
Internal Policy No. 68
on General Data Protection

First published: 18 May 2018

Revised: 25 February 2025

Preface

- (1) This Internal Policy establishes personal data safeguards for natural persons, whether Members of Personnel, research participants or other. It assures EMBL processes and protects personal data in accordance with generally accepted standards. It lays down substantive principles, such as transparency and accountability, formal requirements such as record-keeping and information to data subjects, and eases the restriction of the processing of personal data for scientific research or their transfer to EMBL collaborators outside the EU/EEA. It aims to help relevant staff at EMBL that handle data or whose personal data are handled. It moreover establishes a data protection officer and a supervisory authority (Data Protection Committee).
- (2) The protection of privacy is a fundamental right. At the level of public international law, it was firstly generally formulated in Article 12 of the Universal Declaration of Human Rights, adopted by the UN General Assembly in 1948, and thereafter in Article 8 of the European Convention on Human Rights of the Council of Europe of 1950 and Article 17 of the International Covenant on Civil and Political Rights, adopted by the UN General Assembly in 1966. At European supranational level, data protection is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.
- (3) A more extensive form of general regulation under public international law is the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) and its Additional Protocol of 2001 on supervisory authorities and transborder data flows (ETS No 181). In the European Union, detailed general regulation has taken the form of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). These legal acts incorporate the principles of European data protection law.
- (4) EMBL itself has, at Section 1 3.07 of the EMBL Staff Rules, undertaken to protect the personal data of its Members of Personnel. Moreover, in EMBL Internal Policy No. 53 the protection of data derived from human biological material and processed for scientific research is regulated from a bioethics perspective, and EMBL Internal Policy No. 54 establishes a framework for using EMBL IT facilities in an acceptable way.
- (5) At the same time, freedom of scientific research is declared a fundamental right in Article 27(1) of the Universal Declaration of Human Rights; Article 15(3) of the International Covenant on Economic, Social and Cultural Rights, adopted by the United Nations General Assembly in 1966; Article 12(b) of the Universal Declaration on the Human Genome and Human Rights, issued by UNESCO in 1997; Article 15 of the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (Oviedo Convention) of the Council of Europe of 1997; Article 1(a) of the International Declaration on Human Genetic Data, issued by UNESCO in 2003; and in Article 13 of the Charter of Fundamental Rights of the European Union. Moreover, Article 179(2) of the Treaty on the Functioning of the European Union encourages research centres and universities in their research activities of high quality and supports their free cross-border cooperation.

- (6) As an intergovernmental organisation, EMBL is subject to public international law, entrusted with a number of privileges and immunities necessary for its functions. Accordingly, it has the power to self-regulate data protection. Such self-regulation is necessary to take account of EMBL's status as an intergovernmental organisation, and its focus on scientific research beyond national borders. The protections afforded to EMBL by a number of treaties and general principles of public international law regarding the inviolability of its archives and premises, as well as its immunity from jurisdiction and execution, are particularly well-suited to prevent interference in fundamental rights of data subjects in the areas of national security or law enforcement.
- (7) To maintain compatibility with collaborators, funders, member states and other stakeholders, both in Europe and elsewhere, the system designed by way of self-regulation should be in line with public international law and existing data protection principles so as to enable parties subject to the GDPR to transfer data to EMBL.
- (8) Self-regulation should take the form of an Internal Policy on general data protection. The Director General, after appropriate internal consultation and revision, and having regard to the Agreement Establishing the European Molecular Biology Laboratory, in particular Articles II, VII(2) and XI thereof, and to the Universal Declaration of Human Rights, in particular Article 12 thereof, has therefore issued this Internal Policy No. 68 to apply to all EMBL sites.

Chapter 1: General provisions

Article 1 – Purpose

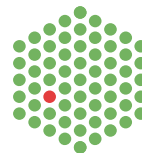
This Internal Policy ensures the protection of the fundamental rights and freedoms of individuals in relation to the processing of their personal data by EMBL and ensures the free flow of such data among scientific researchers.

