NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 30/04/2014

CASE NUMBER: 2014-0496

INSTITUTION: EBA - EUROPEAN BANKING AUTHORITY

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER
Adam Farkas Executive Director European Banking Authority - EBA Tower42 (level18) 25 Old Broad Street London EC2N lHQ United Kingdom

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA
EBA Operations Department/Human Resources

3/ NAME OF THE PROCESSING
Processing of leave and flexitime EBA's Temporary Agents (TAs),Contractual Agents (CA s),Seconded National Experts (SNEs)

4/ PURPOSE OR PURPOSES OF THE PROCESSING
In compliance with the EDPS Guidelines concerning the processing of personal data in the area of leave and flexitime, the purpose of the processing of personal data related to TAs, CAs and SNEs is to monitor and measure the presence/absence of staff in the workplace during core and flexi hours in order to manage the attendance of staff more effectively and to provide better balance between private and professional life. This processing operation is subject to prior- checking [Article 27 paragraph 1] of Regulation 45/2001, since it involves RFID similar technology [where

---

[1] OJ L 8, 12.01.2001.

[2] **Please attach all necessary backup documents**

instead of a batch, technology similar to finger prints technology is used] to collect data needed to monitor:

a) The leave and presence of TAs, CAs and SNEs at their workplace during core and flexi hours
   - it applies to TAs, CAs and SNEs to whom the Decision on working hours and flexitime applies
b) The leave and presence of TAs, CAs and SNEs who opted-out or who will opt-out from the application of the Decision on working hours and flexitime.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Data subjects: EBA's Temporary Agents (TAs), Contractual Agents (CAs) and Seconded National Experts (SNEs).

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA
(including, if applicable, special categories of data (Article 10) and/or origin of data)

Identification data:

First Name Family Name Gender
EBA personal number
Unique number (computed by finger print reader which measures the change in electrical conductivity at a number of places across the reader surface and translates these readings into a unique 125 digit number)

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

According to the Article 4(1) letter (c) of Regulation 45/2001, the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and lor further processed.

EBA Staff Member is informed by an EBA internal guideline about the data protection rules for the purpose of processing of leave and flexitime.

The information provided to the data subject contains:
a) The identity of the controller;
b) The purposes of the processing operation for which the data are intended;
c) Recipients of the data;
d) The processes connected with the clock in and clock out;
e) The existence of the right of access to, and the right to rectify the personal data;
f) The legal basis of the processing operation;
g) The time-limits for storing the data;
h) The right to have recourse at any time to the EDPS.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS
(Rights of access, to rectify, to block, to erase, to object)

EBA's Implementing Rules relating to Regulation (EC) No 45/2001 with regards to the processing of personal data lay down the detailed rules pursuant to which a data subject may exercise his/her rights, the procedure for notifying a processing operation and the procedure for obtaining access to the register of processing operations kept by the Data Protection Officer.

Personal data are processed in compliance with Regulation 45/2001 which means that data subjects may exercise their rights of:

Access: EBA Staff has access to their data regarding their presence at workplace via a client application   installed on their desktop computer in order to check flexitime balances/timesheets via inbuilt reports. The user will not be able to insert time information nor modify any clocking times.

Rectification: The data subjects have a right to update or correct their data by sending a request to HR via e-mail (CC the line manager). There is no built in workflows for data change processes.

Blocking: Candidates can ask for blocking their application for a limited period of time, in order for the data controller to verify the accuracy, including the completeness of the data. A data subject who has requested and obtained the blocking of data shall be informed thereof by the data controller, about the blocking and unblocking action.

Erasure: Candidates have a right to obtain from the data controller the erasure of data (cancellation of the application) in the case they opt out from the flexitime regime, or after the data used for flexitime has been materialised in the form of flexi leave

Objection: Candidates have a right to object to the processing of data related to him/her e.g. to opt out from the flexitime regime.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

The flexitime solution has 3 actors:
a) Staff members (TAs, CAs and SNEs). These actors can:
Automatically process the time tracking data through the finger print scanners. This includes only the check-in and check-out times.
Manually verify their flexitime balances and timesheets via in built reports.
Manually request updates on their flexitime balances and timesheets via sending an e-mail to HR (CC their line manager).

b) Admin users (HR). These actors can:
Manually update, on request, time data available in the Flexitime database.
Manually add a new user and update its related data in the Flexitime database (name, EBA number, gender).
Manually generate reports for HR purpose.
Manually extract leave data from the HR system and upload them into the Flexitime database to have the complete view on the staff presence.

c) The Flexitime system, as an actor, is automatically updating the staff flexitime data for the following scenarios:
Auto Clock out if an employee remains clocked in at midnight. In that case the clock out time will be automatically set to the end of core hours.
If a lunch is not booked then the default 30 minutes lunch will be inserted at clock out.
If a lunch of less than 30 minutes is booked then the lunch will be extended to the default 30 minutes lunch.

10/ STORAGE MEDIA OF DATA

All the data is stored within a Database, hosted within the EBA datacentre.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

As in line with the Article 5 letter (a) of Regulation 45/2001, the personal data may be processed if "processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties... or other legal instrument adopted".

