EUROPEAN DATA PROTECTION SUPERVISOR

# AUDIT REPORT ON THE EUROPEAN COMMISSION'S MEDICAL SERVICE (COM MS)

Brussels, 16 and 17 January 2024
EDPS case number 2023-0976

## *Executive Summary*

*Introduction*

The European Data Protection Supervisor (EDPS) is the independent supervisory authority established by Article 52 of Regulation (EU) 2018/1725 ('EUDPR')[1] responsible for:

- Monitoring and ensuring the application of the provisions of the EUDPR and any other EU act relating to the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data by a EU institution or body;
- Advising EU institutions, bodies, offices and agencies (EUIs) as well as data subjects on all matters concerning the processing of personal data.

To these ends, the EDPS fulfils the duties provided for in Article 57 of the EUDPR and exercises the powers granted in Article 58 of the EUDPR. Among his powers to investigate, the EDPS can carry out investigations in the form of data protection audits. The power to audit is one of the tools established to monitor and ensure compliance with the EUDPR.

This audit is part of the EDPS annual audit plan for 2023 and should be viewed as the final stage before formal action under Article 58 of the EUDPR. The formal Decision was communicated to the Secretary General of the European Commission (COM) by means of an Announcement Letter dated 13 October 2023. The fieldwork was carried out on 16 and 17 January 2024 at the COM MS's premises in Brussels[2].

[1] *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98,*

[2] *Avenue d'Auderghem 19, Brussels.*

Further contact with COM MS took place concerning the minutes and the last item of evidence was received by the EDPS on 21 January 2024. The final minutes of the audit were sent to the Secretary General of the COM on 26 February 2024. The minutes summarised the meetings with the COM and the COM MS staff during the exercise. A list of evidence requested during the audit was provided by the EDPS as an annex to the minutes.

This audit fits into the EDPS Strategy 2020-2024[3]. The Strategy underlines that a distinction should be made between measures which were introduced by EUIs during the COVID-19 crisis that developed naturally and those which accelerated only due to extraordinary circumstances (i.e., the contact-tracing public health measures and COVID-19 self-declarations); the latter should be recognised as temporary and discarded once the crisis is over[4]. In the Strategy, the EDPS also highlighted that the new reality requires that the data protection community continue to strive to reach a fair balance between the need to ensure public health and the right to privacy and the protection of personal data[5].

Overall, the EDPS notes that the COM MS cooperated with the EDPS audit team in an exemplary way.

*Scope of the audit*

This audit focuses on the implementation in practice of the **retention periods applicable to different medical documents**, which are kept in the COM MS's medical files.

Data concerning health is one of the special categories of personal data included under Article 10 of the EUDPR. The COM MS processes health data of thousands of data subjects. Therefore, it is the responsibility of COM MS as controller to adopt necessary and proportionate retention periods for each category of personal data they process and store, in line with Article 4(1)(e) of the EUDPR. The scope of the audit was determined by the EDPS as covering in particular:

- the implementation of recommendations contained in a previous EDPS Opinion on the retention periods of different medical documents.
- the implementation of recommendations from the previous audit, in relation to the design and implementation of a secure disposal process for the paper files, which are no longer necessary as the maximum retention period has elapsed in light of Article 4(1)(e) of the EUDPR.

[3] *https://www.edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf*
[4] *EDPS Strategy, p. 12.*
[5] *EDPS Strategy, p. 10.*

The EDPS intends to accompany the EUDPR compliance process and to point out infringements, as the case may be. This audit additionally provides the opportunity to raise awareness on data protection issues more generally. Whenever relevant and necessary, the EDPS auditors could examine related activities and other related processing operations.

*Key findings of the audit*

The audit report summarises the findings identified during the data protection audit.

Following an analysis of the documents received during the audit, the EDPS established that, in some cases, the COM MS has not satisfactorily implemented in practice the retention periods applicable to certain medical documents kept in the COM MS's medical files. In addition, the COM MS has only partially implemented the recommendations issued by the EDPS in the previous audit.

The **major findings** include the following:

- The COM MS has in some cases **not applied** established retention periods in practice, nor has it **informed** the data subjects accordingly;
- All but one category of paper files have been **kept for longer than necessary**, as the maximum retention period has elapsed;
- The COM MS has not put in place **processes for the application** of the established retention periods in all electronic means of processing medical data, including functional mailboxes, shared drives and the main information system for processing medical data.

*Recommendations and follow up to the audit*

The findings of the audit point to potential non-compliance with the EUDPR. Therefore, the EDPS decided to **refer these matters to the COM MS, as controller, in the form of recommendations,** in line with the powers granted to the EDPS under Article 58(2)(c) of the EUDPR. The EDPS notes that these recommendations must be implemented by the COM MS[6] within the deadlines indicated in the audit report.

[6] *During the onsite audit, COM MS already showed willingness to proceed with the appropriate implementation in practice of the recommendations issued by the EDPS in relation to retention periods applicable to different medical documents.*

The EDPS considers that, in view of the above circumstances, referring a matter to the controller is an appropriate and necessary corrective measure. A primary purpose of the EDPS' power to refer a matter to the controller under Article 58(2)(c) of the EUDPR is to ensure that data subjects are afforded an adequate level of protection and to allow the controller to remedy any finding of inadequacy within the deadline set for each of the recommendations.

Brussels, 05 December 2024

*(e-signed)*
Wojciech Rafał WIEWIÓROWSKI