Article 2 – Scope

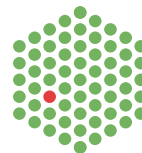
1. This Internal Policy regulates the processing of personal data by EMBL as a legal entity, whether EMBL has the role of a controller or a processor.
2. This internal Policy applies to all EMBL Members of Personnel.
3. For the sake of clarity, this Policy does not apply to data that is rendered anonymous in such an irreversible way that data subjects cannot be identified from the data.
4. Process owners shall be responsible for ensuring that EMBL, as the data controller, complies with its obligations hereunder.

Article 3 – Definitions

For the purposes of this Internal Policy:



- (1) “personal data” means any information relating to an identified or identifiable individual (‘data subject’);
- (2) “data processing” means any operation which is performed on personal data, including the collection, storage, alteration, retrieval, making available or destruction of such data;
- (3) “data controller” means EMBL, the entity that determines alone the purpose and means of personal data processing;
- (4) “joint data controller” means the entities, including EMBL, that jointly determine the purpose and means of personal data processing;
- (5) “consent” means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to processing of personal data relating to him or her;
- (6) “process owner”, regardless of the different terminology used across EMBL sites, means the person who has the responsibility and authority for designing, implementing and managing a particular process and exercises decision making power regarding data processing, including determination of the purposes and means of processing, and who is responsible for the design and implementation of technical and organisational measures in that particular process;
- (7) “personal data breach” means any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes;
- (8) “health-related data” means personal data relating to the physical or mental health of the data subjects;
- (9) “scientific research data” means any personal data created, generated, received and/ or processed in the context of scientific research projects;
- (10) “recipient” means an individual or a legal entity or similar body to whom data are disclosed or made available;
- (11) “data processor” means an individual or a legal entity or similar body which processes personal data on behalf of the data controller;
- (12) “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;
- (13) “data protection officer” means the officer established in Article 19;
- (14) “data protection strategy board” means the board established in Article 22;
- (15) “data protection committee” means the committee established in Article 23.



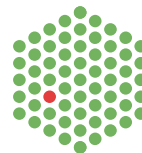
Chapter 2: Principles

Article 4 – Principles

1. Personal data shall be processed in line with this Internal Policy, interpreted in accordance with the principles of European data protection law.

Personal data shall be:

- (a) processed for specified and lawful purposes, and in a manner proportional to these purposes;
 - (b) processed lawfully, fairly and in a manner transparent to the data subject ("lawfulness, fairness and transparency"); the data subject shall be informed of the existence of the processing operation and its purposes, and the process owner shall provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed;
 - (c) collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with these purposes ("purpose limitation");
 - (d) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
 - (e) accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified without delay ("accuracy");
 - (f) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were collected or for which they are further processed ("storage limitation");
 - (g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality"). Access to personal data shall only be granted in accordance with the need-to-know and least privilege principles.
2. Proportionality includes the following considerations:
 - (a) the volume and categories of personal data processed;
 - (b) the number and categories of data subjects; and
 - (c) the intensity, length in time and types of processing.
 3. It shall be for the data controller to comply with these principles and to be able to demonstrate such compliance. The process owner shall be responsible for the compliance with the principles ("accountability").



Article 5– Change of purpose

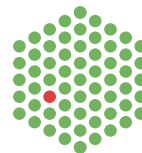
EMBL may process personal data for a different purpose, or for a different time period, than the purpose and period for which they have been originally collected if the new purpose or period is compatible with the original purpose and covered by a legal basis according to Article 6. Data subjects must be informed, individually by notification or collectively through publication, of the change of purpose or period unless the purpose of processing is historical research or archiving or statistics.

Article 6 - Legal basis of processing

1. EMBL may process personal data only insofar as necessary for any of the following:
 - (a) the achievement of the aims laid down in its establishing agreement of 1973;
 - (b) compliance with EMBL Council decisions and with any other rules applicable to such processing;
 - (c) the protection of its legitimate interests; or
 - (d) its day-to-day management, operation and functioning.
2. Where EMBL is processing data in the context of the ELIXIR Hub, paragraph 1(a) hereof shall also include the 'ELIXIR Consortium Agreement Establishing the European Life-Science Infrastructure for Biological Information (ELIXIR)' that entered into force on 12 January 2014, and paragraph 1(b) hereof shall also include the ELIXIR Board Decisions and any other rules applicable to ELIXIR Hub.
3. In other cases, EMBL may process personal data if data subjects have consented or are about to contract, or have contracted, with EMBL and it is necessary to process personal data to enter into or execute the contract.

