

EUROPEAN DATA  
PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI  
SUPERVISOR

Mr Adam FARKAS  
Executive Director  
European Banking Authority (EBA)  
One Canada Square - Floor 46  
Canary Wharf  
London E14 5AA  
UNITED KINGDOM

Brussels, 21 April 2015  
GB/MG/cpl/D(2015) 0675 C 2014-0496  
Please use [edps@edps.europa.eu](mailto:edps@edps.europa.eu) for all  
correspondence

**Subject: Prior checking notification concerning "processing of leave and flexitime"**

Dear Mr Farkas,

On 13 February 2015, the European Data Protection Supervisor (EDPS) received a notification for prior checking concerning "processing of leave and flexitime" from the Data Protection Officer (DPO) of the European Banking Authority (EBA) (case 2014-0496).

The notification, accompanied by a cover letter and a copy of the "specific privacy notice on personal data protection in relation to leave and flexitime", states that the processing in place at EBA (since 1 January 2015, according to the aforesaid privacy notice) is "in compliance with the EDPS Guidelines concerning the processing of personal data in the area of leave and flexitime".<sup>1</sup>

In view of the above, the EDPS focuses its assessment on the differences between EBA's data processing and the EDPS specific Guidelines. Such differences relate to the categories of data undergoing processing and to the security measures.

It has to be noted that, since the data processing referred to in the notification already started at EBA, the notification is 'ex-post'. Hence, the two-month deadline under Article 27.4 of Regulation (EC) No 45/2001 (the Regulation) does not apply to this case, which has been dealt with by the EDPS on a best-effort basis. The EDPS regrets that EBA started the processing operation before having notified it to the EDPS.

---

<sup>1</sup> Guidelines concerning the processing of personal data in the area of leave and flexitime adopted on 20 December 2012 (EDPS 2012-0158), available at:  
[https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-12-20\\_Guidelines\\_Leave\\_Flexitime\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-12-20_Guidelines_Leave_Flexitime_EN.pdf),

The organisational part of EBA entrusted with the processing of personal data is EBA Operations Department/Human Resources. The purpose of the processing is to monitor and measure the presence/absence of EBA staff members in the workplace during core and flexi hours. The flexitime monitoring system will neither be used for the evaluation and appraisal of staff, nor for obtaining workload indicators. According to the notification, the processing operation is subject to prior-checking on the basis of article 27.1 of the Regulation, since it involves the use of Radio Frequency Identification (RFID technology). In this specific case, however, the EDPS notes that the processing operation does not seem to present specific risks to the rights and freedom of data subject and therefore does not fall under Article 27.1. Moreover, the processing does not fall under any of the ground listed in Article 27.2. Therefore, the processing of leave and flexitime is **not** subject to prior checking pursuant to Article 27 of the Regulation.

Having said this, the principles of the Regulation apply and EBA, as controller, must ensure compliance with the Regulation. The EDPS has therefore conducted below a brief analysis of the case.

From the notification<sup>2</sup> and the specific privacy notice<sup>3</sup>, it results that the **categories of data** concerned by the aforesaid processing relating to EBA's staff members are the following.

As "identification data":

- first name;
- family name;
- gender;
- EBA personnel number;
- Department/Unit;
- security card (badge) number.

As 'data stored in the flexitime database'<sup>4</sup>:

- name;
- EBA personnel number;
- gender;
- time data (check in and check out times).

In this regard, the EDPS recalls that pursuant to Article 4.1.(c) of the Regulation personal data must be "adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed". The processing of data on the "gender" does not seem to be relevant for the purpose of the notified data processing. The EDPS therefore recommends EBA to discontinue the processing of this category of data.

Concerning the **security measures** required under Article 22 of the Regulation, the notification specifies that: "the personal data are stored in a dedicated part of the EBA server and access is granted only on an individual basis to those with authorised access"; "any physical files are stored in a lockable filing cabinet within the EBA with restricted access rights to HR staff only".

---

<sup>2</sup> At points 6 and 9 of the notification.

<sup>3</sup> At page 2 of the specific privacy notice, "Categories of data".

<sup>4</sup> "Flexitime database", hosted within the EBA datacentre. See, in this regard, at points 10 of the notification.

The EDPS, having thoroughly analysed the information provided on security measures, considers that in order to adequately implement Article 22 of the Regulation, EBA has to adopt (where it has not done so yet) the following organisational and technical measures:

- perform a risk assessment, define the security needs and suitable security controls as well as the residual risks, all of these formally accepted by EBA management<sup>5</sup>;
- perform a gap analysis regarding the approved security needs and controls and the current situation, and develop and implement a security plan as a result;
- define access rights and how they are attributed in the system;
- review access rights regularly and document this review formally;
- maintain logs of transactions, and document what information is contained in them, who has access to them and what use is done of such information;
- document how backups and restores are done and test the actual procedure.

## Conclusion

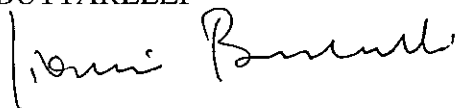
In view of the above, the EDPS considers that there is no reason to believe that the processing of data relating to the "processing on leave and flexitime" at EBA is in breach of the Regulation, provided that EBA:

- 1 - reviews the categories of data undergoing processing (discontinuing the processing of the 'gender' data);
- 2 - adopts the following data security measures:
  - perform a risk assessment, define the security needs and suitable security controls as well as the residual risks, all of these formally accepted by EBA management;
  - perform a gap analysis regarding the approved security needs and controls and the current situation, and develop and implement a security plan as a result;
  - define access rights and how they are attributed in the system;
  - review the access rights regularly and document this review formally;
  - maintain logs of transactions, and document what information is contained in them, who has access to them and what use is done of such information;
  - document how backups and restores are done and to test the actual procedure.

The EDPS expects that EBA implements these recommendations accordingly and will close the case.

Yours Sincerely,

Giovanni BUTTARELLI



Cc: Joseph MIFSUD, Data Protection Officer (DPO), European Banking Authority

---

<sup>5</sup> In this regard, the EDPS remarks that in case of development of a flexitime system using RFID technology a specific risk assessment should be carried out in order to assess the privacy risks; the EU institution or body should take appropriate technical and organisational measures to mitigate the identified risks. See at pages 4 and 17 of the EDPS thematic guidelines concerning the processing of personal data in the area of leave and flexitime.