(To be filled out in the EDPS' office)
REGISTER NUMBER: 1409

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 11/11/2016

CASE NUMBER: 2016-1042

INSTITUTION: ESMA

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

EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA)
103, RUE DE GRENELLE,
F-75007 PARIS, FRANCE

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

Ethics Team
Contact: Sophie Vuarlot-Dignac

3/ NAME OF THE PROCESSING

ESMA Whistleblowing Policy for Staff (the "Policy")

4/ PURPOSE OR PURPOSES OF THE PROCESSING

The purpose of the processing 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")):

[1] OJ L 8, 12.01.2001.

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

- enable reporting of serious irregularities, including fraud, corruption, theft, serious violation of rules on public procurement, and serious violations of professional obligations at ESMA.
- set out reporting channels for whistleblowers.
- manage and follow-up whistleblowing reports.
- establish protective measures and act to prevent potential retaliation against whistleblowers.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Everyone working at ESMA, i.e. temporary agents, contract agents, seconded national experts, on-site consultants, temporary workers (interim staff) and trainees.

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 may contain identification data:

- names and surnames.
- contact details.
- other personal information relevant in this processing operation.

In principle, special categories of data should not be included. In particular information that is of no interest or relevance to the possible allegations will not be processed.

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

A general data protection statement will be published on the website of ESMA.

All individuals affected by a particular whistleblowing procedure will be directly provided with a privacy statement as soon as practically possibly. Affected individuals will usually include whistleblowers, witnesses, members of staff and accused persons. (please see Policy, para. 71, attached to this notification)

Whistleblowers will be informed about possible recipients or categories of recipients of the whistleblower's personal information and be provided with a specific privacy statement as soon as practically possible (e.g. by email). (please see Policy, para. 31, attached to this notification)

The staff member implicated, i.e the staff member accused of some wrongdoing, will be also provided with a specific privacy statement as soon as practically possible, e.g. by email. Where there is substantial risk that such notification would jeopardise the ability of ESMA to effectively investigate the allegation or gather the necessary evidence, notification may be deferred as long as such risk exists. Deferral of information shall be decided on a case-by-case basis; the reasons for restrictions shall be documented and shall be made available to the EDPS if requested in the context of a supervision and enforcement action. (please see Policy, paras. 47-49, attached to this notification)

Specific information to witnesses (including a specific privacy statement) shall be provided as soon as practically possible, for instance before they are being interviewed by ESMA. (please see Policy, para. 53, attached to this notification)

Third parties mentioned in a whistleblowing report shall be informed where this does not involve a disproportionate effort for ESMA. the assessment whether it is disproportionate or not to inform third parties will be carried out on a case-by-case basis. (please see Policy, para. 54, attached to this notification)

The privacy statement is attached to this notification.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

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

Without prejudice to point 7 above and to Article 22(a) and 22(b) of the Staff Regulations, staff members are informed of their right to access their personal data and to have inaccurate data rectified.
These rights may be restricted where such restriction constitutes a necessary measure in order to safeguard:

a) the prevention, investigation, detection and prosecution of criminal offences;
b) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
c) the protection of the data subject or of the rights and freedoms of others; and/or
d) the national security, public security or defence of the Member States;
e) a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).

ESMA can restrict the rights of access and rectification through the issuance of a motivated decision by the controller.

In particular with respect to the rights of the data subjects, ESMA follows the measures outlined in its Implementing Rules on Data Protection relating to the Regulation (EC) No 45/2001 with regards to the processing of personal data which 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 (ESMA/2011/MB/57). The implementing rules are attached to this notification.

Any request for access, rectification, blocking and/or erasing personal data may be directed to the relevant Controller (ethics@esma.europa.eu). The Data Protection Officer is involved if an independent advice with respect to compliance to the provisions of Regulation (EC) No 45/2001 is needed.

As regards right of rectification, reference is also made to Article 11(3) of the Implementing measures referred to above which stipulates that "*If a request for rectification is accepted, it shall be acted upon immediately and the data subject notified thereof. Should a request for rectification 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*."

With respect to right to block, according to ESMA's Implementing Rules, requests for blocking shall specify the data to be blocked. 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 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. Blocked personal data 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.

Furthermore when considering access rights, ESMA shall consider the status of the requester and the current stage of the investigation, in compliance with Regulation (EC) No 45/2001. The level and sensitivity of information held (and any associated risks in disclosure) will vary depending on whether the request is made by:

- the person under investigation;
- the whistleblower/informant; or
- a witness;
- third parties.