Article 7 – Legal basis of processing in the context of employment

1. Pursuant to article 6 par. 1 lit. c EMBL may adopt *rules* to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of:
 - a) the recruitment, the performance of the contract of employment, management, planning and organisation of work, rights and benefits related to employment, and for the purpose of the termination of the employment relationship;
 - b) legal investigations when there is sufficient suspicion of misconduct;
 - c) equality and diversity in the workplace;
 - d) and health and safety at work.
2. EMBL ensures that those rules shall include suitable and specific measures to safeguard the data subject's fundamental rights, in particular in regard to the transparency of processing.



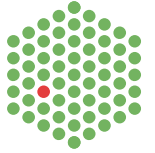
-
3. Where EMBL processes personal data of Members of Personnel on the basis of consent, in order to assess whether such consent is actually free and valid, the following factors shall be considered:
 - a) whether EMBL has complied with Article 14 hereof;
 - b) whether EMBL and the Members of Personnel pursue the same objective;
 - c) whether the processing involves a benefit or advantage for the Member of Personnel which is additional to any and all benefits that EMBL must provide to its Members of Personnel in accordance with the Staff Rules and Regulations, EMBL's obligations under applicable rules for international civil servants, and the provisions of the employment contract;
 - d) whether the Member of Personnel may withhold and/or withdraw said consent without affecting his or her employment status.

Article 8 – Derogation of processing for scientific research

1. No requirements under this Internal Policy shall apply to scientific research data, in cases where, and insofar as, such requirements are likely to render impossible or seriously impair the achievement of that purpose and on condition that the data controller provides appropriate safeguards, for example technical and organisational measures for data encryption, minimisation, pseudonymisation or anonymisation.
2. Where process-owner wishes to rely on the preceding paragraph:
 - (a) a data protection impact assessment in accordance with Article 11 shall be carried out, and submitted to the Data Protection Committee for review always without prejudice to any separate additional approval that may be required by the Bioethics Internal Advisory Committee; and
 - (b) the process-owner shall complete the record required in Article 12(1)(h).

Article 9 – Processing special categories of data

1. Data revealing political or philosophical or religious beliefs, genetic, racial or ethnic origin, trade union membership, sex life or sexual orientation (special categories of data) may be processed only where absolutely necessary for the achievement of EMBL's legitimate aims or with data subjects' consent.
2. Health related data and genetic data shall be processed only when necessary for the achievement of EMBL's legitimate aims or with data subjects' consent.
3. EMBL may only process special categories of data of its Members of Personnel subject to Article 6(1)(b) hereof.



Chapter 3: Duties of process owners

Article 10 – Privacy by design and privacy by default

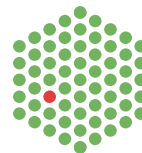
1. Each process owner shall cooperate with the DPO to ensure that technical and organisational measures are implemented at the earliest stages of design of the processing operations, in such a way that privacy and data protection principles are guaranteed right from the start ('data protection by design').
2. By default, each process owner shall ensure that personal data are processed with the highest privacy protection (short storage period, limited accessibility) so that by default personal data are not made accessible to an indefinite number of persons ('data protection by default').

Article 11 – Data Protection impact assessment

1. Where the processing of personal data is likely to present serious risks for the rights or freedoms of data subjects e.g., due to the type or amount of data or the number of data subjects or the purposes of the processing, and in the cases of Article 8, a process owner shall, in advance of the processing, carry out a data protection impact assessment and address any issues such assessment may reveal.
2. The process owner may seek the advice and assistance of the DPO during the preparation of the data protection impact assessment. The DPO shall review the finalised data protection impact assessment and may propose necessary changes.

