EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Director of the Human Resources Department
European Union Intellectual Property Office
Avenida de Europa 4
E-03008 Alicante
Spain

Brussels,
WW/ZS/sn/ D(2017) 6 December 2017
C 2017-0813
Please use edps@edps.europa.eu for all correspondence

Subject: Prior-checking Opinion regarding Feedback event 2017 at European Union Intellectual Property Office (EDPS case 2017-0813)

Dear,

On 18 September 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 "Feedback Event 2017" from the Data Protection Officer (DPO) of the European Union Intellectual Property Office (EUIPO)[2].

As mentioned by the DPO, the notification is an update of the prior check notification 'Peer Feedback Questionnaire at OHIM'[3]. This processing operation is also similar to other notified cases of feedback tools for managers already prior checked by the EDPS[4]. For this reason, this Opinion does not contain a full analysis of all data protection aspects. It rather focuses on those points that diverge from other cases, or those that diverge from the previous notification on 'Peer Feedback Questionnaire at OHIM' or otherwise require improvement[5].

[1] OJ L 8, 12.1.2001, p. 1.
[2] According to Article 27(4) of the Regulation, the EDPS has to provide his Opinion within two months of receiving the notification, not counting suspensions for requests for further information. The deadline was suspended between 22 and 25 September, 10 and 14 November, 14 and 16 November, 21 November and 6 December and on 6 December for DPO consultation. The EDPS shall thus render his Opinion by 12 December 2017.
[3] EDPS case number: 2015-0733, Opinion of 24 November 2015.
[4] Cases 2009-0215, 2013-1290, 2014-0906, 2014-1146, 2015-0733, 2015-0772, 2016-0002, 2016-1007 and 2017-0588.
[5] The notification covers (1) a staff satisfaction survey to provide feedback about the functioning of EUIPO, (2) a peer feedback enabling staff members to perform a self- assessment and provide and receive feedback about and

1. Facts and analysis

1.1. Lawfulness of the processing

The legal basis for the processing operation is Article 24a of the Staff Regulations and Articles 11 and 81 of the Conditions of Employment of Other Servants.

As grounds for lawfulness, EUIPO has stated that the processing of personal information is based the unambiguous, specific, informed and freely given consent of the data subject (Article 5(d)[6] of the Regulation.

The data subject's consent is defined in Article 2(h) of the Regulation as "*any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed".* In this regard, the EDPS underlines that consent should be used with caution in the employment context. Such consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence. Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.

The notification clearly states that participation in the processing operation is voluntary both for the assessed and the assessors. Participation or not does not have consequences over the data subject. Participants can opt-out at any time. However, the privacy statement does not specify that consent can be withdrawn at any time also while the exercise is underway. For the sake of completeness, the privacy statement should make clear that consent covers the whole process, including the group reports (see below under 1.2).

The EDPS **recommends** that the privacy statement make clear that consent covers the whole exercise, including group reports, and that participants can decide to opt-out from the exercise at any time without adverse consequences.

1.2. Processing of group reports

According to the notification, the information provided is processed automatically to produce both group reports and individual feedback reports (including consolidated data preventing the identification of reviewers). While the individual feedback reports are accessible to the data subject concerned only, the group reports can be accessed by the Executive Director, the Director of Human Resources and a limited number of other staff members[7]. Group feedback reports will be developed to provide an organizational overview of the results obtained through peer and 360º feedback. Thy will serve the purpose of allowing EUIPO to understand the strengths and the areas for improvement. They will cover one team leader group report, one manager group report and one staff group report. In order to ensure confidentiality, the reports

from their peers, and (3) a 360° feedback for managers receiving feedback from their peers and from direct report and line managers about their leadership skills. On 14 November EUIPO confirmed that the prior check notification covers only the peer feedback and the 360° feedback as the staff satisfaction survey is not considered to present specific risks to the rights and freedoms of data subjects. Therefore, this opinion refers only to the peer feedback and the 360° feedback under the term of processing operation.

[6] Personal data may be processed only if the data subject has unambiguously given their consent.

[7] However data shown in some sections such as 'summary manager heat map', 'summary team leader heat map 'and 'summary staff heat map' will not be accessible.

will be limited to show aggregate and anonymized data only and will be released only in case the minimum number[8] of individual reports is obtained.

The group reports do not allow for the identification of individual answers provided during the exercise to the online questionnaire. In view of the optional character of the processing operation, the EDPS welcomes the introduction of a criterion relating to a minimum number of participants to issue individual and group reports. However, we highlight the importance of ensuring that these reports will not contain data that may allow identification of individuals, turning aggregated data into personal data.

Furthermore, it is our understanding that sharing group reports does not have the same purpose as producing individual ones[9] and the privacy statement does not indicate either the purpose of the generation of group reports or the categories of data contained therein.

The EDPS **recommends** that the privacy statement clearly define the respective (and different) purposes of the group reports as well as the categories of data contained therein.

1.3. Processing on behalf of the controller

According to the information provided by EUIPO, as included in the privacy statement, the processing of the personal data is entrusted to an external provider based on a Framework Contract. The contractor works with a dedicated sub-contractor on the peer and 360º feedback. All personal data are processed and stored in the external tools owned by the contractor, based in the United Kingdom. EUIPO also informed that the contractor has ISO 27001 certification and it uses a cloud service provider with servers located in the EU. The cloud service provider implements ISO 27001, 27017, and 27018 standards.

EUIPO informed the EDPS on 14 November that data may need to be accessed by the staff of the contractor in a non-EU country without an adequacy decision. EUIPO provided the model standard contractual clauses the contractor is using in its contracts with sub-processors and finally confirmed on 16 November that the contractor guarantees that nobody located outside of the European Union may access the personal data provided by EUIPO.

The contractor has a subcontractor based in the United States. This subcontractor is covered and registered as active participant under the Data Projection Privacy Shield. To mitigate potential risks, the EDPS welcomes that the controller is examining the organizational, technical and IT measures of the sub-contractor to prepare a fully-fledged security risk assessment.

The EDPS welcomes that the framework contract provides for the application of Regulation 45/2001[10] to any processing of personal data related to the contract and it also sets detailed provisions on rights and obligations of the contractor including also subcontracting[11]. Furthermore, the EDPS takes note that both the contractor and its subcontractor are clearly mentioned in the privacy statement.

...

[8] At least 10 individual reports are needed for the group reports and at least 3 persons should provide input for the individual feedback reports to release the reports.

[9] The purpose of individual reports for the peer feedback is enabling staff members to perform a self- assessment and provide and receive feedback about and from their peers. For the 360° feedback for managers the purpose is receiving feedback from their peers and from direct report and line managers about their leadership skills.

[10] Article 1.9.

[11] Articles 12 and 13 of the General Conditions.

2. Conclusion

In this Opinion, the EDPS has made several recommendations to ensure compliance with the Regulation, as well as several suggestions for improvement. The EDPS expects **implementation**, but does not require documentary evidence for the following recommendations made in this Opinion:

1. Clarify in the privacy statement that consent covers the whole exercise including group reports and participants can decide to opt-out at any time.
2. Define the respective purpose of the group reports and the categories of data covered in the privacy statement.

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

Yours sincerely,

Wojciech Rafał WIEWIÓROWSKI

cc.: DPO EUIPO.