



WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

European Insurance and Occupational
Pensions Authority
Westhafenplatz,1, D-60327
Frankfurt Am Main
Germany

Brussels,
WW//D(2018)1198 C 2017-0769
Please use edps@edps.europa.eu for all
correspondence

**Subject: Opinion on the contract renewal procedure at EIOPA, your reference:
DPO-17-003**

Dear,

I refer to the notification regarding the processing operation "Contract Renewal Procedure" from the European Insurance and Occupational Pensions Authority (EIOPA) sent to the European Data Protection Supervisor (EDPS) on 28 August 2017 for prior checking under Article 27 of Regulation (EC) No 45/2001¹ ("the Regulation"). On 19 September 2017 and 10 April 2018 the EDPS sent a request for further information to EIOPA's Data Protection Officer (DPO). The DPO's answer was received by the EDPS on 6 April and 12 April 2018.

The EDPS has issued Guidelines concerning the processing of personal data for staff evaluation ("the Guidelines").² 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 renewal of temporary and contract agent's contracts at EIOPA.

¹ OJ L 8, 12.1.2001, p. 1.

² EDPS Guidelines concerning the processing of personal data in the area of staff evaluation July 2011, page 2 section 1, available at: https://edps.europa.eu/sites/edp/files/publication/11-07-15_evaluation_guidelines_en.pdf.

1) Facts

According to EIOPA, the ground for lawfulness of the data processing operation is Article 5(a) of the Regulation. The processing of personal data is considered as necessary to fulfil the obligations deriving from the Staff Regulations and the Conditions of Employment of Other Servants of the European Union (CEOS)³ for the management of EIOPA staff. The processing operation establishes a decision making process when considering to offer or not a renewal of an employment contract. The renewal of the employment contracts for temporary agents is based on Article 8 and 47 of the Conditions of Employment of Other Servants of the European Union (CEOS) and the renewal of the employment contracts for contract agents is based on Article 85 and 119 of the CEOS. The procedure for dealing with the renewal of employment contracts of temporary and contract agents is based on the rules of the CEOS and EIOPA's draft Procedure on Contract Renewal.

2) Legal Analysis

2.1) Conservation periods

Article 4(1)(e) of the Regulation provides that personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.*"

According to the information provided by EIOPA, two conservation periods were established:

- 1) Contract amendments and letters informing staff members about non-renewals are kept in the personal files of the staff members concerned for 5 years following the end of the employment relationship with EIOPA.
- 2) Contract renewal reports as well as e-mails or other documents exchanged in the context of the contract renewal procedure are kept for 5 years following the end of the respective evaluation procedure⁴.

The EDPS welcomes the fact that EIOPA has established two different conservation periods. In fact, conservation of contract renewal reports and other working documents is set to 5 years after the end of the contract renewal exercise in question, which appears to be a good application of the principle in Article 4(1)(e).

2.2) Information provided to the data subjects

The EDPS welcomes the fact that the Privacy Statement for the notified processing activity is published on the "InCiderNet" EIOPA's intranet, under the HR section⁵. Also, the first e-mail informing the staff member on the contract renewal exercise will contain a link to the privacy statement.

Articles 11 and 12 of the Regulation set out the information to be provided to data subjects in order ensure fairness and transparency of processing including also legal basis of the processing. The Privacy Statement does not refer to any legal basis for the processing operation, therefore **the EDPS recommends to include the respective, specific legal basis.**

With regard to the procedures for staff members to exercise their rights of access, rectification and others, as a suggestion for improvement, **the EDPS suggests including specific contact details of the HR unit acting on behalf of the controller. The EDPS also suggests (as a good**

³ REGULATION No 31 (EEC), 11 (EAEC) laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community (OJ 45, 14.6.1962, p. 1385), as amended.

⁴ See point 13 of the notification and based on information provided by the DPO of EIOPA on 6 and 12 April.

⁵ See point 7 of the notification.

practice) including information on in which time limit data subjects can expect a reaction from the controller (e.g. 3 months for access request, without delay for rectification, etc.).⁶ This information should be provided in the Privacy statement.

1. The EDPS recommends that EIOPA include a specific legal basis in the Privacy Statement for the processing operation.

2.3) Data quality

Pursuant to Article 4(1)(c) of the Regulation, personal data must be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed. Processing of personal data have to be necessary for the legitimate performance of tasks covered by the competence of the recipient, who cannot process the data for any other purpose than for which they were transmitted. This presupposes that the information is indeed limited to what is “necessary” and processed only on a need to know basis also to meet data minimisation requirements under Article 4(1)(c) of the Regulation.

Electronic copies of documents are stored on the H Drive (personal drive) of individual managers and on the HR folder of the I Drive, see point 10 of the notification. EIOPA confirmed that the I Drive is a shared drive and access to the HR folder of the I Drive is granted only to the HR Unit. This seems excessive in the sense of Article 4(1)(c) of the Regulation, therefore the EDPS recommends that access is not granted automatically to all members of the HR unit. EIOPA should give such access rights on a need to know basis only to the members of the HR unit who need to access the personal data for the performance of their tasks related to the contract renewal procedure and management of staff.

The notification and the privacy statement both mention a number of possible recipients of personal data on a need-to-know basis, such as the European Anti-Fraud Office, the European Ombudsman or EU Courts. For your information, with regard to Article 2(g) of the Regulation, authorities which would only receive data in the context of specific targeted inquiries are not considered "recipients" and do not *need* to be mentioned in the privacy statement.⁷

2. The EDPS recommends that EIOPA give access to the personal data processed on a need to know basis, only where it is necessary for the legitimate performance of tasks covered by the competence of the recipient, in line with the requirements of data minimisation.

In this Opinion, the EDPS has made several recommendations to ensure compliance with the Regulation, as well as several suggestions for improvement.

⁶ See EDPS opinion of 12 June 2014 concerning “The processing operations related to renewal of contracts for temporary and contract agents in the Innovation and Networks Executive Agency”, case 2013-1288, page 2, available at: https://edps.europa.eu/sites/edp/files/publication/14-06-12_letter_contract_agents_inea_en.pdf.

⁷ This is an exception to the information obligations in Article 11 and 12, but not to the rules on transfers in Articles 7 to 9. In practice, this means that authorities such as the OLAF, the European Ombudsman or the EDPS do not need to be mentioned in the privacy statement (unless the processing operation in question involves transfers to these organisations as part of the procedure); however, the applicable rules on transfers will always need to be respected.

The EDPS recommends that EIOPA:

1. Include a specific legal basis in the Privacy Statement for the processing operation.
2. Give access to the personal data processed on a need to know basis, only where it is necessary for the legitimate performance of tasks covered by the competence of the recipient, in line with the requirements of data minimisation.

The EDPS suggests for improvement that EIOPA:

1. Include contact details to exercise the right of data subjects under point 14 of the Privacy Statement.
2. Include information on in which time limit a reaction can be expected in the Privacy statement under points 10-13 of the privacy statement.

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

Kind regards,

(signed)

Wojciech Rafał WIEWIÓROWSKI

Cc: Data Protection Officer EIOPA