TEMPLATE - DO NOT EDIT DIRECTLY

Data Processor Agreement

for depositing human genetic and phenotypic data for controlled access data archival and retrieval purposes in the Federated EGA Portugal service

Pursuant to the Regulation (EU) 2016/679 (the General Data Protection Regulation) and other applicable Portuguese laws, the following agreement is entered into

between

INSTITUTO _____, legal entity incorporated under the Portuguese law, with the registry number _____[1], PIC number (_____)[2], set up in _____, Portugal, as Data Controller

and

ASSOCIAÇÃO BIP4DAB (BioData.pt), legal entity incorporated under the Portuguese law, with the registry number 516416120, PIC number 889852005, set up in Oeiras, Portugal, as Data Processor

[1] NIF – Portuguese VAT number

[2] Participant Identification Code (PIC) is a 9-digit number that serves as a unique identifier for legal entities participating in European funding programs. (If applicable)

Clause 1. Purpose of the agreement

The purpose of the agreement is to regulate the rights and obligations of the Parties under the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereafter GDPR) and other applicable Portuguese personal data legislation, including, but not limited to: the Law n. 58/2019, of 8 August, that ensures the implementation, in the national legal order of the GDPR; the Law n. 21/2014, of 16 April on Medical Research (hereafter LMR); the Law n. 12/2005, of 26 January, on personal genetic data and health data, as well as the regulation thereof made by Decree-Law n. 131/2014, of 29 August.

Federated EGA Portugal (hereafter referred to as FEGA Portugal) is a service for archiving sensitive genome and phenotype data, as part of the distributed European network of interlinked services to provide FAIR[3] controlled access for such sensitive human data[4]. The data are accessible and distributed under controlled access policy, whereby access decisions reside in the Data Controller for each dataset, and covered by a Data Access Agreement (DAA), defining the terms and conditions of the use of a specified dataset.

The FEGA Portugal service is implemented in OpenStack and, when applicable, in cooperation with Sub-processors as specified in the attachment to this agreement (Annex III). All archived data in FEGA Portugal are stored encrypted inside a dedicated project for this service. BioData.pt is the legal entity responsible for operating the FEGA Portugal service.

Special categories of personal data will be processed, including data revealing ethnic origin data, genetic data and data concerning health. The agreement is intended to ensure that the personal data are not processed illegally, wrongfully, or processed in ways that result in unauthorised access, alteration, erasure, damage, loss, or unavailability.

The agreement governs the Data Processor's processing of personal data on behalf of the Data Controller, including collection, registration, structuring, retrieval, compilation, storage, disclosure, erasure, or combinations of these, in connection with the use of/processing in the FEGA Portugal service.

Clause 2. Definitions

For the purposes of this Agreement:

'Provider' person from whom the biological material is subject to the sequencing instrument to come off in the format of digital information.

'Data subject' means a natural person as defined in clause 5.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier.

'**Associated data'** means phenotypic and health data associated with genetic data of any provider, alive or deceived.

'Forbidden personal data' means any information that can directly identify a provider, including but not limited to name, addresses, social number or national health number.

