Internal Policy No. 68 on General Data Protection

First issued 18 May 2018

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 international public 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 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 international public 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 international public 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 international public 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 adequate in the sense of Article 45 of the GDPR. Moreover, it should be such as to enable parties subject to the GDPR to rely on appropriate safeguards, or derogations, during any transitional period.

(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.

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 at EMBL and ensures the free flow of such data among scientific researchers.

Article 2 – 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 any organisational entity within EMBL represented by an individual responsible for this entity and its data processing, having decision-making power regarding the entity's data processing and determining the purposes and means of processing alone, or jointly with other entities;

(4) 'organisational entity' means any entity which can be depicted in an organigram;

(5) 'recipient' means an individual or a legal entity or similar body to whom data are disclosed or made available;

(6) 'data processor' means an individual or a legal entity or similar body which processes personal data on behalf of the data controller;

(7) '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;

(8) 'data protection officer' means the officer established in Article 16;

(9) 'data protection committee' means the committee established in Article 20.

Article 3 – Scope

This Internal Policy regulates the processing of personal data by members of personnel at EMBL.

EMBL

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.

2. Personal data shall be processed for specified and lawful purposes, and in a manner proportional to these purposes.

3. 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.

4. It shall be for the data controller to comply with these principles and to be able to demonstrate such compliance.

Article 5 – 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. 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 6 – Freedom of scientific research

1. No requirements under this Internal Policy shall apply to data processing whose direct purpose is scientific research, 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 a data controller wishes to rely on the preceding paragraph:

   (a) a data protection impact assessment in accordance with Article 11 shall be carried out, always without prejudice to any separate additional approval that may be required by the Bioethics Internal Advisory Committee; and

   (b) the data controller shall complete the record required in Article 19(1)(h).

EMBL

Article 7 – 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 covered by a legal basis according to Article 5. 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 8 – 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 transferred from one organisational entity to another or from one site to another. This provision shall not relieve the sender from requiring any form of data processing restriction from the recipient the data controller deems necessary.

Article 9 – 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 international organisation which ensures an adequate level of data protection;

(2) the recipient offers appropriate safeguards;

(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.

Article 10 – Processing special categories of data

1. Data revealing political or philosophical or religious beliefs, trade union membership, sex life or sexual orientation may be processed only where absolutely necessary for the achievement of EMBL's legitimate aims or with data subjects' consent.

2. Data concerning health shall be processed only when necessary for the achievement of EMBL's legitimate aims or with data subjects' consent.

Article 11 – 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 6, a data controller shall, in advance of the processing, carry out a data protection impact assessment and address any issues such assessment may reveal.

2. A data controller may request the DPO to carry out the data protection impact assessment and draft the relevant report for the data controller, except in the case of Article 6 where the assessment needs to involve both the data controller and the DPO.

EMBL

Article 12 – Transparency of processing

1. A data controller shall inform data subjects of:

   (a) the data controller'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 13;

   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.

Article 13 – 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 12(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.

Article 14 – Confidentiality and security of processing

1. The data controller shall ensure the confidentiality, integrity, availability and resilience of processing by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. In grave cases of data breach, the data controller shall inform the Data Protection Committee. The data controller shall also inform the affected data subjects individually or, if that is impracticable, by publication.

Article 15 – Processing of personal data on behalf of the data controller

Where the data controller intends to instruct a data processor to process personal data on its behalf, the data controller 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.

Article 16 – 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 act functionally independently and shall neither seek nor accept instructions from anyone. He/she may be organisationally integrated with any corporate function supporting the role, such as Legal Services.

3. The DPO shall be bound by secrecy.

Article 17 – Duties of the data protection officer

1. The DPO shall monitor the application of this Internal Policy at all EMBL sites.

2. The DPO shall, on request or on his/her own initiative, advise data controllers on their rights and obligations, and data subjects on their rights.

3. The DPO shall act as the contact point for the Data Protection Committee.

4. The DPO shall produce a yearly report for the Director General.

5. 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 regarding such activities.

6. 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.

EMBL

Article 18 – Obligation to provide information and assistance

Data controllers 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 19 – Records and Register

1. Each data controller shall maintain a record of processing activities under its responsibility containing the following information:

   (a) the name and contact details of the data controller, the data protection officer and, where applicable, the joint data controller;

   (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 8, 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 referred to in Article 14(1);

   (h) where a data controller wishes to rely on Article 6(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 6(1) are still required.

2. Each data processor shall maintain a record of all categories of processing activities carried out on behalf of a data controller, containing:

   (a) the name and contact details of the data processor or data processors and of each data controller 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 data controller;

   (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 9, 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 14(1); andthe information required by Article 19(1)(h).The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. Data controllers 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 20 – Data Protection Committee

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 21 – 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 data controllers to restrict or discontinue processing; and

   (e) recommend to the Director General that disciplinary proceedings against data controllers 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.

Article 22 – Complaints and access to justice

1. Any data subject may complain in writing to the Data Protection Committee about any legal or material act or omission of a data controller or a data processor. 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.

2. 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 23, 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 23 – 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.

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 24 – 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 under Section 2 5.01 of the Staff Rules.

Article 25 – 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 order to facilitate the proper administration of justice, and to ensure observance of applicable rules and regulations, including in the area of data protection or other similar national legislation.

EMBL

Article 26 – Entry into force

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

Endorsed by

Christian Scherf
Chair of the Standing Advisory Committee

Date: 18.05.2018

Marzia Sidri
Vice Chair of the Standing Advisory Committee

Date: 18.05.2018

Approved by

Iain Mattaj
Director General

Date: 18.05.18