PUBLIC CONSULTATION RESPONSE | 12 NOVEMBER 2026

# EDPB Guidelines 04/2026

The application of the power to impose administrative fines in relation to other corrective powers under the GDPR

An individual submission • Identifying details withheld

## Summary

Accountability cannot end with the regulator when the regulator's own effectiveness is in question. This submission draws on nine separate data protection complaints concerning sensitive medical data held by dental healthcare providers in Ireland, Portugal and the United Kingdom. The complaints raise serious questions about the accuracy, completeness, accessibility and security of medical records, and the effectiveness of regulatory responses. The UK complaints are included for comparison. The recommendations apply across healthcare.

The purpose is to inform the European Data Protection Board's review of how supervisory authorities choose and apply corrective measures, including administrative fines. The experiences described demonstrate why effective enforcement, clear decisions and meaningful remedies matter to an individual whose medical records cannot be relied upon.

## 1. Distinct layers of accountability

**Healthcare providers as data controllers.** Dental practices, like other healthcare providers, are responsible for the accuracy, completeness and security of the medical records they hold, and must respond to access and rectification requests. These records contain sensitive medical data, falling within the special category of data concerning health under Article 9 GDPR. Relevant obligations include Articles 5, 12, 15, 16 and 32.

**Supervisory authorities.** Separate questions arise about whether the authority examined the evidence submitted, addressed the specific concerns raised and communicated the outcome of its assessment. Where an infringement is established, the question is whether effective corrective action was taken.

**Independent scrutiny.** Articles 77 and 78 GDPR provide for complaints and judicial remedies. Individuals need clear decisions and reasons in order to understand whether their rights have been upheld and to challenge a decision or failure to handle a complaint where necessary.

## 2. Documented experiences of data protection enforcement

Nine separate data protection complaints concerning sensitive medical data were submitted across three jurisdictions: six in Ireland, one in Portugal and two in the United Kingdom.

The complaints concerned medical records held by dental healthcare providers and included:

- Inaccurate and incomplete medical records.
- Failure to provide medical records following a formal access request, despite acknowledging the request.
- Radiographs appearing in medical records that were not taken during the documented consultations, without explanation of their origin.
- Clinical conclusions recorded without documentation of supporting assessments.
- Missing documentation concerning treatment, its rationale and follow-up care.
- Omission of radiographs previously supplied by the patient from medical records provided in response to a subject access request.
- Unannounced hand delivery of confidential medical records to a patient's private residence.
- Omission of significant categories of medical data from responses to access requests.

Each complaint was supported by documentary evidence.

These complaints do not represent the full extent of the complainant's concerns regarding the accuracy, completeness and handling of medical records. Further complaints had also been considered in relation to records held by other healthcare providers.

## Regulatory outcomes

### Ireland — Data Protection Commission

Of the six complaints submitted, four received responses. Three recommended returning to the healthcare provider, while one requested the original access request and related correspondence. Two complaints received no response.

In one case, the original access request and confirmation from the provider that the records would be supplied had already been included in the complaint. The provider had not complied with the request, yet the complainant was directed back to the provider.

None of the responses communicated a finding on whether a GDPR infringement had occurred or identified any corrective action taken or proposed.

### Portugal — CNPD

Registration of the complaint was acknowledged. No subsequent substantive response has been received.

### United Kingdom — Information Commissioner's Office

In both cases, the ICO declined to undertake a more detailed investigation, referring to considerations including significant harm, wider impact and broader data protection concerns. Both complaints were recorded for information purposes.

Neither response determined whether the healthcare provider had complied with data protection law.

The complainant deliberately focused the complaints on the handling of medical data rather than detailing the harm experienced. The absence of detailed information about clinical or other harm should not be interpreted as evidence that the concerns regarding sensitive medical data were insignificant.

### Collective outcome

Across nine separate complaints, no determination of whether a data protection infringement had occurred was communicated to the complainant, nor was any corrective action identified.

The complainant was left without any clear indication of what had been investigated, what conclusions had been reached or whether their data protection rights had been upheld.

## 3. Importance of accurate medical records

Medical records are essential for continuity of care and future treatment. They are also relied upon by clinical experts and courts in medical negligence proceedings and, in the case of dental records, for forensic identification after death.

Article 16 GDPR distinguishes between the rectification of inaccurate personal data and the completion of incomplete data through a supplementary statement.

The addition of a supplementary statement should not substitute for the investigation and rectification of factual inaccuracies in medical records.

Patients should not have to rely on the cooperation of the healthcare provider whose medical records they dispute in order to secure their data protection rights. Providing independent oversight and enforcing those rights are the responsibility of the supervisory authority.

The continued reliance on inaccurate medical records can have significant clinical consequences and, in some circumstances, legal consequences.

## 4. Recommendations for Guidelines 04/2026

### 4.1 — Effective corrective action

Where an infringement is established, the choice of corrective measure should address the infringement and secure compliance.

### 4.2 — Statutory deadlines

Individuals should not have to repeatedly pursue data controllers to obtain compliance with statutory deadlines. Article 12(3) generally requires a response within one month, subject to a properly notified extension where permitted. The duration of non-compliance should inform the assessment under Article 83(2).

### 4.3 — Sensitive medical data

The seriousness of an infringement involving medical data should be assessed even where only one individual is affected. Proof of physical injury from treatment should not be a condition for assessing a data protection infringement.

### 4.4 — Clear findings

An unresolved complaint is not the same as a finding that no infringement occurred. Decisions should explain the evidence considered, the relevant GDPR provisions and the reasons for the conclusion.

### 4.5 — Regulatory decisions

Supervisory authorities should explain their choice of corrective action, including a fine, another corrective measure, a combination of measures, or why no action was taken.

### 4.6 — Corrective measures and fines

Corrective orders and administrative fines should reflect the seriousness and circumstances of an infringement, secure compliance and discourage further non-compliance. Referring the individual back to the controller should not be a substitute for effective enforcement.

## 5. Regulatory accountability

Effective enforcement requires accountability from both data controllers and supervisory authorities. Individuals should receive clear explanations of decisions, the legal basis for those decisions and what corrective action has been taken. Where concerns remain unresolved, there must be a meaningful route to independent scrutiny.

Articles 57(1)(f) and 77(2) GDPR require complaint handling and communication of progress and outcomes. Article 78 provides for judicial remedies, including where an authority fails to handle a complaint or inform the individual of progress or outcome within three months.

## Conclusion

The experiences presented show why GDPR rights must be backed by effective enforcement. The Guidelines should reinforce that corrective measures are selected according to the seriousness and circumstances of established infringements, and that decisions are explained.

**Accountability cannot end with the regulator when the regulator's own effectiveness is in question.**

**Evidence note.** This submission is based on documented complaints, medical records and correspondence with data protection authorities. Identifying details have been withheld to protect privacy.

Public sources: EDPB Guidelines 04/2026 public consultation • Regulation (EU) 2016/679 (GDPR), Articles 5, 9, 12, 15, 16, 32, 57, 58, 77, 78 and 83.