ELIXIR-IT Acceptable User Policy

Conditions for the Use of Omics Platform Services Provided by ELIXIR-IT (AUP)

The Italian Node of the European Research Infrastructure ELIXIR has been formally established as a Joint Research Unit (JRU) under the name **Italian Bioinformatics Infrastructure** (ELIXIR-IIB or ELIXIR-IT). ELIXIR-IT is coordinated by the **National Research Council (CNR)** and currently includes 30 partners, among which various universities, research institutes, and public providers of Cloud and High-Performance Computing (HPC). (For updates on the composition of the partnership, please refer to the ELIXIR-IT website: https://elixir-italy.org/) (hereinafter referred to as **ELIXIR-IT**).
The Italian ELIXIR Node aims to establish the **Italian Bioinformatics Research Infrastructure (IIB)**, which is distributed across multiple centers. Its mission is to support all Italian researchers working in the fields of **Bioinformatics and Life Sciences**, promoting knowledge exchange and skills development. Additionally, it seeks to integrate national platforms for omics data production and ICT, leveraging a wealth of internationally recognized and publicly available bioinformatics resources and contributing to their integration within the European infrastructure.
Another primary goal of **ELIXIR-IIB** is to **organize training activities**, both basic and advanced, across different bioinformatics application areas. These initiatives aim to support the education of young bioinformaticians, a highly demanded professional profile both nationally and internationally.
ELIXIR activities are structured into **technology platforms**, which coordinate the delivery of **high-quality services** for the life sciences and facilitate the integration of national services into the broader **ELIXIR infrastructure**.
ELIXIR-IT operates through six key platforms:

- **Compute**
- **Data**
- **Interoperability**
- **Tools**
- **Omics**
- **Training**

Use of the provided services is open to the entire **national scientific community** and enterprises, subject to a specific request submitted in accordance with the procedures and policies defined by **ELIXIR-IT**. Access is granted only after reading, understanding, and explicitly accepting the **terms and conditions** outlined in this document.
These **Acceptable Use Policies (AUP)** apply to the services within the **Omics platform**.
The **Omics Platform** provides services for **omics data generation**, including **high-throughput nucleic acid sequencing** and **large-scale characterization of metabolomes and proteomes**.
The equipment has been primarily acquired through funding from the **PON CNR.BiOmics** and **PNRR ELIXIRxNextGenIT** projects, supported by the **Italian Ministry of University and Research**. This funding has enabled **ELIXIR-IT** to develop a **rich portfolio of genomic and proteomic analysis instruments**, accessible to the entire scientific community.
For a list of available equipment and laboratories, please visit the **ELIXIR-IT website**: https://elixir-italy.org/
Examples of services offered:

- **Whole genome, exome, and transcriptome sequencing**
- **Single-cell genome and transcriptome sequencing**, including **spatial resolution analysis**
- **Microbiome analysis** through **metagenomics** and **DNA metabarcoding sequencing**
- **Optical mapping of chromosomes**
- **Epigenetic analysis**
- **Metabolomics and proteomics analysis**

The services provided within the **Omics Platform** also leverage selected resources from the **ELIXIR-IT Compute Platform**, enabling **bioinformatics analysis**, as well as **storage, sharing, and retrieval** of research results.

Definitions

- **Service Provider Institution:** The institution that, as a member of ELIXIR-IT, provides a service within the Omics Platform, including the use of resources from the Compute Platform.
- **Service Manager:** The individual responsible for managing the service offered within the platform and/or included in the ELIXIR-IT Service Delivery Plan, in coordination with the Platform Leaders (Omics and Compute) of ELIXIR-IT. The Service Manager ensures access, oversees operations, and monitors the performance of the provided service.
- **Compute Platform System Administrator:** Any individual within the institution providing the service under ELIXIR-IT, who is assigned to manage computing resources on behalf of the Service Manager.
- **Service Access Administrator User:** A system administrator user with the necessary privileges to manage cloud resources, add users, and administer services.
- **User:** Any individual who, in any capacity, obtains access permissions or the right to use services provided by ELIXIR-IT.

