(To be filled out in the EDPS' office)
REGISTER NUMBER: 1458

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 05/05/2017

CASE NUMBER: 2017-0466

INSTITUTION: EIOPA

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

FAUSTO PARENTE,
EXECUTIVE DIRECTOR,
EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY – EIOPA
WESTHAFENTOWER
WESTHAFENPLATZ 1
60327 FRANKFURT AM MAIN
GERMANY

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

Philip Codrai -Anti-Fraud Officer

3/ NAME OF THE PROCESSING

Processing of personal data relating to individuals affected by a particular whistleblowing procedure (i.e. the whistleblower – wrongdoer – witness – third party).

4/ PURPOSE OR PURPOSES OF THE PROCESSING

[1] OJ L 8, 12.01.2001.
[2] **Please attach all necessary backup documents**

The purpose of the processing operation is to (on the basis of Articles 22a, 22b and 22c of the Staff Regulations and Articles 11 and the 81 of Conditions of Employment of Other Servants of the European Union ("CEOS")):

- enable reporting of serious irregularities, including fraud, corruption, or other serious professional wrongdoing in the European Insurance and Occupational Authority (EIOPA);
- set out reporting channels for whistleblowers; manage and follow-up whistleblowing reports;
- establish protective measures and prevent potential retaliation against whistleblowers.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Everyone working within EIOPA, (i.e. temporary agents, contract agents, seconded national experts, on-site consultants, temporary workers (interim staff) and trainees) when acting as / being a whistleblower/informant – person under investigation/wrongdoer – witness – third party.

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

The whistleblowing report, as well as the information transmitted to OLAF and the reports that form part of an internal investigation, may contain identification data such as: names, contact details and other personal data.

In particular, the identity of whistleblowers will be treated in confidence, i.e. their name will not be revealed to the persons potentially implicated in the alleged wrongdoings or to any other person without a strict need to know, unless:

a) the whistleblower personally authorises the disclosure of his identity;
b) this is a requirement in any subsequent criminal law proceedings; and/or
c) the whistleblower maliciously makes a false statement.

Depending on the irregularity reported, special categories of data may also be processed such as: information relating to the economic or social behaviour of an individual.

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

All individuals affected by a particular whistleblowing procedure (i.e. the whistleblower – wrongdoer – witness – third party) are *immediately* provided, either in hard copy or by e-mail, with a copy of: (a) the Policy on Whistleblowing pertaining to EIOPA's operations; (b) the privacy statement as an annex to the Policy. Both the Whistleblowing Policy and the privacy statement are also published on InCiderNet, EIOPA's Intranet.

In particular,

- the persons involved in a whistleblowing procedure, and more precisely the whistleblower, are notified of the possible recipients or categories of recipients of his/her personal data;
- where there is substantial risk that notifying the alleged wrongdoer of the processing operation at an early stage would jeopardise the ability of OLAF, local law enforcement or EIOPA to effectively investigate a specific allegation or gather the necessary evidence, such a notification

may be deferred for as long as such risk exists. This will be decided on a case-by-case basis, the reasons for restrictions will be documented and will be made available to the EDPS if requested in the context of a supervision and enforcement action;

- the third parties mentioned in a whistleblowing report are informed only when this does not involve a disproportionate effort for EIOPA. The assessment whether it is disproportionate or not to inform third parties is assessed on a case-by-case basis.

With regard to *external whistleblowers*, every person who enters into a contract with EIOPA is informed (i) that it is possible to raise suspicions of suspected serious irregularities either with EIOPA or OLAF and (ii) that making use of this possibility in good faith will not result in any retaliation, reprisal or other negative action on the part of EIOPA.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

(Rights of access, to rectify, to block, to erase, to object)

EIOPA's Implementing Rules on Data Protection provide for specific rules and procedures, according to which data subjects may exercise their rights of access, rectification, erasure and objection.

In addition to that, as far as the right of *access* and the right of *rectification* are specifically concerned, EIOPA's Policy on Whistleblowing and the privacy statement attached to the latter lay down detailed rules pursuant to which data subjects may request access to or rectification of their personal data found in whistleblowing reports.

When dealing with access requests, EIOPA considers the status of the requester and the current stage of the investigation, as well as the rights of the persons involved in a whistleblowing report, pursuant to Article 20(1)(a) and (c) of Reg. 45/2001.

If access is granted to the personal information of any individual concerned by the whistleblowing, the personal information of third parties (such as informants, whistleblowers or witnesses) is removed from the documents, except in exceptional circumstances, such as when the whistleblower authorises such a disclosure, this is required by any subsequent criminal law proceedings, or the whistleblower maliciously makes a false statement. If a risk remains of third party identification, access might be deferred.

