Privacy Notice

This privacy notice explains what personal data EMBL collects, for what purposes, how it is processed, and how we keep it secure, in the context of:

The exercise of DPO tasks and duties

1. Who is responsible for the processing

The EMBL data controller (and joint-controller if applicable) contact details are:

Data Protection Office
Meyerhofstraße 1
69117 Heidelberg
dpo@embl.org

2. What personal data do we process

The following categories of personal data may be processed:

Internal staff:

- name, surname, email and phone number
- department/unit and title
- EMBL site
- username
- signature.

Externals:

- name, surname, email and phone number
- if disclosed by the person (e.g. via email signature, letter or attached document): title, signature, physical address, country of residence
- when exercising a data subject right: a certified copy of the passport, with all personal data included therein.

In addition, for both internal staff and externals, the DPO may process any personal data that will be provided by the enquirer, or a third party (regarding themselves or other individuals), in the context of information exchanged with them via email, meeting, mobile phone or letter. E.g. company, organizational entity, description of concerns, personal case, circumstances, description of facts, opinions and assessments. In addition, DPO may, while investigating, access additional information about the enquirer or third-party related to them.

For cooperation activities, contact details (such as name, surname, email address, country of residence, physical address, company, title and telephone number) of external stakeholders (mainly DPOs), their statements/opinions exchanged during the cooperation (e.g. via email) and any other related information they provide may be processed.

If applicable, the following categories of sensitive data may be processed:

When fulfilling its tasks, the DPO may gather and manage sensitive data, such as health data, racial or ethnic origin, trade union membership, sex life or sexual orientation.

3. For what purposes do we process your personal data

Your personal data will be processed for the following purposes:

A data protection officer (DPO) shall be appointed by the Director General (Article 19 of IP68) and have the following tasks (Article 20 of IP68):

- The DPO shall monitor the application of IP68 within EMBL
- 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
- The DPO shall handle all requests by data subjects for the exercise of their rights, in accordance with Article 16 of IP68 and any complaints in accordance with Article 25 of IP68
- The DPO shall act as the contact point for the Data Protection Committee (DPC)
- The DPO shall produce a yearly report for the Director General
- 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 DPC 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 regarding such activities
- The DPO may, after consultation with the EMBL Standing Advisory Committee where required, propose sectoral guidance or standard operating procedures in areas of IP68 requiring further formalisation to the Director General
- 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.

Additionally,

- Article 10(1) of IP68 states that 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 way that privacy and data protection principles are guaranteed right from the start ('data protection by design')
- Article 11(2) of IP68 refers to the fact that 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(3) of IP68 mandates the DPO to keep a central register of Records of Processing Activities. This register was kept in Alfresco until mid-2025 and is currently kept in Smartsheet (see dedicated privacy notice).
- Article 15 of IP68 mentions that any personal data breach shall be reported to the DPO, who shall monitor, advise and assist the process owners in case of data breaches (see the dedicated privacy notice). In grave cases of data breach, the process owner supported by the DPO shall inform the DPC.

In carrying out its tasks, the DPO will, at any time, process all necessary personal data and shall have access to all premises, facilities, documents and media.

The DPO also cooperates (e.g. awareness raising exercises) with national and international entities and will support, to the best of its capacity, the DPC and Data Protection Strategy Board (if they deem it necessary).

4. What is the legal basis for processing

We rely on the following legal basis(es) to process your personal data:

The processing is based on:

- Article 6(1)(d) of IP68, necessary for the functioning of EMBL.
- When processing special categories of personal data, processing is based on Article 9, legitimate interest and for EMBL staff, to comply with EMBL Council decisions.

5. Who can access your personal data

The following categories of recipients may access your personal data:

EMBL internal recipients:

In general, personal data processed in the scope of DPO's tasks are accessed only by the Data Protection Officer and the staff members of the Data Protection Office.

To perform its tasks, the DPO may have to disclose the enquirer's personal data with other EMBL departments (e.g. in the case of a data subject request, the data controller will be informed). The disclosure will always take place on a strict need-to-know basis and only the strictly necessary personal information will be shared.

For the personal data included in the register of records, they may be disclosed with the DG and the DPC.

For the personal data in the EMBL tools used by the DPO, they may be accessed by the IT Team for support purposes, on a strict need-to-know basis.

EMBL external recipients:

To perform its tasks, the DPO uses tools that are provided by EMBL, e.g. Google Calendar, Zoom, Alfresco, ownCloud, Smartsheet, Webmail, some MS 365 applications (like Outlook, Word, PowerPoint, Excel and OneNote) and Cisco Jaber.

Processors are based in EU but may transfer personal data to the US.

As principle, personal data will not be shared with other external stakeholders. However, in the context of complaints, personal data may be shared with the ILOAT (EMBL staff) or ad-hoc arbitration (externals). Exceptionally, on a strictly necessary and need-to-know basis, personal data may be shared with external stakeholders (e.g., when organising an event with a third-party or if external legal consultation is needed in the case of arbitration).

6. How long do we keep your personal data

Your personal data will be kept for the following period of time:

Personal data processed in the EMBL tools used by the DPO is subject to the retention policies of each specific tool.

Personal data shared with IOs is subject to the specific IO retention policy when shared with them.

7. How do we protect your personal data

We have adopted the following measures to protect your personal data:

Risk Management & Controls: Regular risk assessments of information assets, Implementation of control measures, Periodic review of access rights.

Training & Access: Mandatory security awareness and data protection training, Access granted based on job roles, Strict management of privileged accounts, Cryptographic key management.

Incident Response & Recovery: Cyber security incident management process, Regular penetration testing, Disaster recovery planning, Business continuity measures.

Compliance & Privacy: Protection of personal data in adherence with IP68 and other contractual obligations, Biometric data security, Rigorous due diligence of third-party data hosting such as cloud services, Regular compliance monitoring.

8. Data subjects' rights and oversight mechanism

Under Article 16 of the EMBL Internal Policy No 68, data subjects have the following rights:

- a right not to be subject to a decision made by automated means (i.e. without any human intervention)
- a right to request access to your personal data

- a right to request information on the reasoning underlying data processing
- a right to object to the processing of personal data
- a right to request erasure or rectification of your personal data.

When the legal basis to process personal data is consent, please note that you have the right to withdraw your consent at any time.

Please note that those rights can be subject to limitations, as described in Article 16 (2) of the EMBL Internal Policy No 68.

If you wish to exercise your rights or wish to contact the data controller regarding any other data protection related matters, you can contact us using, by sending an e-mail to: info@embl.de or by sending a letter to: Meyerhofstraße 1 69117 Heidelberg Germany.

Advice on data protection matters can also be obtained from the EMBL Data Protection Officer (DPO), under Article 20 (2) of the EMBL Internal Policy No 68. The DPO can be reached by email at dpo@embl.org or by letter at: EMBL Data Protection Officer, EMBL Heidelberg, Meyerhofstraße 1, 69117 Heidelberg, Germany.

If you wish to complain under Article 25(1) of the EMBL Internal Policy No 68, you may do so with the DPO by email at dpo@embl.org.

If you believe that the response of the DPO is unsatisfactory or if the DPO has failed to respond within three months from receipt of the complaint, you may complain in writing to the Data Protection Committee. It can be reached by email at dpc@embl.org or by post at: EMBL Heidelberg, Data Protection Committee, Meyerhofstraße 1, 69117 Heidelberg, Germany.

Last update: 22/09/2025