Terms and Conditions

Users of the services offered by the Platform Omics are required to comply with the following terms and conditions:

1. Processing is carried out exclusively based on an agreement/project that clearly defines the purpose of the research activity to be conducted.
2. The user undertakes to comply with all the conditions set forth in this document, as well as those specified in the **"Acceptable User Policy - Terms of Use, QM Policy, and ELIXIR-IT Services Privacy Policy"**, where relevant to the specific service of interest.
3. The user commits to delivering **sensitive samples (e.g., human samples) in anonymous or pseudonymized form**.
4. The **transportation of biological samples** shall be conducted in a manner that ensures their **quality, integrity, availability, and traceability**.
5. The **electronic transfer of genetic data** must be carried out through **secure communication channels** via **web applications** using the services provided by the **ELIXIR-IT Compute Platform**.
6. **Genetic data and biological samples** contained in **lists, registries, or databases** shall be processed using **encryption techniques** or **identification codes**. These solutions must ensure that, given the volume of data and samples processed, the information remains **temporarily unintelligible** even to those authorized to access it. Identification of data subjects should only be possible **in case of necessity**, minimizing the risks of **accidental disclosure** and **unauthorized access**.
7. If **lists, registries, or databases** are maintained electronically and contain **genealogical or health-related information**, the applied techniques must also enable the **separate processing of genetic and health data from other personal data** that could directly identify the individuals concerned.
8. The obligations set forth in **Article 9 of the GDPR** and the **provisions of the Italian Data Protection Authority** (Regulation on the processing of special categories of data, issued under **Art. 21(1) of Legislative Decree No. 101 of August 10, 2018**, published in the **Official Gazette No. 176 of July 29, 2019**) remain in effect. This includes **rules on data storage, external transport, and access control** to **protected premises**.
9. Users acknowledge that the **Omics Platform services** are also subject to the **laboratory regulations** available at the following link: **Google Drive document**.

Additional Terms and Conditions for Users of the Omics Platform Who Also Utilize the Cloud Services Provided by the ELIXIR-IT Compute Platform

1. The User must be identified through Life Science AAI or another two-factor authentication system deemed equivalent.
2. Access is subject to prior approval by the Service Manager.
3. The Service Access Administrator User may, at their discretion, grant access to other Users for the resources assigned to them, under the following conditions:

a. a. The Service Access Administrator agrees to identify every User to whom access is granted and must be able, at any time, to provide ELIXIR-IT with a list of such Users.
b. The Service Access Administrator undertakes to have each User sign this AUP, as well as the documents listed in point 1 and any subsequent updates, along with the usage rules for computing resources adopted by ELIXIR-IT. The Service Administrator must block access for Users who do not accept the new versions of the aforementioned documents. They also commit to verifying that Users have completed a basic cybersecurity course, which may be delivered in e-learning mode, as provided by the User's home institution/organization.
c. The Service Access Administrator shall NOT share privileged access to the resources assigned to them.

4. The User shall **not share** their ELIXIR-IT service access credentials.
5. The User agrees to **promptly follow any instructions** communicated by the Service Manager.
6. The User commits to **reporting any violations** of these conditions to the Service Manager.
7. The **Service Access Administrator** consents to having the resources they instantiate subjected to **periodic security scans** and agrees to **promptly address or mitigate any reported vulnerabilities**, following any suggestions provided.
8. Use of the resources is granted **solely for the purposes** specified in the **JRU founding act** of ELIXIR-IT.
9. The User acknowledges that, while **ELIXIR-IT** and the **Service Provider Institution** offer assistance and endeavor to **promptly resolve** any service interruptions, they **cannot guarantee continuous service**.
10. The User acknowledges that, **unless otherwise agreed**, neither **ELIXIR-IT** nor the **Service Provider Institution** can be held **responsible for data backup**.
11. The User accepts that **logs will be kept** regarding the use of services offered by the **ELIXIR-IT Compute Platform**, in accordance with **applicable regulations**, **CNR regulations**, and those of other participating institutions, as well as the **Regulation on the use of ICT infrastructure resources** that form part of **ELIXIR-IT**.
12. The User acknowledges that personnel made available by the **JRU partner institutions**, who contribute to the operation of the infrastructure, may **monitor the resources** in use.
13. The **Compute Platform Administrators**, acting under the delegation of the Service Manager, may provide support upon **specific request** from the User, provided that the User has configured **SSH key-based access** to their machines.
14. If the User requests **maintenance** services, they are responsible for **backing up their data** beforehand. Any **data loss** resulting from maintenance cannot, under any circumstances, be attributed to the personnel made available by **ELIXIR-IT** or by the **Service Provider Institution** tasked with performing the maintenance.

