**Data processing agreement**

Between

The Consiglio Nazionale delle Ricerche (CNR) and The Università (if applicable), Italy as JRU member(s) of the ELIXIR-IT research infrastructure, coordinated by the Consiglio Nazionale delle Ricerche (CNR) and, for it by the Istituto di Biomembrane, Bioenergetica e Biotecnologie Molecolari based in Bari, Via Giovanni Amendola nr. 122/O (“ELIXIR-IT”)

and

\_\_\_\_\_\_\_\_\_, with registered office at \_\_\_\_\_\_\_ [specify the registered office address of Data Controller 2], represented by its legal representative \_\_\_\_\_\_\_\_ [specify the full name of the legal representative of Data Controller 2] PEC:

**Preamble**

This Data Processing Agreement concerns the processing of personal data in the research activity called FEGA.

The European Genome-phenome Archive (EGA) is a service for permanent archiving and sharing of all types of personally identifiable genetic and phenotypic data (Personal Data) resulting from biomedical research project, jointly managed by the European Molecular Biology Laboratory (EMBL) and the Centre for Genomic Regulation (CRG). The submitted Personal Data are accessible and distributed under controlled access policy, whereby access decision reside with the Data Access Committee (DAC), created or defined by the Data Producer for each dataset, and covered by a Data Access Agreement (DAA), defining the terms and condition of the use of a specified dataset.

The Italian Node has signed a Collaboration Agreement for the operation of a Node within the Federated European Genome-phenome Archive (EGA), in order to define the rights and obligations of the Node concerning the provision of Node Services, as well as the role of EGA Central in ensuring alignment and coordination among all Nodes within the EGA Federation;

The Italian FEGA Node relies on the storage services provided by the ELIXIR-IT platform, in particular those delivered within the Compute Platform.

The research activity in this field concerns access to the services provided within the FEGA project. The Federated European Genome-phenome Archive is a federated, distributed service for the long-term storage and sharing of all types of human data resulting from biomedical research projects, where the data is consented for sharing in a controlled access context.

These clauses shall not affect the obligations to which the Data Controller is subject under Regulation (EU) 2016/679.

These clauses do not, by themselves, guarantee compliance with the obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

These clauses shall be read and interpreted in light of the provisions of Regulation (EU) 2016/679.

These clauses shall not be interpreted in a way that is inconsistent with the rights and obligations provided by Regulation (EU) 2016/679 or that would prejudice the fundamental rights or freedoms of data subjects.

In the event of any conflict between these clauses and the provisions of related agreements in force between the parties at the time of acceptance of these clauses, or concluded thereafter, these clauses shall prevail.

The Parties agree as follows:

**Art. 1**

**Scope of Application**

**1.1** The Parties mutually acknowledge that, within their respective organizations, they are aware of and apply all applicable current and forthcoming regulations concerning the processing of personal data, both primary and secondary, relevant for the proper management of the Processing, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter “GDPR”).

**1.2** The Parties mutually acknowledge that the data exchange under this Agreement complies with the principles of lawfulness as determined by specific regulations.

(to adapt) In the context of the \_\_\_\_\_\_ project, the present research activity \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:  
a) Directly from data subjects, in previous projects;  
b) Pre-existing clinical and outpatient records;  
c) Open data databases;  
d) Datasets produced by public or private entities, both national and international;  
e) Internal and external databases;  
f) Existing biobanks;  
g) Electronic devices used in past studies.

The project partners, acting as independent data controllers, are responsible for the proper management of these data collections, ensuring that all operations comply with the security measures set forth by the Data Protection Authority, in particular those indicated in point 4.2, letters a), b), and d), regarding the custody and security of genetic data and biological samples.

Furthermore, in accordance with the Data Transfer Agreements (DTA) concluded with each partner, compliance with all applicable regulations is ensured. These agreements confirm that all necessary consents have been previously obtained in accordance with legal and ethical requirements, reflecting the partners’ ongoing commitment to data protection and adherence to research ethics.

The management of genetic data will be carried out through the ELIXIR-IT infrastructure, and the privacy policies, Terms of Use, and Acceptable User Policy specifically defined for these services, as described in Article 5 of this Agreement, will be adopted.