Article 12 – Records and Register

1. Each process owner shall maintain a record of processing activities under its responsibility containing the following information:
 - (a) the name and contact details of the process owner, the data protection officer and, where applicable, the joint data controller(s);
 - (b) the purposes of the processing;
 - (c) a description of the categories of data subjects and of the categories of personal data;
 - (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in non-EEA ("European Economic Area") countries or international organisations;
 - (e) where applicable, transfers of personal data to a non-EEA country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in Article 18, the documentation of how the conditions for the transfer are satisfied;
 - (f) where possible, the envisaged time limits for erasure of the different categories of data;



-
- (g) where possible, a general description of the technical and organisational security measures required under Article 4(2) g);
 - (h) where a process owner wishes to rely on Article 8(1):
 - a rationale of why compliance with specific requirements is likely to render impossible or seriously impair the achievement of the purpose of the processing;
 - an outline of appropriate safeguards taken and their intended efficacy; and
 - a timeline for review to assess if the derogations established in Article 8(1) are still required.
2. Each data processor shall maintain a record of all categories of processing activities carried out on behalf of a process owner, containing:
- (a) the name and contact details of the data processor or data processors and of each process owner on behalf of which the processor is acting, and of the data protection officer;
 - (b) the categories of processing carried out on behalf of each process owner;
 - (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in Article 18, the documentation of how the conditions for the transfer are satisfied;
 - (d) where possible, a general description of the technical and organisational security measures referred to in Article 4(2)(g); and the information required by Article 12(1)(h). The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
3. Process owners and data processors shall submit their records to the data protection officer, who shall maintain them centrally in a register. That register shall be accessible to the Director General and shall be made accessible to the Data Protection Committee on request.

Article 13 – Processing of personal data by data processors

Where the process owner intends to instruct a data processor to process personal data on its behalf, the process owner shall use only data processors providing sufficient guarantees to implement appropriate technical, legal and organisational measures in such a manner that processing will meet the requirements of this Internal Policy and to ensure the protection of the rights of the data subject. Where the data processor is a third-party, the data processor shall be engaged only upon the conclusion of an appropriate data processing agreement.

Article 14 – EMBL’s Information duties towards data subjects

1. A process owner shall inform data subjects of:
- (a) the process owner’s identity and primary contact details;

- (b) the legal basis and the purposes of the intended processing;
- (c) the categories of personal data processed;
- (d) any recipients or categories of recipients of the personal data; and
- (e) instructions how to exercise the rights set out in Article 16;

as well as any necessary additional information in order to ensure fair and transparent processing.

2. Paragraph 1 shall not apply, where:
 - (a) the data subject already has the relevant information; or
 - (b) personal data have not been obtained from the data subject and the processing is expressly prescribed by rules or providing the information of paragraph 1 proves to be impossible or involves disproportionate effort in particular for processing for archiving purposes in the public interest, historical research purposes or statistical purposes.
3. Where vulnerable data subjects (including children) are involved, the information of paragraph 1 hereof must be provided in a manner and with the use of language that they understand.

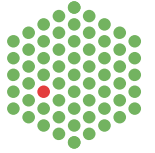
Article 15 – Personal data breach

1. The process owner shall report any personal data breach to the DPO immediately, upon becoming aware of the data breach.
2. The DPO shall monitor, advise and assist the process owner in case of personal data breaches.
3. In grave cases of personal data breach, the process owner supported by the DPO shall inform the Data Protection Committee. On assessment by the DPO or at the instructions of the Data Protection Committee, the process owner shall also inform the affected data subjects individually or, if that is impracticable, by publication.

Chapter 4: Rights of data subjects

Article 16 – Rights of the data subject

1. Every data subject shall have a right:
 - (a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of data (i.e., without any human intervention), without having his or her views taken into consideration;



-
- (b) to request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her; the communication in an intelligible form of the data processed; all available information on their origin, on the preservation period as well as any other information that the data controller is required to provide in order to ensure the transparency of processing in accordance with Article 14(1);
 - (c) to request knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;
 - (d) to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the data controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms; and
 - (e) to request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data, if these are being or have been processed contrary to the provisions of this Internal Policy.
2. Paragraphs 1(d) and (e) shall not apply where processing is necessary:
- (a) for compliance with a legal obligation which requires processing according to the rules to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
 - (b) for archiving purposes in the public interest, historical research purposes or statistical purposes in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - (c) for the establishment, exercise or defence of legal claims.

Chapter 5: Transfers

Article 17 – Transfer of personal data to recipients within EMBL

The transfer of personal data within EMBL shall not be restricted on the mere ground of the data being within EMBL or from one site to another. This provision shall not relieve the sender from complying with the principles laid down in Article 4 and requiring any form of data processing restriction from the recipient the data controller deems necessary.