[3] https://www.go-fair.org/
[4] https://ega-archive.org/

'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal or deoxyribonucleic acid (DNA) analysis.
'Genomic data/information' means information based on an individual's genetic data, such as a sequence of DNA or the results of genetic testing as well as all the data embedded in the dataset(s), i.e, files generated by a sequencing instrument of genetic material and their respective digital processing, i.e, sequencing files, including but not limited to sequencing reads, DNA libraries, and genomic sequence variations (VCF files).
'Dataset' means files with genetic information generated by a sequencing instrument of genetic material and their respective digital processing, i.e, sequencing files, including but not limited to sequencing reads, DNA libraries, and genomic sequence variations (VCF files).
'**Data processing'** means any operation performed on personal data, including the collection, sequencing, encoding, storage, alteration, retrieval, making available or destruction of such data.
'**Data processor'** means BIP4DAB (BioData.pt) and any person responsible for this entity, alone or together processing data on behalf of the data controller.
'**Data controller'** means Instituto de Medicina Molecular João Lobo Antunes, having decision-making power regarding the persons authorised by it to submit personal data into FEGA, whom will be listed as authorised persons in the "FEGA Submission Account – Authorised Users", which shall be updated and communicated to the processor whenever there is an addition or withdrawal of access permissions.
'**FEGA Submission Account – Authorised Users'** means a dynamic list, provided by the controller to the processor, of people to whom the Processor can provide credentials to use FEGA.
'Data submitters' means any of the authorised users of the Controller's FEGA account.
'**Data requester'** means an individual or a legal entity or similar body whom/which place a request of access with FEGA.
'DAC' means Data and Assessment Committee of each data submission, which approve/reject requests to access datasets.
'**Recipient'** means person or entity to whom/which genetic data and/or associated personal health data are disclosed or made available upon DAC's approval;
'GDPR' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
'Declaration of Helsinki' means WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects, according to its last amendment.
'Declaration of Taipe' means WMA Declaration of Taipei in Ethical Considerations Regarding Health Databases and Biobanks.
'**Pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
'Anonymization' means the technique to render information anonymous in such a manner that the data subject is not or no longer identifiable, *i.e.*, samples can neither directly nor indirectly, with reasonably means according to recital 26 of the General Data Protection Regulation (EU) 2016/679, be linked to the sample donor.

Clause 3. Limiting clause

The purpose of the Data Processor's processing of personal data governed by this agreement is to pre-process and safely archive the data in encrypted form within FEGA Portugal on behalf of the Data Controller, and when instructed by the Data Controller, to re-encrypt the data and provide access to safe download functionality to requesters that are approved by the DAC.

The FEGA Portugal helpdesk will provide advice to data submitters on which metadata to include in a submission, but **the Data Controller is solely and fully responsible for deciding which metadata per subject to include in the dataset**. Metadata are here considered being of two types: 1) Descriptive summary level data on experiments and study level to be made publicly available, three variables that may be included are phenotype category, control/case, and sex; and 2) Individual, per subject, level phenotype data that may be of different types including health information and are considered part of the sensitive data to be archived. Published descriptions of a dataset made available publicly (without controlled access) in the FEGA portal, will not be allowed to include information that, directly or indirectly, can identify individuals in the data set.

For further details on categories of data processing and permitted data processing tasks, please refer to Annex I.

For the datasets deposited in FEGA Portugal, the Data Controller has established a Data Access Committee (DAC) that will be the contact point for processing requests for access to their deposited data in FEGA Portugal.

The Data Processor may not transfer personal data covered by this agreement to partners or other third parties without the prior approval of the Data Controller through the DAC.

Clause 4. Instructions

The Data Processor will follow the written and documented instructions of the Data Controller for the processing of personal data in FEGA Portugal.

The Data Controller and the Data Processor are both obliged to comply with all obligations under the applicable Portuguese personal data legislation governing the use of FEGA Portugal for the processing of personal data.

The Data Processor is obliged to notify the Data Controller if it receives instructions from the Data Controller that conflict with the provisions of the applicable Portuguese personal data legislation.

Data Controller undertakes to use the FEGA Portugal services only as they are authorised in connection with their ongoing research / clinical activities. This is also related to the principle of data minimization regarding access to and use of personal data. In particular, the Data Controller must be able to document the legal basis to share data from FEGA Portugal to requesters the controller approves for download access, in order to facilitate further data processing. It is thus the responsibility of the Data Controller to organise and maintain any agreements needed for such further data processing. All communication regarding this required documentation to FEGA Portugal shall be in accordance with instructions from the controller, administratively organised through DAC. Data Controller, through DAC, undertakes to set as mandatory requirement, for any requester, a written application form that must include information about the purposes of the institution to which the applicant belongs, the types of research to be carried out, those responsible, its potential risks and benefits, the conditions and duration of storage, the measures taken to guarantee the privacy and

confidentiality of information and prediction regarding the possibility of communicating or not the results obtained with this material.