ELIXIR-IT reserves the right to modify this document in the future. The contents of any new version shall entirely replace the present version and shall have the same legal effect. New versions will be published on the ELIXIR-IT website at least one month prior to their effective date, and a copy will be sent, using the email address provided at registration, to all Users, who will have the opportunity to withhold acceptance. Failure to accept the new version will result in the forfeiture of the right to use the resources. Continued use of the services offered by the Compute Platform after the new version comes into effect shall constitute acceptance thereof.
Any violation of this AUP may lead to the suspension or revocation of the User's access to the resources provided by the service.

Terms of Use for the Utilization of the Omics Platform Services Provided by ELIXIR-IT (ToU)

The Italian Node has been formally established as a Joint Research Unit (JRU), coordinated by the National Research Council (CNR), which includes several universities, research institutes, and public providers of Omics services.
ELIXIR-IT makes Omics Resources available through its OMICS platform, also to third parties (hereinafter referred to as Users).
Access to the Platform is provided under the conditions outlined in the Acceptable User Policy, Terms of Use, QM Policy, and ELIXIR-IT Services Privacy Policy documents.

1. The User declares to have all the necessary technical knowledge to use the Resources made available by ELIXIR-IT and undertakes to ensure that all individuals to whom they may grant access comply with the provisions of this document and the documents listed (acceptable User Policy, Terms of Use, QM Policy, and ELIXIR-IT Services Privacy Policy documents).

2. . The User shall indemnify and hold harmless ELIXIR-IT and the entity providing the service from any claims or demands for damages made by any party arising from the violation of the aforementioned provisions or, in any case, from the conduct of the User and/or individuals to whom they have granted access.

3. Access authorization is granted by the Service Manager or their delegate for a limited period, corresponding to the duration of the relationship under which the activity with the provided IT resources is permitted.
4. Log files related to access to the provided services will be retained for six months and made available to the Judicial Authority (AG).
5. The User/Service Access Administrator is allowed to use the Resources in compliance with and within the limits of the Project/Agreement/Contract under which access was granted. Therefore, it is prohibited to:
    a) To use the Resources for commercial purposes or for profit, transmit commercial or advertising material (spamming), or allow third parties to use the Resources for such activities.
    b) To engage in activities that may damage, destroy, compromise the security of the Resources, or violate confidentiality and/or cause harm to third parties.
    c) To carry out activities aimed at bypassing the provisions of this document or those in point 1 of this document, or to obtain services beyond those agreed.
    d) o use IP addresses other than those assigned, in case the transfer of human genetic data in electronic format is done through communication channels of the "web application" type provided by the ELIXIR-IT Compute Platform.
    e) To create, transmit, or store images, data, or other material that is offensive, defamatory, obscene, indecent, or that violates human dignity, especially if related to sex, ethnicity, religion, political opinions, or personal or social condition.
    f) To access or use any system without authorization, including attempts to scan and verify potential vulnerabilities.
    g) To falsify the headers of TCP/IP packets, email messages, or any part of a message that describes its origin or path.
    h) To engage in port scanning, network scanning, denial of service (DoS), and distributed denial of service (DDoS) activities.
    i) To host services that distribute unauthorized traffic, such as open relay or TOR exit nodes.
    j) To engage in Virtual Currency Mining activities.

k) To operate or run any type of game server.

5. The Service Access Administrator agrees, also on behalf of those to whom they have granted access to the Resources, to use them exclusively for lawful purposes and in compliance with national, EU, and international law, as well as with the regulations and customary practices for the use of networks and services accessed.

6. The user is aware that the entity providing the service will return (where possible) or dispose of the biological samples after the requested service has been completed.
7. The user agrees to comply with the regulations intended for the protection of biological samples collected and sent to the Service Manager for the purpose of execution, including the provisions of the Personal Data Protection Authority, and, where applicable, the regulations established by Circular No. 16/1994 of the Ministry of Health and Circular No. 3/2003 of the Ministry of Health and subsequent amendments
8. The Service Access Administrator declares to be the exclusive administrator of the Resources (to the extent that the definition of administrator is appropriate for the obtained Resources) and therefore the sole responsible party for:
    a) Managing the data and/or information and/or content processed on the platform, ensuring their security, backup, and any activity necessary to maintain their integrity, committing to apply suitable and adequate security measures;
    b) he content of information and data accessible and/or made available on the platform and, in any case, transmitted or made online by the User;
    c) Malfunctions of the Resources due to uses not in compliance with the provisions of this document;
    d) The loss or disclosure of access credentials;
    e) Managing access to the Resources by ensuring the modification of access credentials at least every 12 months.