When access is granted to the personal information of any concerned individual, the personal information of third parties (such as informants, whistleblowers or witnesses) should be removed from the documents, except in exceptional circumstances if the whistleblower authorises such a disclosure, if this is required by any subsequent criminal law proceedings or if the whistleblower maliciously makes a false statement. If a risk remains of third party identification, access should be deferred.
(please see Sections 11.4-11.5 of the Policy attached to this notification)

9/ AUTOMATED / MANUAL PROCESSING OPERATION

After the submission of a whistleblowing report to a manager within ESMA, the manager shall transmit the relevant information to the Executive Director and/or the Ethics Officer. Transmission of such documents shall be done either in a sealed and confidential envelope in person (if the manager receives physical copies) or via email, using password protected files.
The persons originally receiving whistleblowing reports, and any other persons with access to such reports and related documents, are obliged to hand over to the Ethics Officer all copies and related documents.
The Ethics Officer shall transmit to OLAF the whistleblowing report without delay, after having deleted personal information as necessary. (please see section 11.1 of the Policy attached to this notification)

In cases where personal information reported is of no interest or relevance to the investigation, such information will be promptly erased. This is particularly important for special categories of data, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life. For example, in case a whistleblower alleging that one of his or her colleagues has committed a fraudulent activity and in his or her report happens to disclose his colleague's religion and previous health problems, this information shall be deleted immediately or returned to the sender.
In this respect, persons handling whistleblowers' reports will always follow the rules of data quality enshrined in Article 4(1) of Regulation (EC) No 45/2001. Thus, the investigators handling the files

will do a first check of the reports as soon as possible. (please see section 11.3 of the Policy attached to this notification)

10/ STORAGE MEDIA OF DATA

All information included in and related to a whistleblowing report shall be treated as confidential information in accordance with ESMA's Data Classification Policy.
Physical evidence which contains personal information must be stored securely in safes or, if any Department does not have safes, in secured cupboards. Electronic evidence must be stored in encrypted files to which access shall be restricted only to authorised persons in charge of dealing with this processing operation. The access rights to physical and electronic evidence shall be reviewed regularly. Furthermore, access to whistleblowing reports (either in electronic or paper form) will be monitored through an access log. (see section 11.2 of the Policy)

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

The processing of data with regard to whistleblowing procedures is an obligation in accordance with Articles 22a, 22b and 22c of the Staff Regulations, Articles 11 and 81 CEOS.

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

Strictly on a need-to-know basis:
Ethics Officers
HR
Head of Unit concerned
Head of Department concerned
Officers appointed for the internal administrative investigation
Executive Director

Personal data may be transmitted to OLAF as part of the whistleblowing report, though the Ethics Officer transmits the whistleblowing report to OLAF, after having deleted personal information, which is not necessary for the assessment of the case.

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.
If a staff member contests an Executive Director's decision, the disciplinary file may be referred to the Court of Justice of the European Union.
It may happen that data are transferred to the competent national authorities such as a national Court where there is an infringement of national law. In such instances, 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 ESMA, 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

If no investigation is initiated, the information should be deleted as soon as possible.

When an internal investigation is opened, the personal data can be kept as long as the investigation is ongoing. In any case, personal information should be deleted promptly and usually within two months of the completion of the investigation, since it concerns sensitive information.
After the transferal of the whistleblowing report to OLAF, ESMA shall also carefully follow what actions OLAF takes. If OLAF starts an investigation, it is not necessary for ESMA to keep the information for a longer period, therefore ESMA will destroy the personal data promptly and usually within two months. In case OLAF decides not to start an investigation, the information should be deleted without delay.
(see section 14 of the Policy)

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

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 the 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.
Please see Articles 12 and 13 of ESMA/2011/MB/57, Decision of the Management Board on Implementing rules relating to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (as amended) (attached to this notification).
(Please, specify the time limits for every category, if applicable)

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.

No personal data will be stored for statistical purposes.

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

Transfers of data to third countries or international organisations are not envisaged. Nevertheless, should the need for such transfers of data arise, all transfers will be assessed on a case-by-case basis. In particular, data will be transferred only when it is necessary for the legitimate performance of

tasks covered by the competence of the recipient. Furthermore, all transfers of data are subject to the requirements of Directive 95/46/EC. (Policy, para. 68)

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

ESMA will process data related to (suspected) offences, eventually transmit it to OLAF and may conduct an internal investigation regarding the accused persons' conduct.

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

This notification constitutes a prior-checking notification pursuant to Article 27 of Regulation (EC) No 45/2001.

PLACE AND DATE:

PARIS, 11 NOVEMBER 2016

DATA PROTECTION OFFICER:

SOPHIE VUARLOT-DIGNAC

INSTITUTION OR BODY:

EUROPEAN SECURITIES AND MARKETS AUTHORITY (ESMA)