Clause 5. Types of information and data subjects

The Data Processor processes the following personal data on behalf of the Data Controller:

a) Genetic data, that may include: reads, libraries, and genomic variant files.
b) FEGA submission ID.

The personal data apply to the following data subjects:

a) Providers who have consented to dispose of biological material to extract genetic data, which sequencing was allowed, as well as sharing for health research purposes. These individuals are research subjects in a study developed by a research lab of the Controller.

b) Data submitters - the Data Processor will in addition register and store information associated with the use of the service by data submitters. The current version of the Terms of Service (ToS) and Privacy Policy (PP) at signing is included in Annex II of this Data Processing Agreement. These may be updated and the most up to date version of the ToS and PP are available on the FEGA Portugal website[5], all users will be notified prior to any change for FEGA Portugal ToS and PP.

The lawfulness of the processing according to the data protection legislation:

Lawful basis for processing health and genetic information is informed consent, that is based on a free, specific, informed and explicit manifestation of will, through which the data subject accepts, by means of a declaration or unequivocal positive act. According to the Portuguese law, consent may cover several areas of research, provided that ethical standards recognized by the scientific community are respected. However, data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose. The extension of the informed consent must be taken into account by the DAC when assessing the data request.

Clause 6. Data Controller's responsibility

The Data Controller is responsible for ensuring that Personal Data embedded in datasets and transmitted to the Data Processor are pseudonymised and encrypted in transit and at rest, when applicable.

Data Controller is responsible at each time:
- to demonstrate the existence of Data subject's informed consent for participation in the research project;

[5] https://fegaportugal.biodata.pt/

- to demonstrate the existence of Data subject's informed consent for the processing of personal data, or any other suitable legal basis for processing Personal Data;
- to obtain appropriate ethical or other approvals for processing Personal Data embedded in the submitted datasets;
- to comply with and to be able to demonstrate compliance with applicable Data Protection laws;
- to control the distribution of Personal Data.

Clause 7. Satisfactory data security

The Data Processor will implement appropriate technical, physical, and organisational safety measures to safeguard the personal data covered by this agreement from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability. The archived data is further stored encrypted for additional security. These measures will not be less protective than those laid down in the Portuguese law-decree nº65/2021, of 30th July, which regulates the law nº46/2018, of 13th August, which jointly constitute the legal Portuguese framework applicable to cyberspace security, or any other legislation which may affect the above-mentioned provisions

The Data Processor will document its own security organisation, guidelines and routines for security, risk assessments and established technical, physical or organisational security measures. The documentation will be made available to the Data Controller on request.

The Data Processor will establish continuity and contingency plans for effective handling of serious security incidents. The documentation will be made available to the Data Controller on request.

The Data Controller shall keep confidential any security documentation which the Data Processor makes available to the controller.

Residual risk management:

Controller's template for data access agreements between a Data Access Committee and a Data Requester, should include a paragraph on the risk of re-identification of individuals as follows:

> "*The Recipient agrees not to attempt to re-identify any individuals. The recipient further agrees to not link or combine these Data with other information or archived data available in a way that could re-identify the Provider, even if access to that data has been formally granted to the Recipient or is freely available without restriction. Additionally, The Recipient (as data processor) undertakes to use the data to the solely authorized purpose and to cooperate with the Data Controller, regarding the exercise of data subject rights, moreover commits to the Data Controller to send immediate notification of any data breach. In any case, the recipient is prohibited from using the information in a way that violates GDPR or the Declaration of Helsinki or the Declaration of Taipei*"

Clause 8. Confidentiality

Only employees of the Data Processor, who need to access personal data that is processed on

behalf of the Data Controller to operate the FEGA Portugal services, may be granted such access. The Data Processor is required to document guidelines and routines for control of access. The documentation will be made available to the Data Controller on request.