**Art. 2**

**Relationships between Independent Data Controllers**

**2.1** The Parties will process personal data independently, for purposes related to the execution of the project, upon signing a Data Transfer Agreement (DTA) with CNR on behalf of ELIXIR-IT and, in any case, in compliance with applicable law and as agreed in the study protocol.

Furthermore, for access to ELIXIR-IT services, the Parties will enter into specific agreements regarding access to the resources, in which they commit to comply with the Terms of Use (ToU) and the Acceptable Use Policy (AUP).

2.2 In relation to the use of the aforementioned data within their own organizations, the Parties shall therefore assume the status of independent Data Controllers pursuant to Article 4, no. 7) of the GDPR, both among themselves and towards the data subjects to whom the processed personal data relate.

**Article 3**  
**Type of Data Subject to Exchange**

3.1 The Parties mutually acknowledge that “communication” refers both to the transmission of data and to the sharing of databases, for the purposes of accessing ELIXIR-IT services.

3.2 The data flow is described in Figure 1 attached to this Agreement.

3.3 With regard to the exchange of information, the following is specified:  
The transfer of data for the purposes of accessing services provided by ELIXIR-IT will be carried out in full compliance with applicable personal data protection regulations and transfer security requirements.

**Data Pseudonymization:**

Personal data relating to participants of pre-existing study cohorts will be provided to the FEGA project in already pseudonymized form by the original data controllers.

Data Transfer:

Pseudonymized data will be transferred electronically via ELIXIR-IT. The use of this platform ensures:

* Data Encryption: Data will be encrypted both during transfer and storage, using encrypted channels implemented by ELIXIR-IT in accordance with the security requirements of Article 32 of the GDPR.
* Authentication and Access Control: Only authorized personnel will be able to access the data through asymmetric key-encrypted tunnels, using two-factor authentication and/or asymmetric key-based authentication mechanisms.

**Genotyping and Sequencing of DNA Samples:**

* Samples included in the clinical cohorts of cardiovascular diseases and patients affected by mild cognitive impairment will undergo genome-wide genotyping using SNP arrays specifically selected to enable clinical research studies, association validation, risk profiling, preventive screening, pharmacogenomics studies, and precision medicine applications, widely used in areas such as polygenic risk and nutrigenomics. For this purpose, DNA samples will be sent from the participating institutes to the designated external company.
* Samples included in the clinical cohorts of neurological diseases, both common and rare, including “rare genetic disorders,” will undergo whole-genome sequencing. This activity is aimed at both genetic risk profiling and the identification of genetic and molecular determinants associated with the aforementioned diseases. To this end, DNA samples will be sent directly from the respective participating institutes to the specifically selected external companies tasked with performing this activity.

**Audit Trail:**

A complete record of all operations performed on the data will be maintained to ensure transparency and accountability of activities.

The transfer will be planned and monitored to minimize any risk, ensuring compliance with the protection standards required by European and international regulations.

**3.4** The communication for the purpose of accessing ELIXIR-IT services will concern the following categories of data (to be adapted according to the dataset): personal data of patients assisted by the project partners, or of volunteers participating in research projects conducted by the project partners, including:

* Sex and age;
* Anthropometric data and health-related data collected during medical visits, hospitalizations, emergency room admissions, as well as examinations and assessments carried out at the Healthcare Facility. In particular, the data concern diagnoses, medical procedures, administered therapies, laboratory test results, medical devices, and biological samples;
* Genetic data.

The data subjects are:

* Patients who have received healthcare services from the project partners as part of normal clinical practice; such patients may include minors, persons temporarily unconscious (e.g., in a coma), and individuals under guardianship or incapacity;
* Volunteers who have participated in previous research projects conducted by the partners.

For administrative, management, and/or activity monitoring purposes, data concerning the personnel involved in the study will also be processed.

**Art.4**

**Legal Compliance**

**4.1** As independent Data Controllers, the Parties are required to comply with all relevant regulations on the protection and processing of personal data applicable to the relationships between the data holder and the recipient under this Agreement, as well as those applicable to the relationships between the controller and the data subject, and between the controller and public authorities.