9. The User/Service Access Administrator agrees to promptly report any use of the Resources that does not comply with the provisions of this document or any security violations they become aware of.
10. The User/Service Access Administrator agrees, also on behalf of those whom they have allowed to use the Resources, not to install software without a valid license.
11. The User/Service Access Administrator is the sole and exclusive responsible for any action carried out without prior formal agreement with ELIXIR-IT, related to the use, management, and administration of the Resources, with respect to which they agree to:
    a) Comply with and ensure that third parties comply with the applicable regulations, including those related to personal data protection under EU Regulation No. 679/2016 and Legislative Decree No. 196/2003 and its amendments, as well as those modified and supplemented by Legislative Decree 101/2018 and its amendments.
    b) Indemnify and hold ELIXIR-IT and the service provider harmless from any and all claims or demands for direct or indirect compensation for damages, of any nature or kind, made by anyone.
12. The User/Service Access Administrator agrees to indemnify and hold ELIXIR-IT and the service provider harmless from any and all third-party claims or demands for damages caused to them by or through the use of the Resources, covering the costs, compensations, liabilities, and legal expenses that may arise from liability actions, and agrees to inform ELIXIR-IT of any actions taken against them.
13. ELIXIR-IT and the service provider will not be held liable in any case for the use of the Resources in relation to critical situations that may involve, by way of example, risks to the safety of individuals, damage to the environment, services intended for people, or damage to facilities.
14. ELIXIR-IT and the service provider will not be liable in any case for the information, data, or content entered, transmitted, or otherwise processed by the User/Service Access Administrator in the use of the Resources, or generally related to the use of the Resources, and they reserve the right to take any action to protect their rights and interests.

15. The User remains the sole owner, in accordance with EU Regulation No. 679/2016 as well as Legislative Decree No. 196/2003, as amended and supplemented by Legislative Decree 101/2018, of the processing of the data entered and/or processed in the Platform.
16. ELIXIR-IT and the service provider reserve the right to activate automatic intrusion detection (IDS) and intrusion prevention (IPS) systems to detect and prevent any violations of the platform's security rules.
17. ELIXIR-IT and the service provider reserve the right to monitor compliance with the rules of this Policy by activating, among other measures, network traffic monitoring activities and filtering systems on the network perimeter devices.
18. ELIXIR-IT and the service provider reserve the right to remove or block any content or resource that violates the provisions of this document.
19. The User/Administrator is required to inform the Service Manager and include a thank-you and/or citation to ELIXIR-IT and the Service used if the use of the service provided by ELIXIR-IT results in a scientific or educational outcome, publication, poster,abstract, or oral presentation.
20. ELIXIR-IT and the service provider, at their discretion and without the exercise of this option being contested as a breach or violation of any potential contract, reserve the right to suspend the availability of Resources, even without prior notice, in the event that:
    a. The User/Administrator of access to the Service violates even one of the provisions contained in the Usage Policy.
    b. There are valid reasons to believe that the Resources are being used by unauthorized third parties.
    c. Cases of force majeure occur, or circumstances arise that, in the unquestionable judgment of ELIXIR-IT and the service provider, require emergency interventions or the resolution of security issues, danger to the entire network, and/or to people or property. In such cases, the availability of the Resources will be restored when ELIXIR-IT has determined that the causes for the suspension have been effectively removed or eliminated.
    d. The User becomes involved, in any capacity, in any legal or even extra-legal civil, criminal, or administrative dispute where the dispute concerns actions and behaviors carried out through the Resources.
    e. The suspension is requested by the Judicial Authority.