Employees of the Data Processor have a duty of confidentiality in respect of documentation and personal data, including but not limited to genetic data and health data, to which they gain access in accordance with this agreement. This provision also applies after termination of the agreement. The duty of confidentiality includes employees of any sub-processors, if applicable, and third parties who perform maintenance (or similar tasks) on systems, equipment, networks or buildings that the Data Processor uses to provide the service.

The Data Controller shall provide equivalent access control and have equivalent duty of confidentiality concerning all documentation made available by the Data Processor in accordance with this agreement.

Portuguese legislation defines the scope of the duty of confidentiality for employees of the Data Controller, the Data Processor, any sub-processors, if applicable, and third parties.

Clause 9. Security Breach Notification

The Data Processor shall notify the Data Controller without undue delay, and in any event within less than two business days, if personal data processed on behalf of the controller is exposed to a breach of security.

The Data Processor's notification should, at minimum, include the information as provided in article 33/3 of the GDPR, namely information that describes the security breach, which registered subject is affected by the breach, what personal data are affected by the breach, what immediate measures are implemented to address the breach and what preventive measures may have been established to avoid similar incidents in the future.

The Data Controller is responsible for ensuring that the data subjects and the Portuguese Data Protection Authority are notified when required.

Clause 10. Transfer to countries outside the EU/EEA

The Data Processor will never carry out any transfers of personal data stored in FEGA Portugal to countries outside of EU/EEA, except as specified below.

The Data Controller may authorise access to data in FEGA Portugal to non-EU/EEA citizens, provided that the provisions laid down in Chapter 5 of the GDPR are applied to ensure that the level of protection afforded to natural persons is guaranteed. Upon approval, the dataset will be made available for the requester in encrypted format to be further processed according to the conditions as agreed with the Data Controller.

- It is a prerequisite assumption from FEGA Portugal that the Data Controller has the legal mandate to authorise such data access, transfer and processing.
- The Data Controller is responsible for establishing separate agreements as required for each recipient of their dataset that is being granted access to from FEGA Portugal.
- If the agreements between the Data Controller and the data requester allows the dataset to be transferred to and stored in countries outside of EU/EEA, this is permitted directly from the FEGA Portugal service.

Clause 11. Safety audits and impact assessments

The Data Processor will regularly implement security audits of its own work with safeguarding of personal data from unauthorised or unlawful access, alteration, erasure, damage, loss, or unavailability.

Security audits will include the Data Processor's security goals and security strategy, security organisation, guidelines, and routines for security work, established technical, physical, and organisational safeguards and the work of data security at sub-processors to this agreement. It will also include routines for warning the Data Controller in the event of security breaches, and routines for testing of emergency and continuity plans.

The Data Processor will document the security audits. The Data Controller will be granted access to the audit reports on request.

If an independent third-party conducts security audits at the Data Processor, the Data Controller will be informed of which auditor is being used and be given access to the summaries of the audit reports on request.

Additionally, the Data Processor will assist the Data Controller in ensuring compliance with the obligation to carry out a Data Protection Impact Assessment when required by applicable Portuguese laws.

Clause 12. Assistance to the Data Controller Regarding Data Subjects Actions

The Data Controller has the control to define the settings of its notifications from the DAC Portal, regarding the actions it must take, namely access requests. The Data Processor will not notify the Data Controller upon each data access request and shall not respond to the request itself .

The Data Processor will assist the Data Controller in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights according to the GDPR, taking into account the nature of processing as defined in this Agreement.

In the event of a request for the erasure of personal data, the Data Processor undertakes, upon receipt of an order from the Data Controller, to permanently erase the data requested.

The Data Controller undertakes to give instructions for the erasure only after the request has been under review and validation by the Data Controller.