The Data Controller transferring data for access to the services, in accordance with the provisions set out in the AUP and ToU (attached to this Agreement), guarantees that prior consent from the data subject for the disclosure of data and samples to third parties has been obtained.

**Art. 5**

**Security Measures**

5.1 The Parties agree on the adequacy of the security measures implemented to ensure the secure exchange of data.

5.2 In particular, they confirm the implementation of the following measures:

Training and Awareness of Personnel  
All staff members involved in data processing are regularly invited to attend training courses on personal data protection. They are properly informed about the data management plan, data access policy, and code of conduct. All members who have access to the data and later terminate their employment relationship will have their user accounts deleted and access revoked.

Security of IT Channels  
The transfer of genetic data in electronic format is carried out through secure communication channels using the services provided by the ELIXIR-IT Compute platform.  
Data in transit are protected through encryption compliant with internationally recognized standards, both symmetric (e.g., AES-256 or equivalent) and asymmetric.

Access Controls and Strong Authentication

* Multi-factor authentication (MFA) is required for system access.
* Access roles and profiles are based on the *principle of least privilege*, granting each user only the permissions necessary to perform their duties.
* Identity and Access Management (IAM) solutions are in place, with regular updates of access rights.

Encryption and Robust Pseudonymization  
The project exclusively uses pseudonymized data from the outset. The association databases and decryption keys—allowing re-identification of pseudonymized data—are held by the data providers (the involved CNR Institutes and IRCCSs), which adopt appropriate technical and organizational measures to ensure information security.  
Data, both in transit and at rest, are protected by encryption compliant with internationally recognized standards (e.g., AES-256 or equivalent).

Version Control and Regular Backups  
Regular backups are performed and stored in segregated and secure environments to ensure recovery in case of damage or tampering.  
Daily backups and data retention of at least 30 days are maintained on separate IT systems.

Audit Logs and Access Traceability  
The IT system implements an audit logging mechanism to record all activities performed on personal data, allowing detection of unauthorized access or use and identification of security incidents.  
Log files contain detailed information on access events, operations performed, and timestamps, in compliance with the accountability principle.  
Such records are securely stored for a minimum of six months, in line with cybersecurity best practices and applicable guidelines.

Security Assessments and Regular Updates  
The IT system is subject to regular security assessments to identify and mitigate vulnerabilities. These assessments include:

* Periodic audits: Scheduled analyses of security configurations, access permissions, and implemented data protection measures.
* Penetration testing: Simulated tests to identify potential security flaws, performed at least annually or more frequently after major updates.
* Security policy review: Regular verification to ensure policies remain aligned with the latest technological and regulatory standards.

Additionally, the system is maintained through:

* Software updates: Timely application of security patches and system updates to prevent exposure to known vulnerabilities.
* Continuous monitoring: Implementation of monitoring tools to detect suspicious activity, anomalies, or unauthorized access in real time.

Vendor Evaluation and Responsibility Contracts  
Vendors are selected based on their data protection capabilities, including certifications (e.g., ISO/IEC 27001) and security policies.  
Relationships are governed by contracts compliant with Article 28 of the GDPR, including obligations to process data only under the controller’s instructions, adopt adequate security measures, notify data breaches, and obtain authorization for any sub-processors.  
Vendors are subject to regular audits to verify compliance with regulatory and contractual obligations, with particular attention to sensitive data such as genetic or health information.

Malware Protection  
The IT system employs advanced measures for the prevention, detection, and mitigation of malware, in accordance with Article 32 of the GDPR. These measures include:

* Antivirus and anti-malware solutions: Regularly updated software to protect against known threats and new variants.
* Continuous monitoring: Intrusion detection/prevention systems (IDS/IPS) and behavioral analysis tools to identify suspicious activity in real time.
* Secure use policy: Restrictions on the installation of unauthorized software, with centralized update management.
* Periodic training: Raising user awareness about malware risks, such as phishing and suspicious attachments.
* Incident response plans: Protocols to promptly contain and resolve infections, restore data, and report to authorities when required.  
  All measures are regularly tested to ensure effectiveness and updated against emerging threats.

Data Partitioning  
Within the IT system, genetic and health data are processed separately through logical and physical partitioning.

Data Minimization  
Only the data necessary and foreseen by the study protocol are processed.