Article 18 – Transfer to recipients outside EMBL

Any data controller or processor may transfer personal data to recipients outside EMBL on one of the following conditions:

- (1) the recipient is established in a country or in an international organisation which ensures an adequate level of data protection;
- (2) the recipient commits contractually to offer appropriate safeguards that provide a level of data protection at least equivalent with the level of protection offered hereunder;
- (3) the data subject has consented to such transfer; or
- (4) the transfer is needed for the conclusion or performance of a contract with the data subject, for important reasons of public interest, for legal claims or to protect the vital interests of a data subject.

Chapter 6: Data Protection Governance

Article 19 – Data protection officer

1. A data protection officer (DPO) shall be appointed by the Director General and be answerable only to him/her.
2. The DPO shall enjoy functional independence and shall neither seek nor accept instructions from anyone.
3. Without prejudice to the previous paragraph, the DPO, including his/ her staff may, strictly for administrative and organisational purposes, be part of another function supporting the role, such as Legal Services.
4. The DPO shall, where appropriate, make recommendations to the DG for changes to administrative issuances.
5. The DPO shall be provided with the staff, financial and other resources required for the performance of his/ her duties.
6. The DPO shall be bound by secrecy during and after the exercise of his/ her functions.

Article 20 – Duties of the data protection officer

1. The DPO shall monitor the application of this Internal Policy within EMBL.
2. The DPO shall, on request or on his/her own initiative, advise process owners on their rights and obligations, and data subjects on their rights. Such advice shall not be binding, but process owners must document the reasons for not complying with the DPO's advice and recommendations.
3. The DPO shall handle all requests by data subjects for the exercise of their rights, in accordance with Article 16 and any complaints in accordance with Article 25.
4. The DPO shall act as the contact point for the Data Protection Committee.
5. The DPO shall produce a yearly report for the Director General.
6. The DPO shall report to the Staff Association every six months on the state of data protection in staff-related processing activities. That report shall include any information on the workings of the Data Protection Committee

which the latter authorises the DPO to report to the Staff Association. The DPO shall moreover respond to questions of general concern which the Staff Association may at any time submit to him or her regarding such activities.

7. The DPO may, after consultation with the EMBL Standing Advisory Committee where required, propose sectoral guidance or standard operating procedures in areas of this Internal Policy requiring further formalisation to the Director General.
8. DPO will ensure that regular and mandatory programmes are conducted for all Members of Personnel as practicable and progressively as possible in all EMBL sites, to ensure awareness and compliance with this Internal Policy.

Article 21 – Obligation to provide information and assistance to the DPO

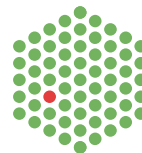
Process owners shall cooperate with the DPO by assisting him/her and making available any information needed to carry out his/her tasks. They shall, in particular, involve the DPO in the process of designing new information systems, so that measures of data protection are built in those systems from the start.

Article 22 – Data Protection Strategy Board (DPSB)

1. The Board stands as an Advisory Board in relation to the Data Protection Implementation Project and assists the DPO in fulfilling the objectives of the project. Together they are responsible for the successful delivery of the plan.
2. The DPSB shall adopt its terms of reference and rules of procedure.
3. The DPSB shall consist of four permanent members and a Chairperson appointed by the DPO. The permanent members shall represent IT, COO/ Legal and Science of EMBL.

Article 23 - Data Protection Committee (DPC)

1. A Committee is established to supervise the application of this Internal Policy.
2. The DPC shall consist of three members appointed by the Director General. Two appointments shall be external to EMBL, with demonstrable data protection expertise, and one appointment shall be internal to EMBL. No such appointment shall be for less than three years. Members of the DPC shall refrain from any act or activity which is incompatible with their functions and are required to excuse themselves from decision making in cases of potential conflicts of interest.
3. The DPC shall meet at least once a year.
4. Each member shall be entitled to one vote. Decisions shall be taken by majority.
5. The DPC shall adopt its rules of procedure.
6. The members of the DPC shall be subject to the obligation of confidentiality.



7. The DPC may ask any relevant EMBL officer and any external data protection expert for assistance or advice.
8. Every three years, the DPC shall submit a written report to the Director General.
9. The DPC shall act in complete independence and impartiality. It shall neither seek nor accept instructions. EMBL shall provide the DPC with sufficient resources.
10. Secretarial costs of the DPC shall be borne by the EMBL budget. The secretary of the DPC shall enjoy independence in the discharge of its function within the EMBL administration.