Clause 13. Use of Sub-processors

The Data Controller authorises the Data Processor to process data, including personal data, engaging the Sub-processors listed in the Annex III to this Agreement. The Data Processor shall inform the Data Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Data Controller sufficient time to be able to object to such changes.

Clause 14. Return and erasure

Upon termination of this agreement, the Data Processor is obliged to return and erase any personal data, including but not limited to genomic data sets, which are processed on behalf of the Data Controller under this agreement. Both parties shall agree how the return of the personal data will take place, including the format to be used. Both parties are mutually responsible to initiate communication on the matter of return and erasure, in due time to allow the practical execution of return and erasure within the time frame of the legal approval for the deposited data set.

Erasure is to be carried out by the Data Processor within 30 days after the termination of the agreement for any reason. Backup of personal data will be automatically erased no later than 90 days after the original data is erased. The backup data will only be available to a few system administrators in this period.

The Data Processor will execute erasure of the data upon to Data Controller order for erasure, using a compliant Data Erasure Software to Permanently Erase or anonymize Data from Storage Devices, using as minimum level of security a purge method after which will notify Data Controller, if applicable. An Example of “Certificate of Sanitization” is enclosed in Appendix IV.

The Data Controller will be notified before and when this visibility change is executed. This can be reversed by documenting a legal basis for the extended approval period. The Data Controller has 15 days to inform, by writing its intention to extend the mentioned period. If no extension documentation is provided within 30 days, the above rules of erasure will be executed as specified above.

Erasure of personal data such as user profiles and usage data of FEGA Portugal web portal and services, is specified in the ToS and PP of these services, and is not included in this agreement.

Similarly, erasure of personal data such as user profiles and usage data of other services in the Federated EGA network, is governed by the ToS and PP documents accepted by the users for these services and must be enforced by these service providers as Data Processors.

Clause 15. Breach of the Agreement

In case of breach of the terms of this agreement caused by errors or omissions on the part of the Data Processor, the Data Controller may cancel the agreement with immediate effect. The Data Processor will continue to be obliged to return and erase personal data processed on behalf of the Data Controller.

The Data Controller may require compensation for financial loss suffered by the Data Controller because of errors or omissions on the part of the Data Processor, including breach of the terms of this agreement.

The Data Processor shall be liable for the damage caused by processing, including for the payment of penalties ruled in Chapter 8 of the GDPR, where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Clause 16. Duration of the Agreement

This agreement applies from the moment that the Data Processor starts processing personal data on behalf of the Data Controller, where the maximum duration is set in the approval for

the Data Controller to store data in FEGA Portugal.

This agreement shall remain in force for as long as there is a need to carry out any processing operation on personal data. This agreement can only be terminated after the return and complete deletion of all processed personal data, including any back-ups.

Clause 17. Contacts

Contact person at the Data Processor for any questions related to this agreement is: BIP4DAB Executive Director, email: direcao_executiva@biodata.pt, telephone: +351 931 814 814

Contact person at the Data Controller for any questions related to this agreement is: _____, email: _____, telephone: _____

17. Choice of Law and Resolution of Disputes

The Parties' rights and obligations under this agreement are determined in full by Portuguese law. Any disputes arising out of this Agreement shall be first sought to be resolved through negotiations. If unsuccessful, the matter shall be resolved through the Portuguese legal system.

This agreement is in 2 – two copies, one to each of the parties.