21. If users use the ELIXIR-IT Resources for the storage and processing of human genetic data, compliance with the provisions of the GDPR and the applicable national legislation will be ensured, including the provisions outlined in the Garante's decision identifying the requirements contained in the General Authorizations Nos. 1/2016, 3/2016, 6/2016, 8/2016, and 9/2016, insofar as they are compatible with the Regulation and with Legislative Decree No. 101/2018, which implements the December 13, 2018 Code.
22. The transfer of genetic data relating to humans, to access the services, is carried out through protected communication channels, specifically requiring the use of an encrypted channel based on the SSH protocol for data transmission.
    a. Users can access and consult genetic data only through login with the entry of User ID and Password.
    b. Users who access the Resources:
        1. Must ensure that the use of the data does not violate any rights held by third parties;
        2. Must ensure the anonymization or pseudonymization of the data used in accordance with the provisions of the GDPR;
        3. Must ensure the separate processing of genetic and health data from other personal data that allows identification of the data subject.
23. If research activities carried out using the services provided by the ELIXIR-IT Compute Platform result in a publication/poster/abstract or any scientific outcome submitted for publication, the user/service administrator agrees to cite the services used and ELIXIR-IT within the scientific publication.

ELIXIR-IT reserves the right to modify this document in the future. The content of such new versions will entirely replace the current version and have the same value as this document. These new versions will be published on the ELIXIR-IT website (https://elixir-italy.org/) at least one month prior to their effective date. Failure to accept the new version will result in the loss of the right to use the Resources.

Applicative Notes: This Terms of Use (ToU) and Acceptable Use Policy (AUP) template for services aims to be a "Template" that contains essential requirements that should apply to all services offered by ELIXIR-IT to ensure compliance with current regulations.

- Each entity providing the service can personalize the proposed documentation by adding the relevant personal and reference details.
- Each entity customizes the document based on the services offered, excluding its application to services outside the scope of these terms.
- Each entity is also required to add its own logo (in addition to the ELIXIR-IT logo).
- These ToU and AUP must be signed together with the privacy policy for services and referenced in any contracts/agreements governing access to the services.

Privacy Policy for Services (IPS)

Why this notice

In accordance with EU Regulation 2016/679 (hereinafter "Regulation") and Legislative Decree No. 196 of June 30, 2003, as amended by Legislative Decree 101/2018, this notice describes how personal data of users accessing the services of ELIXIR-IT through the entities that provide them are processed. These entities are identified within the Service Delivery Plan (SDP):

ELIXIR-IT

The Italian node of the European ELIXIR Infrastructure is organized as a Joint Research Unit (JRU) named the Italian Bioinformatics Infrastructure (ELIXIR-IT). It is coordinated by the National Research Council (CNR) and currently includes several partners, including universities, research institutes, and public providers of Cloud and High-Performance Computing (HPC) services. (hereinafter ELIXIR-IT).

The Italian ELIXIR Node aims to establish an Italian Bioinformatics Infrastructure (IIB) distributed across multiple centers and intends to support Italian researchers in the field of Bioinformatics, promoting the exchange and development of skills, systematizing various internationally recognized and publicly available bioinformatics resources, and contributing to their integration into the European infrastructure.

ELIXIR-IT also provides both basic and advanced training activities in various application areas of Bioinformatics to support the training of young bioinformaticians, a growing demand at national and international level.

The activities of ELIXIR-IT are divided into technological areas, called platforms. They coordinate the provision of high-quality computational services for life sciences and lead the integration of national services into the ELIXIR-IT infrastructure. ELIXIR-IT includes six operational platforms (Compute, Data, Interoperability, Tools, Omics, and Training).

The services provided are open to employees and associates of the entities that are members of the JRU and to third-party personnel participating in activities defined in a contract or agreement with ELIXIR-IT or with any JRU member, as authorized by the JRU manager, upon reading, understanding, and explicitly accepting the terms and conditions specified in this document.

Data Controller

Name of the service provider entity: (e.g., Institute of Biomembranes, Bioenergetics and Molecular Biotechnologies (CNR-IBIOM))
Address of the service provider entity: Via Giovanni Amendola, 122/O 70126 Bari (BA), Italy
Email: segreteria@ibiom.cnr.it
PEC: protocollo.ibiom@pec.cnr.it

Data Protection Officer

Data Protection Officer (for the service provider entity): Dr. Ing. Roberto Puccinelli
Email: rpd@cnr.it or dpo@cnr.it
PEC: rpd@pec.cnr.it

Processing of Personal Data for Service Use

ELIXIR-IT provides an infrastructure and a set of services for scientific research purposes or for the purposes outlined in the agreement for the establishment of the JRU or defined by other participants in the JRU.

The service is available to JRU members and their employees, or those with access through a project, contract, or agreement with the entity providing the service, as outlined in the Service Delivery Plan of ELIXIR-IT, upon reading, understanding, and explicitly accepting the terms and conditions specified in this document.