In particular, each Party undertakes to apply appropriate and adequate security measures to protect the personal data processed under this Agreement against the risks of destruction (even partial), accidental or partial loss, unauthorized access or modification, and any processing not permitted or inconsistent with the purposes of collection.

**Art. 6**

**DPIA**

**6.1** All Parties have jointly prepared the Data Protection Impact Assessment (DPIA) for the FEGA Project in accordance with Article 35 of the GDPR, with respect to the processing operations under their responsibility. The DPIA is attached to this Data Processing Agreement (where required).

**Art. 7**

**Obligations of Authorized Personnel**

**7.1** The Parties undertake to ensure that access to the personal data subject to exchange is granted only to those individuals, and only to the extent, necessary for the execution of the Project, and that the use of personal data by each Controller complies with the same commitments undertaken by the data holder regarding the lawful processing and security of the data, with measures appropriate to the type of data subjects and the associated risks.

**7.2** The Parties undertake to duly authorize and instruct, in writing, the personnel involved in the processing of personal data and to ensure that such personnel receive regularly updated training.

**Art. 8**

**Further Transfers**

**8.1**  
The Parties agree that personal data received under this Agreement shall not be transferred to any third party, except in the following cases:  
a) the transfer is necessary for the establishment, exercise, or defence of legal claims in specific administrative, regulatory, or judicial proceedings;  
b) the transfer is necessary in order to protect the vital interests of the data subject or of another natural person; or  
c) the Party that has received the data has obtained the explicit consent of the data subject for the specific transfer, after having informed them of its purposes, the identity of the recipient, and any potential risks of such transfer, in particular due to the absence of adequate data protection safeguards.

**8.2**  
In all cases, the Party intending to make a transfer to third parties shall inform in advance the Party from which the data were originally received and, upon request, shall provide a copy of the information supplied to the data subject or to the third-party recipient.

**8.3**  
Any further transfer shall in all circumstances comply with the safeguards set out in this Agreement and with all applicable data protection legislation, including obligations regarding security, transparency, and purpose limitation.

**Art.9**

**Liability**

**9.1**  
Without prejudice to any non-derogable provisions of the law, no Party shall be held liable for the processing carried out by the other Party, except in cases of mismanagement or mishandling during the original collection and transfer of personal data. The Parties undertake to indemnify and hold harmless the other Party from any damages, including legal costs, that may arise from claims made by third parties – including data subjects – as a result of any unlawful or improper processing attributable to each Party.

**Art. 10**

**Organizational Arrangements**

**10.1**The Parties mutually warrant that the data processed by each of them under this Agreement are subject to thorough compliance checks with the relevant personal data protection regulations—including the GDPR—and further undertake to cooperate optimally with each other in the event that one Party receives requests for the exercise of data subject rights pursuant to Articles 12 et seq. of the GDPR, or requests from supervisory authorities concerning processing activities under the responsibility of the other Party.

.

**Art. 11**

**Exercise of Data Subject Rights**

**11.1**  
The Parties undertake to assist each other promptly and effectively in facilitating the exercise of data subject rights and to comply without undue delay with the obligations falling within their respective responsibilities.

**Art. 12**

**Duration**

**12.1**  
This Data Processing Agreement shall remain in effect for [………………] from the date of its signature.

**Art. 13**

**Termination**

**13.1**  
Each Party may freely and unilaterally withdraw from this Agreement prior to the agreed term by providing 90 days’ notice via certified email (PEC).  
The Parties agree that the exercise of the right of early withdrawal is not subject to any payment.  
Any exercise of the right of withdrawal shall have no retroactive effect on services already performed under this Agreement.  
The exercise of the right of withdrawal by one Party shall not affect the sole responsibility of each Party for the processing operations carried out under its responsibility.  
Even in the event of early withdrawal, the Parties remain obliged to indemnify and hold harmless the other Party from any damages, including legal costs, that may arise from claims by third parties – including data subjects – as a result of any unlawful or improper processing attributable to each Party.

**Art. 14**

**Governing Law and Jurisdiction**

The competent court for any dispute arising from this Agreement shall be the Court of Rome.

CNR-IBIOM

By:

Title: Director

Date:

**Part II**

………………………………………..