Place and date

……..	……
(signature)	(signature)
Data Controller (XXXX)	Data Processor (BioData.pt)

Annex **I - Categories of data subjects, categories of data processed, lawfulness of the processing, permitted data processing tasks**

Data subjects, as defined in Clause 2. 'Definitions for the purposes of this Agreement', to whom belong the personal data processed by the Data Processor:

- Data Submitters
- Providers

Categories of data as defined in the GDPR, Article 4(2), processed by the Data Processor:

- Regarding Data Submitters - authorised users listed on the 'Authorised_submitters_list iMM'
    - Name
    - institutional email

- Regarding Providers
    - Genetic data, including genomic data as defined in clause 2 of this agreement
    - Health data
    - Phenotype

Lawfulness of the processing, as foreseen in the GDPR and other applicable law

- Regarding Data Submitters – performance of a contract to which the data subject is party – article 6/1, b) GDPR

- Regarding Providers – Informed Consent - article 6/1,a) and article 9/2, a) or j) GDPR. As foreseen in article 9/4 GDPR, Portugal has further conditions, including limitations, with regard to the processing of genetic and health data, specifically concerning the informed consent, which Data Controller grants to has been duly complied.

Categories of data processing tasks as defined in the GDPR, Article 4(2), performed by the Data Processor:

- Storage
- Structuring
- Making data available
- Erasure or destruction

FEGA Portugal will, on behalf of the Data Controller, pre-process and safely archive the data in encrypted form within our archival service. When instructed by the Data Controller, FEGA Portugal staff will re-encrypt the data and provide access to safe download functionality to requesters that are approved by the Data Controller.

To improve FAIR data quality of a deposited data set, the FEGA Portugal service team may continuously update the formats of data files to follow community standards. The original data files will remain in the dataset, and updated data files in new formats will be added as a supplement. The Data Controller will be informed in the event of such an update to a data set and given the opportunity to quality control the new data files.

Other standard data processing operations in FEGA Portugal include re-encryption of data

when rotating encryption keys for security reasons, performing data integrity checks and computation of non-identifiable quality control summary statistics.

Personal data that the Data Processor processes on behalf of the Data Controller may not be processed for any other purpose than stated above, without the prior written approval of the Data Controller.

Annex II - FEGA Portugal Terms of Service and Privacy Policy

Current versions of FEGA Portugal services Terms of Service and Privacy Policy are included for reference, both last updated 25/06/2024.

Terms of Service

Definitions:

The Service consists of the storage of data under BioData.pt's FEGA Node, in Portugal.

Accounts and Pricing

In order to use The Service you must have an EGA Account that must be obtained from the ega-archive.org website. Your registration data is primarily used so you may persistently store data on The Service. The operators of The Service will not provide your registration data to any third party unless required to do so by law.

The Service depends on heavy storage capacity, therefore, its usage requires a fee that will mostly depend on the data volume of the project or submission. Upon submission evaluation by FEGA Portugal, a quota will be attributed to the user.

Your access to The Service is provided under the condition that you abide by the quota on data storage, or any other limitations placed on The Service. Attempts to subvert these limits by using multiple accounts or through any other method may result in termination of all associated accounts.

Use of Service

Data transfer is automatically encrypted by using the underlying SFTP protocol. Data storage is encrypted with Crypt4GH encryption format. If there are restrictions on the way your research data can be stored and used, please consult your local institutional review board or the project principal investigator before uploading it to any public site, including The Service. Your access to the service may be revoked at any time for reasons deemed necessary by the operators of The Service. You acknowledge that you are responsible for compliance of all of your data processing activities carried out on The Service with applicable laws and regulations of Portugal, the European Union as well as any laws or regulations of other legislations or any other restrictions that might be applicable due to the provenance, intended use, legal ownership of or any licensing or other legal restrictions imposed on the data being processed.

Disclaimer

The Service is provided to you on an "AS IS" BASIS and WITHOUT WARRANTY, either express or implied, including, without limitation, the warranties of non-infringement, merchantability, or fitness for a particular purpose. THE ENTIRE RISK AS TO THE QUALITY OF THE SERVICE IS WITH YOU. This DISCLAIMER OF WARRANTY constitutes an essential part of this service agreement.

TEMPLATE - DO NOT EDIT DIRECTLY

Privacy Policy

Definitions:

The Service consists of the storage of data under BioData.pt's FEGA Node, in Portugal.