The services to which this notice applies are all those described in the technical annex to this contract.

Processing refers to any operation or set of operations regarding the collection, registration, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, deletion, and distribution of data related to the users of the services.

The service provider entity collects information to improve or develop services, generate technical insights, and ensure support.
The data processed for the use of the services are of the types specified below.

Types of Data Processed

Data provided by the user
These are all personal data provided by the user during navigation on the website, such as when registering, accessing a reserved area, or using a service.
Processing for these purposes is carried out with the explicit consent provided by the user, and the data is kept only for the duration of the requested activity. Specific notices may be published for the provision of certain activities.
The optional, explicit, and voluntary sending of emails to the addresses indicated on this site results in the subsequent acquisition of the sender's address, necessary to respond to requests, as well as any other personal data included in the message.
Sensitive or judicial data, if provided by the user, will be deleted.

Accounting Data
To access the ICT services provided by ELIXIR-IT through the service provider entity (e.g., CNR-IBIOM), user registration is required through a Life Science AAI authentication service or an identity provider recognized by CNR, as defined in the agreement/contract.

Monitoring Data
As part of the service activities, the service provider entity's personnel responsible for monitoring and managing user support interventions or conducting periodic security scans may process data related to access logs (including SSH access data).

Communication and Dissemination

The data may be communicated by the Data Controller in the course of their activities and to provide their services, to:

- Public Administrations;
- Service providers, hosting providers, and cloud service providers;
- Judicial Authority.

The collected data will not be disseminated or communicated to third parties, except as provided by the notice and the law, and in any case, only in the manner allowed by them. The data may be accessed by the service provider entity's personnel within their respective functions and in compliance with the received instructions, solely for achieving the purposes outlined in this notice. Recipients will be appointed, if necessary, as Data Processors by the Data Controller, who may be asked for an updated list of the Data Processors. These Data Processors, under the contract, are required to use the personal data exclusively for the purposes indicated by the Data Controller, not to retain them beyond the specified duration, nor to transfer them to third parties without explicit authorization.

Methods of Processing

Personal data processing is primarily carried out using electronic procedures and supports, and in a lawful, correct, and appropriate manner, limited to what is necessary to achieve the purposes of the processing, for only the time necessary to fulfill the purposes for which they were collected, and in any case, in compliance with the principles outlined in Article 5 of EU Regulation 2019/679 GDPR.
Specific security measures are implemented to prevent data loss, unlawful or incorrect use, and unauthorized access.

Location of Data Processing

Personal data processing related to the ELIXIR-IT services provided by the service provider entity takes place at the service provider's facilities and is managed solely by technical staff of the office responsible for processing or by Data Processors appointed by the Data Controller who operate within the European Union. The User's personal data may be transferred to a country other than the one where the User is located. The User can verify whether any of the transfers described above occur by reviewing the section of this document related to details on the processing of Personal Data or by requesting information from the Data Controller by contacting them through the provided contact details.

Duration of Processing

The service provider entity processes the personal data collected for the time necessary to enable the use of the requested service and in any case, no longer than 12 months from the cessation of its use.

Rights of the Data Subject

Data subjects have the right to request access to personal data, rectification or deletion of data, limitation of processing, or to object to processing as provided in Articles 15 and following of the Regulation. The request must be submitted by contacting the Data Protection Officer at the contact details provided above.
Data subjects also have the right to lodge a complaint with the Data Protection Authority (https://garanteprivacy.it) or take appropriate legal action (Articles 77 and 79 of the Regulation).

Updates

This notice is subject to updates in accordance with national and EU regulations. It is recommended to consult it periodically. In case of failure to accept the changes made to this notice, the user can request the deletion of their personal data from the Data Controller.
Unless otherwise specified, the privacy policy published on the site continues to apply to the processing of personal data collected until its replacement.

Application Notes:

This privacy policy template for services aims to be a "Template" containing key requirements common to all services offered by Elixir-IT to ensure compliance with current regulations. The privacy policies for services are mandatory.

- Each service provider entity can personalize the privacy policies by including the identification and reference data of the Data Protection Officer and the entity itself.
- Each service provider customizes it according to the services offered.
- Each service provider is required to include their own logo (in addition to the Elixir-IT logo).
- These policies must be signed together with the ToU and AUP for service access and referenced in any contracts/agreements governing access to the services.