Temporary/Contract Agents, SNEs:
Regulation (EU) No 1093/2010 of the European Parliament and the Council of 24 November 2010 establishing EBA;

Temporary/Contract Agents:
Staff Regulations of Officials (SR) and the Conditions of Employment of Other Servants of the European Communities (CEOS), and in particular Art. 55 (SR) in case of permanent staff and Art. 16 (CEOS) for other servants.

SNEs
EBA Management Board Decision EBA DC 017 dated 12 January 2011 on Secondment of National Experts.

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

The access rights to the personal data of data subject are restricted to the EBA HR staff. Recipients within Authority:
HR staff in charge of administration of flexitime;
Heads of Units in charge of the approval of the time sheets of staff under their management responsibility.

Recipients outside Authority, if requested (European Union institutional bodies):
Internal Audit Service of the Commission and the Court of Auditors (for audit purposes); OLAF;
Court of Justice of the European Union;
European Ombudsman;
European Data Protection Supervisor.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Article 4 paragraph l. letter (e) of Regulation 45/2001 states 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.

Data on the flexitime schedule of employees will be retained only during the current calendar year. They will be deleted once the flexi leave days accrued in the previous year have been spent and the transfer of unused days of annual leave to the following year has been closed, and at the latest by the end of March of the following year.

However, in case the calculation of daily working hours is done at the level of the head of department/unit and is based on intermediate statements, the raw data should be destroyed after the validation of the monthly assessment by the head of department/unit taking into account the period during which staff can lodge a complaint, therefore the conservation should not be longer than three months at the latest.

The flexitime monitoring system will not be used as a tool for the evaluation and appraisal of staff nor for obtaining workload indicators.

Flexitime data on staff members who leave the EBA or of those members who opt out of the flexitime scheme shall be deleted within one to two months or immediately after the days of flexi leave are spent, whichever comes first, as there is no justification for retaining them any longer, subject to the rights of the data subjects mentioned in the flexitime rules of the EBA.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS
(Please, specify the time limits for every category, if applicable)

According to the EBA Implementing Rules, Article 12:
If the ground for the request of blocking data is the inaccuracy of the data, as referred in paragraph (1) letter (a), the Data Controller shall immediately block the data for the period necessary for verifying the accuracy and completeness of the data. A data subject who has requested and obtained the blocking of data shall be informed thereof by the Data Controller. He or she shall also be informed of the fact that data are to be unblocked at least 15 working days before they are unblocked. The Data Controller shall take a decision as soon as possible and at the latest within 15 working days of receiving a request for data to be blocked. If the request is accepted it shall be acted upon within 30 working days and the data subject notified thereof. Should the request for blocking be rejected, the Data Controller shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the rejection. In automated filing systems, blocking shall be ensured by technical means. The fact that personal data are blocked shall be indicated in the system in such a way as to make it clear that the data may not be used. Personal data blocked pursuant to this Article shall, with the exception of their storage, only be processed for purposes of proof, or with the consent of the data subject or for the purpose of protecting the rights of third parties.

According to the EBA Implementing Rules, Article 13: The data subject shall have the right to obtain from the Data Controller the erasure of data if the processing thereof is unlawful. If the request is accepted, it shall be acted upon immediately. If the Data Controller deems the request unjustified, he or she shall have 15 working days within which to inform the data subject by means of a letter stating the grounds for the decision.

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES
(If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification)

Not applicable

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Not applicable

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING *(Please describe)*

As Foreseen In:

   Article 27.2.(a)
(Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,)

   Article 27.2.(b)
(Processing operations intended to evaluate personal aspects relating to the data subject,)

   Article 27.2.(c)
(Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,)

Article 27.2.(d)
(Processing operations for the purpose of excluding individuals from a right, benefit or contract)

☒ Other (general concept in Article 27.1)

The processing operation relates to flexitime.

In compliance with the EDPS guidelines concerning the processing of personal data in the area of leave and flexitime we understand that the EBA flexitime system would in principle not be subject to prior-checking due to the fact that:
• it does not explicitly include the evaluation of staff, their conduct, efficiency or
• shall not be processed in the staff appraisal procedure.

A specific feature of the EBA flexitime system is that it will use a technology similar to fingerprints reader for the purpose of measurement of flexitime (clock-in, clock-out). The technology shall ensure that the fingerprints of the data subjects are neither read nor stored and according to the provider nor is the reader a form of optical device.

Instead, the reader technology measures the change in electrical conductivity at a number of places across the reader surface and translates these readings into a unique 125 digit number. It is this unique number alone that is stored in the database for use when the data subject places his/her finger on the reader. According to the technology provider, it shall not be possible to 'reverse engineer' the number into any form of finger pattern or fingerprint.

However, we fully understand the EDPS standpoint included in its guideline on the prior- checking when Radio Frequency Identification (RFID) is used in HR related matters. As mentioned in the EDPS Guidelines concerning the processing of personal data in the area of leave and flexitime, it requires that when RFID is used in HR related matters, such application involves the processing of personal data and thus would according to Article 27 (1) of the Data protection regulation require prior-checking.

17/ COMMENTS

PLACE AND DATE: LONDON, UNITED KINGDOM. 30/04/2014

DATA PROTECTION OFFICER: JOSEPH MIFSUD

INSTITUTION OR BODY: EUROPEAN BANKING AUTHORITY - EBA

1238/2014-0496