This privacy policy will explain how The Service uses the personal data we collect from you when you use our website.

Topics:

- What data do we collect?
- How do we collect your data?
- How will we use your data?
- How do we store your data?
- What are your data protection rights?
- What are cookies?
- How do we use cookies?
- What types of cookies do we use?
- How to manage your cookies
- Privacy policies of other websites
- Changes to our privacy policy
- How to contact us
- How to contact the appropriate authorities

What data do we collect?

The Service collects the following data:

- EGA username
- Information about your data uploads to The Service or data retrievals from The Service
    - Including public keys provided by you for encryption purposes

How do we collect your data?

We collect data and process data in the form of server logs when you:

- Connect to our servers via SFTP to upload data.
- Perform a dataset submission to the archive.
- Perform a dataset retrieval from the archive after access approval by the respective Data Access Committee.

We collect data and process data when you:

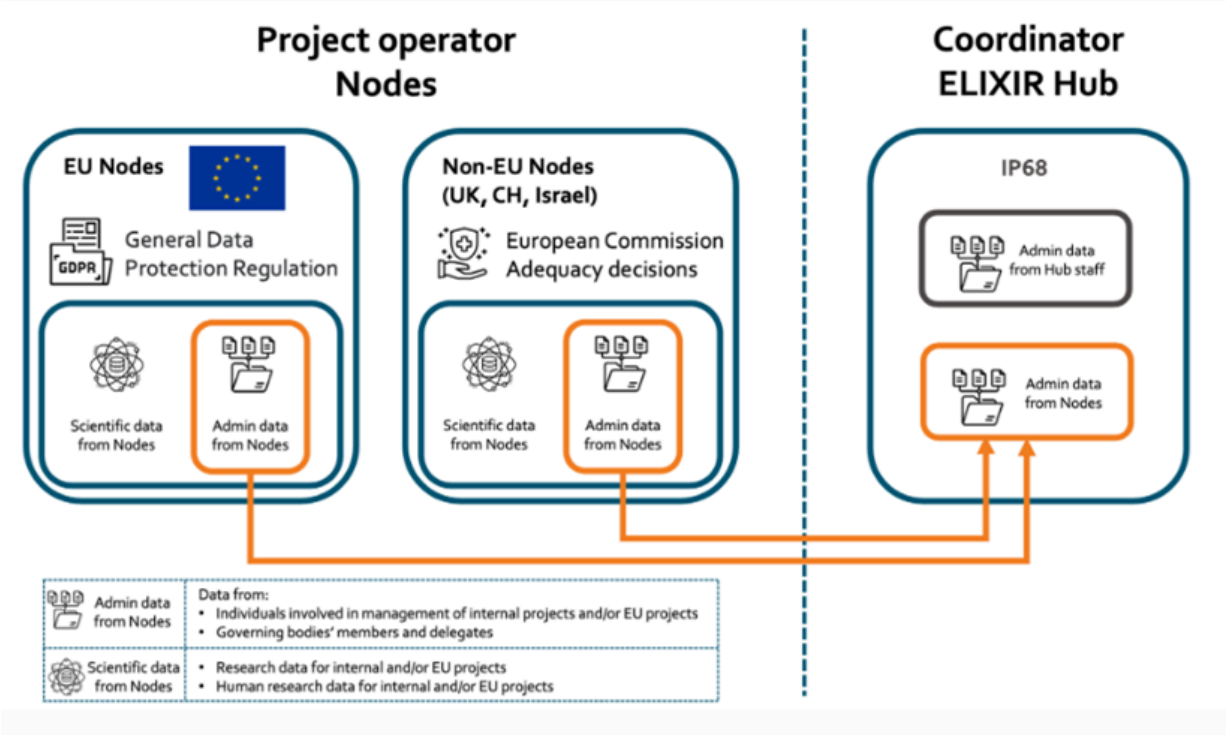
- Voluntarily complete a customer survey or provide feedback on any of our message boards or via email.