Article 24 – Powers of the Data Protection Committee

1. The DPC shall have preventive and corrective powers. In particular, it may:
 - (a) hear complaints from data subjects;
 - (b) access all files where personal data are processed;
 - (c) launch and conduct investigations;
 - (d) order process owners to restrict or discontinue processing; and
 - (e) recommend to the Director General that disciplinary proceedings against process owners be launched.
2. The DPC shall exercise its powers in proportion to the intensity of the infringement of this Internal Policy and mindful of the intergovernmental nature of EMBL.

Chapter 7: Redress

Article 25 – Complaints and access to justice

1. Any data subject may complain in writing to the DPO about any legal or material act or omission of a process owner or a data processor. The DPO shall respond within 45 days. If the data subject believes that the response of the DPO is unsatisfactory or if the DPO has failed to respond within three months from receipt of the complaint, the data subject may complain in writing to the Data Protection Committee.
2. The Data Protection Committee must decide on the complaint within two months of receipt. It may extend that time-limit, if it considers the complaint to rest on complicated facts or legal considerations and gives prior notice to the complainant.
3. The data subject may challenge the decision of the Data Protection Committee, if he/she considers it affects him/her adversely. He/she may do so by lodging a request for ad-hoc arbitration in accordance with Article 26, in order to finally and exclusively settle the matter, except for EMBL Members of Personnel who shall proceed

in accordance with Chapter 6 of the EMBL Staff Rules and Staff Regulations.

Article 26 – Arbitration

1. Any dispute, controversy or claim arising out of or relating to the processing of personal data under this Internal Policy and brought by data subjects other than EMBL Members of Personnel, shall be finally and exclusively resolved by arbitration under such procedure to be determined by the tribunal, provided that the procedure of Article 25 has been exhausted.
2. It is agreed that:
 - (a) the tribunal shall consist of one arbitrator, who is to be fully legally qualified, admitted to the bar in any one or more of the countries where EMBL has a site, and who can evidence expertise in the field of personal data protection;
 - (b) in default of the parties' agreement as to the arbitrator, the appointing authority shall be the German Institution of Arbitration (DIS);
 - (c) the seat of the arbitration shall be Heidelberg (Germany);
 - (d) the law governing the arbitration shall be this Internal Policy; the statutory documents of EMBL; and the general principles governing the law of international organisations and the rules of general international law;
 - (e) the language of the arbitration shall be English, German, or French, at the discretion of the data subject; and
 - (f) the data subject agrees, where required, to sign a separate arbitration agreement setting out the nature of the dispute and submitting to arbitration in accordance with this article.

Article 27 – Remedies and Sanctions

1. The Data Protection Committee when deciding on complaints, and the ad-hoc arbitrator when deciding on appeal, shall have the power to award appropriate remedies to data subjects, including compensatory measures.
2. An infringement of this Internal Policy may constitute misconduct and shall be addressed in accordance with EMBL rules of procedure for disciplinary proceedings, Section 2 5.01 of the Staff Rules and Regulations and the EMBL Internal Policies on Whistleblowing (Internal Policy No. 69), on Investigation (Internal Policy No.72), on Hearings (Internal Policy No. 73), and Pre-assessment (Internal Policy N° 75).

Article 28 – Cooperation

EMBL will at all times co-operate with competent authorities in its host countries, its member states, and on an international and supranational level, in the area of data protection.

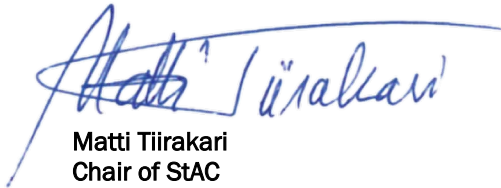
Chapter 8: Final provision

Article 29 - Entry into force

After its adoption, this Internal Policy shall enter into force on the day of its publication.

Date and signatures

Endorsed by



Matti Tiirakari
Chair of StAC

Date: 11.02.2025



Renato Alves
Vice-Chair of StAC

Date: 12.02.2025

Approved by



Edith Heard, FRS

Director General

Date: 25.02.2025