WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr [...]
Executive Director,
European Insurance and Occupational Pension Authority (EIOPA)
Westhafenplatz 1
60327 Frankfurt am Main
Germany

Brussels,
WW/DHo/sn/D(2018)1130 **C 2017-0284**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior-checking Opinion regarding the processing of health data at the European Insurance and Occupational Pension Authority (EIOPA) (EDPS case 2017-0284)

Dear Mr [...],

On 7 March 2017, the European Data Protection Supervisor (EDPS) received a notification for prior checking under Article 27 of Regulation (EC) No 45/2001[1] ('the Regulation') on 'the processing of health data' from the Data Protection Officer (DPO) of the European Insurance and Occupational Pension Authority (EIOPA).[2]

The EDPS has issued Guidelines concerning the processing of health data in the workplace by Union institutions and bodies[3] ('the Guidelines'). Therefore, this Opinion analyses and highlights only those practices which do not seem to be in conformity with the principles of the Regulation and with the Guidelines. In the light of the accountability principle guiding his work, the EDPS would nonetheless like to highlight that *all* relevant recommendations made in the Guidelines apply to the processing operations put in place for the processing of health data at EIOPA.

[1] OJ L 8, 12.1.2001, p. 1.
[2] As this is an ex-post case, the deadline of two months does not apply. [list suspensions]. This case has been dealt with on a best-effort basis.
[3] Available on the EDPS website: https://edps.europa.eu/sites/edp/files/publication/09-09-28_guidelines_healthdata_atwork_en.pdf

Grounds for prior checking

According to the Guidelines, 'processing operations involving health data are subject to prior-checking in conformity with Article 27(2)(a) of Regulation (EC) 45/2001, since they are likely to present a specific risk to the rights and freedom of data subjects'.

According to the notification, EIOPA's ground for the prior-checking of the processing operation at stake refers to Articles 27(2)(a) and 27(2)(b) of the Regulation. While Article 27(2)(a) provides for prior-checking in cases of processing of health data relating to health, Article 27(2)(b) refers to processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct. In this specific case, the processing of health data at EIOPA is not intended to evaluate the ability, efficiency and conduct of employees.

Thus, in line with the Regulation and the Guidelines, the processing operation at hand is subject to prior checking according to Article 27(2)(a) of the Regulation.

Data transfer to third countries

Article 9 of the Regulation provides that personal data may only be transferred to recipients who are not subject to national law adopted pursuant to Directive 95/46/EC under certain conditions. Adequacy of protection should be assessed in view of the criteria set forth in Article 9(2). Exceptional cases are provided for in Article 9(6).

In the notification, EIOPA refers to the possibility of transferring data to third countries only if the respective national legislation applies a level of protection of personal data, which is at least equivalent to Directive 95/46/EC. EIOPA has further clarified that such transfer would only occur in exceptional circumstances such as the urgency for medical files being sent to a third country following a staff member's request.[4]

The EDPS **recommends** inserting in the privacy statement a specific paragraph on possible personal data transfers to third countries, informing staff members under which circumstances such a data transfer may occur.

Information to data subjects

Articles 11 and 12 of Regulation 45/2001 provide that data subjects must be informed of the processing of data relating to them and list a range of general and additional items. The latter apply insofar as they are necessary in order to guarantee fair processing in respect of the data subject having regard to the specific circumstance of the processing operation. In the present case, medical data are partly provided by the data subject and partly by the Commission's medical services or external doctors and medical providers.

EIOPA's privacy statement does not mention the legal basis of the processing at hand. The EDPS, in light of the Guidelines, **recommends** adding the legal basis for each specific processing operation on health data (pre-recruitment visits, annual medical check-ups and health related administrative data) to the privacy statement.

[4] As per email sent by EIOPA's DPO, dated 23 January 2018.

Conclusion

In this Opinion, the EDPS has made some recommendations to ensure compliance with the Regulation and suggestions for improvements. Provided that such recommendations are implemented, the EDPS sees no reason to believe that there is a breach of the Regulation.

In light of the accountability principle, the EDPS expects EIOPA to implement the above recommendations accordingly and has therefore decided to **close the case**.

Yours sincerely,

(signed)

Wojciech Rafał WIEWIÓROWSKI

Cc: [...], DPO, EIOPA