How will we use your data?

The Service collects your data so that we can:

- Facilitate the authentication and authorization to The Service. Since the authentication and authorization to The Service is based on an EGA account.
- Keep track of which submission was performed by which user.
- Security and audit purposes to track all data transfers of files under controlled access regime due to their sensitive content (human genome phenome information).

Any transferring of personal data to EMBL will rely on the derogation of 'important reasons of public interest' under Article 49(1)(d) of the GDPR and will be processed according to the adequacy decision Policy No 68 on General Data Protection, which can be accessed here https://www.embl.org/documents/wp-content/uploads/2021/07/IP68-Data-Protection-EN-18052018.pdf



How do we store your data?

Data is stored in two ways:

1. PostgresSQL database, which include:
    a. Information on FEGA data access management, *i.e.* who owns and has access to the data.
    b. User data: username, full name, institution, email.
2. Server Logs, which include:
    a. Changes to FEGA data access privileges.
    b. Session information, collected every time you connect to our servers.

What are your data protection rights?

The Service would like to make sure you are fully aware of all your data protection rights. Every user of The Service is entitled to the following:

The right to information (GDPR Art. 13 and 14) - The Service shall provide you with information on the processing of your personal data at the time when your personal data is collected.

The right to access (GDPR Art. 15) – You have the right to request The Service for copies of your personal data and information of the data processing. We may charge you a small fee for this service.

The right to rectification (GDPR Art. 16) – You have the right to request that The Service correct any information you believe is inaccurate. You also have the right to request The Service to complete the information you believe is incomplete.

The right to erasure (GDPR Art. 17) – You have the right to request that The Service erase your personal data, under certain conditions.

The right to restriction of processing (GDPR Art. 18) – You have the right to request that The Service restrict the processing of your personal data, under certain conditions.

The right to data portability (GDPR Art. 20)– You have the right to request that The Service transfer the data that we have collected to another organisation, or directly to you, under certain conditions.

The right to object to processing (GDPR Art. 21)– You have the right to object to The Service's processing of your personal data, under certain conditions.

If you make a request, we have one month to respond to you. If you would like to exercise any of these rights, please contact us.

Cookies

Cookies are text files placed **on your computer** to collect standard Internet log information and visitor behaviour information. **When you visit our website fegaportugal.biodata.pt**, we may collect information from you automatically through cookies or similar technology.

For further information, visit https://allaboutcookies.org.

How do we use cookies?

- We use cookies from third-party partner Google for analytics services to improve your experience on our website.

What types of cookies do we use?

- Analytics – They collect data for statistical purposes on how visitors use a website, they don't contain personal information such as names and email addresses and are used to help us understand how you use and how we can improve your experience on our website.

How to manage cookies

You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.

Privacy policies of other websites

The Service website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Changes to our privacy policy

The Service keeps its privacy policy under regular review and places any updates on this web page.

How to contact us

If you have any questions about The Service's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us.

Email us at: fegaportugal@biodata.pt

How to contact the appropriate authority

Should you wish to report a complaint or if you feel that The Service has not addressed your concern in a satisfactory manner, you may contact the BioData.pt Data Protection Officer.

Email: dpo@biodata.pt

Should you wish to contact the national supervisory authority because you feel that you data has not been processed in a lawful manner, you should fill a complaint in www.cnpd.pt

Annex III. Sub-processors

Entity	Location	Processing	Transfers
FCCN/FCT	(…), Lisbon, Portugal	Hosting	Not applicable

Appendix IV – Example of Certificate of Sanitization

CERTIFICATE OF SANITIZATION		
PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITIZATION DETAILS		
Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct		
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other:		
Method Details:		
Tool Used *(include version)*:		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)*		
Details:		
SIGNATURE		
I attest that the information provided on this statement is accurate to the best of my knowledge.		
Signature:		Date:
VALIDATION		
Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date: