European Federation of Periodontology

# Standard Operating Procedure

## External Requests for Personal Data

**14-04-2026**

# 1. SCOPE

As a principle, the EFP-EdC does not sell, trade or otherwise transfer to outside parties any collected personal data.

This Standard Operating Procedure (SOP) details the process to be followed by the EFP Education Committee (EFP-EdC) when an external entity expressly request personal data from the EFP pertaining to its partners, accredited members, students, staff, or other stakeholders.

It does not apply to subject access requests for personal data made by Data Subjects.

# 2. DEFINITIONS

- Personal data: any information related to an identified or identifiable natural person ("data subject").

- Data subject: data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. In practice, these also include all data which are or can be assigned to a person in any kind of way.

- External entity: any individual, organization, or body that is not part of the EFP but submits a request for information or data that is held by the EFP-EdC.

# 3. RESPONSIBILITY

The Data Protection Officer is responsible for answering any personal data request, including requests from external entities, and must receive said request at the following email address: dataprotection@efp.org.

# 4. PROCEDURE

## 4.1. Request

### 4.1.1. Written request

All requests for personal data or information from external parties must be submitted in writing to the DPO.

Any member of the EFP-EdC who receives such a request is required to immediately forward it to the DPO, using the email address specified within the present SOP (III).

### 4.1.2. In-person request

Solicitors seeking in-person access must notify the DPO by email at least two weeks in advance of their intended office visit. The DPO will then arrange the visit and communicate the scheduled date and time to the relevant onsite staff.

### 4.2. Identity verification

The identity of the person making the request should be confirmed. This may be done by calling the entity on a general telephone number and confirming the contact details, role and status of the requestor.

### 4.3. Request review

A review of the authority for the claim on the personal data should be carried out with reference to any mandates cited by the entity. Any existing letter of authorization giving this mandate should be requested.

Any supporting information provided by the entity should also be reviewed. In addition, a check should be made to ensure that all applicable aspects of the claim, such as the explanation of the purpose of the request, have been provided.

### 4.4. Legal support

The Committee should send every request to the DPO who will seek legal advice where:

- the request involves large volumes of personal data;
- there is a high risk to data subjects;
- the legal basis is unclear or contested; or
- the request may pose reputational or regulatory risks.

### 4.5. Decision

The DPO decides on disclosing personal data following an external request. The options available are to:

- Grant the request fully and disclose all personal data.
- Grant the request partially, disclosing only some of the data while redacting or withholding other personal or unrelated information.
- Deny the request entirely.

#### 4.5.1. Acceptance

As a principle, the EFP-EdC shall ensure that only the minimum amount of personal data necessary to fulfil the purpose of the request is disclosed.
To uphold this principle, the following measures must be taken whenever possible:

- irrelevant or excessive data must be redacted;
- anonymised or aggregated data should be provided instead of identifiable data.

#### 4.5.2. Data Subject Consent

Any disclosure of personal data to an external entity requires the EFP-EdC to ensure a lawful basis, such as legitimate interests, contractual necessity, or explicit consent. If

relying on consent, a signed Data Subject Consent Form (Annex I) must be secured before sharing the data.

For transfers of personal data outside the EEA, the EFP-EdC must obtain a signed Data Subject Consent Form (Annex II) from each data subject before sharing the data. This form must explicitly detail the transfer, potential risks, and purpose, and is required as an added layer of protection, even when other lawful grounds for transfer exist..

#### 4.5.3. Refusal

Any refusal to grant the request for personal data should be communicated and justified in writing to the requesting entity .

A request for personal data may be refused where:

- no lawful basis for disclosure exists;
- the identity or authority of the requester cannot be verified;
- the request is excessive or disproportionate;
- the data can reasonably be obtained directly from the data subject; or
- disclosure would infringe the rights and freedoms of the data subject.

All refusals must be documented and justified in writing.

#### 4.5.4. Additional information

In cases where the requests are unclear or incomplete, the DPO may request additional information to clarify why the data is not being disclosed. Any such supplementary information provided must then be reviewed before making a final decision.

## 5. SECURED TRANSFER

Where personal data is disclosed, it must be transmitted using secured communication channels.

Any email containing personal data must be clearly marked “Confidential” in the subject line and sent only to authorized recipients.

The following notice must be included in such emails:
*“This email contains personal data and confidential information intended solely for the designated recipient(s). It must not be shared, forwarded, copied, or disclosed to any unauthorized person and must be handled with appropriate care and confidentiality.”*

## 6. TIMELINE

All requests must be handled within defined timeframes:

- acknowledgement of receipt: within five (5) working days;
- completion of identity verification: without undue delay;

- final decision: within thirty (30) calendar days of receipt, unless the request is complex.

Where additional time is required, the requesting entity shall be informed in writing, including the reasons for the delay.

## 7. RECORD

Full and accurate records of the above process should be made and retained. These should include:

- details of the request made and the requesting entity;
- the process carried out to confirm the identity of the requestor;
- the reasoning for the decision to disclose or not to disclose the personal data;
- where personal data is disclosed, details of the personal data disclosed and the method of disclosure.

## 8. DATA BREACH CONSIDERATIONS

Any accidental or unlawful disclosure of personal data must be treated as a potential personal data breach and notified immediately to the DPO.

## 9. REVIEW

This SOP shall be reviewed whenever there are significant changes in legal or operational requirements.

# ANNEX I - CONSENT FORM WITHIN EEA

## DATA SUBJECT CONSENT FORM
**(Within the *European Economic Area* (EEA))**

I, **[Full name]**
understand that the **European Federation of Periodontology** is sharing my personal data:

- **[Personal Data Subject to this Request]**
-
-

with **[External party]** located in the **[Country]**.

I hereby give my explicit, informed consent for this transfer to occur, for the purpose of:

- **[Specify the processing activity for which consent is being given]**

I understand I may withdraw this consent at any time by submitting a request via email to dataprotection@efp.org.

Signed by **[name]**:

Signature:

Date:

# ANNEX II - CONSENT FORM OUTSIDE OF THE EEA

## DATA SUBJECT CONSENT FORM
**(Outside of the *European Economic Area* (EEA))**

I, **[Full name]**
understand that the **European Federation of Periodontology** is sharing my personal data:

- **[Personal Data Subject to this Request]**
-
-

with **[External party]** located in the **[Country]**.

I acknowledge that this country has not received an adequacy decision from the European Commission and that potential risks (e.g., government surveillance, insufficient data subject rights) may be associated with this transfer.

I hereby give my explicit, informed consent for this transfer to occur, for the purpose of:

- **[Specify the processing activity for which consent is being given]**

I understand I may withdraw this consent at any time by submitting a request via email to dataprotection@efp.org.

Signed by **[name]**:

Signature:

Date: