuance of an adequacy decision by the Commission, according to article 45 of the GDPR.

9.3 In any case, the project partners categorically state that they will not transfer the personal data collected during the use of the iPROLEPSIS app to any third parties for their direct use for promotional purposes (marketing).

10 Security

10.1 The secure processing of the end users' personal data is of utmost importance to us. Our project partners take all appropriate organizational and technical measures to ensure the confidentiality, integrity, and availability of the personal data collected under this Policy.

10.2 The project partners acknowledge the purposes described in the grant agreement or any other official documentation of the iPROLEPSIS project, determine the means of processing according to the aforementioned project related purposes and implement the appropriate technical and organizational measures to protect the data being processed. The project partners and any third parties collaborating with them on the processing of personal data, have already fully understood and complied with this policy. No third party can access personal data processed by the project partners without signing a cooperation and confidentiality agreement.

10.3 In compliance with the applicable European and national legislations on the protection of personal data, our project partners have appropriately trained and educated their staff, follow appropriate security policies, and use appropriate technical and operational tools, such as anonymization (whenever applicable), pseudonymization, data encryption, and continuous and targeted staff training.

10.4 Within the framework of the "risk-based approach," which is a novelty of the GDPR, the project partners implement the necessary measures on a case-by-case basis, both primarily preparatory and during processing, to ensure the integrity and security of the end users' personal data. Some of the measures we have taken as a project partners to ensure the integrity and security of data include the commitment of the partners with confidentiality clauses, the identification, restriction, and recording of individuals (physical or electronic) with access to databases, personal data, files, etc., conduction of access policies and measures for secure storage and access control, especially for the special categories of personal data that will be stored in the iPROLEPSIS data management infrastructure.

11 Actions in Case of a Data Breach event

11.1 Despite our project partners' efforts to ensure the integrity and security of the end users' personal data, the rapid development of technology may lead to the emergence of new, unforeseen methods that could result in malicious loss, misuse, alteration, or destruction of their personal data. While our project partners cannot absolutely guarantee the security of the personal data in every unforeseen situation, they do guarantee vigilance and effective management of potential risks, always in collaboration with the competent authorities, beyond the security measures already taken.

11.2 According to Article 33 of the GDPR, the data controller shall notify, without undue delay and, if feasible, within 72 hours of becoming aware of the personal data breach, the supervisory authority as per Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. When notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay. If it is not possible to provide the information simultaneously, it may be provided gradually without unjustified delay.

11.3 Additionally, according to Article 34 of the GDPR, if the personal data held in the project partners' records are breached in a manner that may pose a high risk to the end users' freedoms and rights, we have the corresponding obligation to inform them without undue delay, as provided for in the applicable General Data Protection Regulation (GDPR).

12 Contact

If you have any questions or comments regarding this Privacy and Personal Data Protection Policy, the measures taken by our project partners to protect your personal data or you wish to exercise any of your rights as a data subject, please contact us at the designated email address or the mean of communication provided to you during the consent provision process.

Additionally, the end users could proceed to the aforementioned actions by contacting the authorized legal partner of the project, Diadikasia Business Consulting Symvouloi Epicheiriseon AE, via the email legalint@diadikasia.gr.

13 Validity of the Privacy and Personal Data Protection Policy

This Policy was published by the Project partners on 13/06/2024 and is subject to periodic improvement and revision. For this purpose, we encourage the end users to periodically review this Policy to stay informed about how we manage the end users' personal data.