By:

Title:

Date:

…………………………………………

By: \_\_*(scientific coordinator)*

Title:

Date:

…………………………………………

By: \_\_ *(scientific coordinator)*

Title:

Date:

**FOR ELIXIR-IT**

ELIXIR-IT

By:

Title: Head of the Node

Date:

##### DATA TRANSFER AGREEMENT

BETWEEN

**The Consiglio Nazionale delle Ricerche (CNR) and The Università (if applicable), Italy as JRU member(s) of the ELIXIR-IT research infrastructure, coordinated by the Consiglio Nazionale delle Ricerche (CNR) and, for it by the Istituto di Biomembrane, Bioenergetica e Biotecnologie Molecolari based in Bari, Via Giovanni Amendola nr. 122/O** (“ELIXIR-IT”) (in the following also called“Provider”)

and

**Part I**, a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(in the following called“Recipient”)

ELIXIR-IT and Part I may be referred to herein individually as a “Party” or together as the “Parties” (also individually referred to as the “Provider/Recipient” and collectively the “Parties”)

**Recitals**:

**a)** Consiglio Nazionale delle Ricerche (**CNR**) is a public organization; whose duty is to carry out, promote, spread, transfer and improve research activities in the main sectors of knowledge growth and of its applications for the scientific, technological, economic and social development;

**b)** ELIXIR-IT is the Italian Node of ELIXIR, the European infrastructure for life science data, supporting basic and translational research by providing bioinformatics services and facilitating access to data in the fields of biological sciences. The Italian Node of ELIXIR is coordinated by the National Research Council (CNR) and has been formally established as a Joint Research Unit (JRU) among all partners including research institutes, universities and technological institutions.

**c)** Provider is the CNR (and a member of the JRU of ELIXIR-IT) (if applicable) which has extensive expertise, skills and specific Know-how on the bioinformatic services offered through ELIXIR-IT platforms and validated by QM Policy approved;

**d)** The European Genome-phenome Archive (EGA) is a service for permanent archiving and sharing of all types of personally identifiable genetic and phenotypic data (Personal Data) resulting from biomedical research project, jointly managed by the European Molecular Biology Laboratory (EMBL) and the Centre for Genomic Regulation (CRG). The submitted Personal Data are accessible and distributed under controlled access policy, whereby access decision reside with the Data Access Committee (DAC), created or defined by the Data Producer for each dataset, and covered by a Data Access Agreement (DAA), defining the terms and condition of the use of a specified dataset.

**e)** the Italian Node has signed a *Collaboration Agreement for the operation of a Node within the Federated European Genome-phenome Archive (EGA)*, in order to define the rights and obligations of the Node concerning the provision of Node Services, as well as the role of EGA Central in ensuring alignment and coordination among all Nodes within the EGA Federation;

**f)** the Italian FEGA Node relies on the storage services provided by the ELIXIR-IT platform, in particular those delivered within the Compute Platform.

**d)** Submitter/data owener is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

**e)** The Parties agree that the purpose of this Agreement (hereinafter referred to as the “Purpose”) is to establish and operate a repository for the provision of the services of the Italian FEGA Node within the Federated European Genome-phenome Archive (FEGA).  
In particular, the repository shall enable the secure storage, management, and controlled access to genomic, phenotypic, and related datasets, in compliance with applicable ethical, legal, and technical standards.  
The data and materials transferred under this Agreement shall be used exclusively for the implementation, maintenance, and operation of the Italian FEGA Node services and for ensuring interoperability and alignment with the EGA Federation and ELIXIR-IT platforms.

**f)** The Provider has received from the Submitter (or Data Owner) the data necessary for the establishment, validation, and operation of the repository, in order to enable the provision of services of the Italian FEGA Node within the Federated European Genome-phenome Archive (FEGA) (hereinafter referred to as the “Purpose”).  
Such data are transferred exclusively for the implementation, testing, and secure operation of the repository and shall be used solely within the scope of the activities necessary to provide the FEGA Node services, ensuring compliance with the applicable ethical, legal, and technical requirements, as well as with the policies of the EGA Federation and the ELIXIR-IT infrastructure.

g) The Submitter (data owner) is willing to provide the Provider with the Data, and the Provider agrees to accept such (Material and) (if applicable) Data from the Submitter (data owner), under the terms and conditions set forth in this Agreement.