The before-mentioned safeguards are taken into consideration also after the closure of an investigation.

Data subjects may address any request regarding the exercise of their rights to EIOPA's Data Controller (the Executive Director), the DPO, as well as the Anti-Fraud officer, by sending an e-mail to the respective functional mailboxes. A reply is given to such requests normally within 15 working days.

Further to that, and in accordance with Articles 11(1)f(iii) and 12(1)f(iii) of Reg. 45/2001, data subjects may at any time recourse to the EDPS, requesting the protection of their rights.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

The processing of personal data contained in whistleblowing reports may be both manual and automated.

Irrespective of the communication channel used by the whistleblower, a paper file is prepared by the Anti-Fraud officer and stored in a secured cupboard in his room. Electronic documents related to the procedure are stored in a secure area of SharePoint, only available via EIOPA's intranet with access rights only permitted to persons specifically defined by the Appointing Authority on a need-to know basis.

The procedure followed when handling whistleblowing reports is described in detail in EIOPA's Policy on Whistleblowing.

10/ STORAGE MEDIA OF DATA

Physical evidence containing personal information is stored securely in safes or, if any Department does not have safes, in secured cupboards. Electronic evidence is stored in a secure SharePoint area to which access is restricted. The access rights to physical and electronic evidence is reviewed regularly.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Lawfulness

The processing of personal data with regard to whistleblowing procedures falls under Article 5(a) of Reg. 45/2001.

Legal Basis

Articles 22a, 22b and 22c of the Staff Regulations and Articles 11 and 81 of the CEOS.

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

The recipients of the data, strictly on a need-to-know basis, are potentially the following:

- Anti-Fraud Officer;
- HR -where as a consequence of an investigation a disciplinary decision is taken, which has a financial impact or involves a change in the grade, it is forwarded to HR for the adjustment of the salary, HR then requests the salary adjustment to the Paymaster's Office;
- Head of Unit concerned;
- Head of Department concerned;
- Staff members appointed for the internal administrative investigation;
- Executive Director;
- Legal Team and external lawyers;
- OLAF;
- European Court of Auditors (in case of audit);

- EU Courts (in the event of a case being brought before them) and/or European Ombudsman;
- Judicial and other competent national authorities (in case of infringement of national law) - if data are transferred at the request of a national authority, it must establish the 'necessity' for the transfer. If, on the other hand, data are transferred on the sole initiative of EIOPA, it will be for the latter to establish the 'necessity' for the transfer in a reasoned decision.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

The following retention periods will be applied as concerns whistleblowing reports:

- Personal information that is not relevant to the allegations is not further processed;
- If no investigation is initiated or planned (by OLAF, local law enforcement and/or EIOPA), the information will be deleted as soon as possible, and usually within 2 months from the final decision that no investigation will be launched by any party;
- Should any investigation (OLAF, law enforcement, EIOPA) conclude without indicating wrong-doing on the part of the implicated person, personal information will be deleted promptly and usually within 2 months of the completion of the investigation;
- Should any investigation (OLAF, law enforcement, EIOPA) find there to have been wrong-doing on the part of the person implicated and EIOPA adopts remedial measures via an administrative procedure: a) if no appeals are made and there is no clear need to retain the personal data (i.e. no suspicion of links to further cases of fraud), the personal data will be deleted within two months following the conclusion of the procedure; b) should it be deemed that there is a need to further retain the personal data, EIOPA will only do so for a maximum of 2 years, following the completion of any relevant investigation.
- If a case is brought before the EU or the national Courts, personal data will be kept for a period of up to 2 years following the conclusion of the relevant proceedings.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

According to Articles 12 and 13 of EIOPA's Data Protection Implementing Rules:

The data controller shall take a decision 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 rejection.

The data controller shall reply within 15 working days of receiving a request for *erasure*. 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.

Data kept for historical or statistical purposes will be stored on an anonymous basis.

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

It might be necessary to transfer personal data contained in whistleblowing reports to third countries' judicial or other competent authorities. In such cases, it shall be ensured that the transfer will only be performed if the respective national legislation applies a level of protection of personal data that is at least equivalent to Directive 95/46/EC. If this is not the case, the data subject shall be asked to unambiguously give his/her consent.

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)

17/ COMMENTS

N/A

PLACE AND DATE: FRANKFURT, 02/05/2017

DATA PROTECTION OFFICER: CATHERINE COUCKE

INSTITUTION OR BODY: EIOPA