##### Accordingly, the Parties have agreed as follows:

Submitter (data owner) agrees to transfer to Provider the following Data:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*indicare quantità e specifiche tecniche precise)*

(in the following called “Material/Data”).

The data transferred by the Submitter (data owner) to the Provider (hereinafter referred to as “Data”) are the property of the Submitter, including Background Technology (any know-how and patent rights related to the Purpose, developed or acquired by either Party prior to signing, or subsequently independently of the performance of the scientific activity but useful for the achievement of such Purpose). Each Party shall retain full ownership of its Background Technology and shall have the right to use the other Party’s Background Technology solely for the purpose of performing the scientific activity. Each Party shall be free to disclose its Background Technology at any time during the execution of the Work or Scientific Program (choose one of the two definitions) under this Agreement.

Any other use of data beyond the aim established in this agreement is strictly prohibited. Commercial use of -------- data (as detailed in Annex A) or results deriving from ------ data (as detailed in Annex A) is strictly prohibited as well, unless approved by an ad hoc agreement extending the here described Terms of use.

This Material (Data) will be used by the Provider solely in connection with the purpose of this Agreement, for \_\_\_\_\_\_\_\_\_\_\_\_ and more specifically for \_\_\_\_\_\_\_\_\_\_\_\_\_\_ (specify)

1. To the extent permitted by law, Provider agrees to treat in confidence, for a period of 3 (three) years from the date of its disclosure, Data that is/are marked “CONFIDENTIAL” (hereinafter “Confidential Information”), except for information that:

* was previously known to Provider or that is or becomes publicly available through no fault of Provider or
* which is lawfully disclosed to Recipient without a confidentiality obligation or
* that is independently developed by Provider without the benefit of any disclosure by Provider.

Provider shall use the same degree of care in maintaining the confidentiality of the confidential information as it uses with respect to its own information that is regarded as confidential and/or proprietary. Furthermore, Provider will restrict the access of all confidential Information to only those of its employees, consultants and external collaborators who need to be informed for the purposes for which the confidential Information is provided.

4. All publications or any other dissemination relating to the use of the Data shall indicate that *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*has/have been provided by the Provider, by the means of the ELIXIR-IT.

**If positive or interesting results, data or inventions relating to the use of the Data (in the following called the “Results”) are obtained, the Parties should establish a joint exploitation agreement regarding the exploitation terms of such Results.**

##### 5. The Data is being supplied to Provider with no warranties of any kind, either expressed or implied. There are no expressed or implied warranties of merchantability or fitness for a particular purpose, or that the use of the Material and/or Data will not infringe any patent, copyright, trademark or other third party’s proprietary rights.

6. The Data will be delivered to the Provider after the signature of this Agreement.

##### 7. Nothing in this Data Transfer Agreement shall or may be construed as granting Provider any right or licence to Data for any use other or further than the \_\_ (*specificare, tenendo conto di quanto indicato in premessa e al punto 2*), described here above.

##### 8. This Agreement shall be governed by and construed in accordance with the laws of Italy. The Parties agree on settling any dispute, arising from this Agreement, out of court. If an amicable settlement cannot be reached, all disputes arising out of or in connection with this Agreement shall be settled in first instance by the relevant court in Rome.

9. No amendment or modification of this Agreement shall be valid or binding on the Parties unless made in writing and signed on behalf of each of the Parties by their respective duly authorized representatives.

##### 10. This Agreement shall become effective upon the latest date of signing and will expire \_\_\_\_\_\_\_\_\_\_\_\_ *(indicare).* The obligations of confidentiality will be in effect for five (5) years starting from the above effective date.

**PROVIDER**

CNR-IBIOM

By:

Title: Director

Date:

**Submitter**

………………………………………..

By:

Title:

Date:

…………………………………………

By: \_\_*(scientific coordinator)*

Title:

Date:

…………………………………………

By: \_\_ *(scientific coordinator)*

Title:

Date:

**FOR ELIXIR-IT**

ELIXIR-IT

By:

Title: Head of the Node

Date: