(To be filled out in the EDPS' office)
REGISTER NUMBER: 1439

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 28/02/2017

CASE NUMBER: 2017-0243

INSTITUTION: FRONTEX

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

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

The European Border and Coast Guard Agency (Frontex)
Plac Europejski 6
00-844 Warsaw
Poland

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

Head of the Legal Affairs Unit (and his/her designate)

3/ NAME OF THE PROCESSING

Whistleblowing Procedure

4/ PURPOSE OR PURPOSES OF THE PROCESSING

Under Article 22a, b and c of the Staff Regulations, a staff member has a duty to report serious wrongdoing. This report is called an internal report. It will contain personal data.

Frontex specifically needs to comply with Article 22c of the Staff Regulations this states:

"In accordance with Articles 24 and 90, each institution shall put in place a procedure for the handling of complaints made by officials concerning the way in which they were treated after or in consequence of the fulfilment by them of their obligations under Article 22a or 22b. The institution concerned shall ensure that such complaints are handled confidentially and, where warranted by the circumstances, before the expiry of the deadlines set out in Article 90.
The appointing authority of each institution shall lay down internal rules on inter alia:

[1] OJ L 8, 12.01.2001 ('THE DATA PROTECTION REGULATION')
[2] Please attach all necessary backup documents

— the provision to officials referred to in Article 22a(1) or Article 22b of information on the handling of the matters reported by them,
— the protection of the legitimate interests of those officials and of their privacy, and
— the procedure for the handling of complaints referred to in the first paragraph of this article."

Frontex has drafted rules concerning whistleblowing (Annex I). The European Data Protection Supervisor is asked to refer to those draft rules.

they cover:

- definitions
- procedure (including making an internal report, reporting to OLAF, making a further report by the whistleblower (a so-called external report) further measures to be taken by senior management, the conclusion of the procedure, and an undertaking by senior management to handle complaints confidentially and within deadlines set in Article 90 Staff Regulations)
- contacts (i.e. to check the scope of the rules with either the Director of Corporate Governance or the Head of Legal Affairs Unit)
- protection for whistleblowers (including protection against retaliation, confidentiality and anonymity, possibility for the whistleblower to moved to another agency unit/entity, no adverse consequences for appraisal and promotion, the limits of such protection)
- protection for persons concerned (including information that is to be given to them, and protection for them e.g. of their identity)
- protection of other data subjects (including information that is to be given witnesses and third parties)
- right of access to personal data (for whistleblowers and others involved in the whistleblowing procedure – which includes a right to rectification)
- conservation rules for personal data (including deletion within four months of the conclusion of the procedure)
- entry into force (including repeal of the Frontex internal document known as 'reporting suspected improprieties')

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Frontex staff members, witnesses and third parties involved in the whistleblowing procedure.

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

Data likely to be found in the course of a whistleblowing procedure. These documents may contain names, contact details and other personal data. Prohibition in principle on processing special categories of data according to Article 10(1) of the Data Protection Regulation[3].

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

Information to data subjects is set out *inter alia* in Articles 15, 17 and 18 of the rules. Specifically they include:

The person concerned must be informed at the earliest possible stage about the content of the internal report, unless providing her/him with specific information might need to be deferred.

Necessary information to witnesses must be provided as soon as practically possible.

Third parties referred to in an internal report must be provided with necessary information as soon as practically possible, unless such information would involve a disproportionate effort.

[3] In accordance with paragraph 11 of the EDPS Guidelines on Processing Personal Information within a whistleblowing procedure.

Further information is included within the rules and the privacy statement (Annex I and II).

A copy of both Annex I and II is to be given to those staff members who make an internal report, and new staff members on the commencement of employment at Frontex. It is also to be given to all current employees, individuals concerned in the alleged serious wrongdoing, together with all witnesses and third parties in a whistleblowing procedure.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

Data subjects are informed of their rights and of how to exercise their rights via the rules concerning whistleblowing and the privacy statement.
Requests for access from data subjects are dealt with under Article 19 of the rules (Right to access). Data subjects also have a right of rectification of any incomplete or inaccurate data without delay.
In cases where it is necessary to postpone informing the person concerned about the opening of an administrative inquiry into issues raised by a whistleblower so as not to jeopardise the conduct of this inquiry, the reasons for doing so will be explained in a note to be added to the file. If it is necessary, for the same reason, to limit the right of the person concerned to access or rectify his or her personal data, the reasons for this limitation will be explained in the decision on such a request.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Automated and manual.

The processing operation is both. Irrespective of the communication channel used by the person, a paper file is prepared by the Legal Affairs Unit, and stored in a safe of the Legal Affairs Unit. Electronic documents related to the procedure are stored on a network drive accessible only to the Head of Legal Affairs Unit (and his/her designate). In order to decide on the appropriate course of action, the Executive Director, the Deputy Executive Director, the Director of Corporate Governance, the Head of Legal Affairs Unit (or his/her designate), the Head of Unit concerned may request a paper copy of the file for consultation. Recipients will be reminded to destroy all copies and related documents. Consultation by any other authorised person shall take place in the office of the Head of Legal Affairs Unit.

The personal data is used solely for the purpose for which it was provided, namely the whistleblowing procedure and any subsequent procedures directly triggered by it, such as disciplinary procedures.

10/ STORAGE MEDIA OF DATA

Files related to the whistleblowing procedure are to be stored securely. Data stored in paper files is kept in a safe located in the office of the Head of Legal Affairs Unit. Electronic files are stored on a network drive of the Legal Affairs Unit with restricted access.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Article 22c of the Staff Regulations (is the main legal basis).
Secondarily, it is Article 22a, 22b, 24 and 90.
The Management Board's Decision on rules concerning whistleblowing.

The processing operation is lawful on the basis of Article 5(a) of the Data Protection Regulation (the processing is necessary for the performance of a task carried out in the public interest, namely the management and functioning of the institution).

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

Executive Director, Deputy Executive Director, Director of Corporate Governance, the Head of Unit concerned, the Head of Legal Affairs Unit (and his/her designate).

Disciplinary board members, the European Court of Auditors, EU courts, the EDPS, OLAF and national judicial authorities.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

- Files which do not lead to the opening of an inquiry ('non-case') will be destroyed immediately on the date on which the Executive Director decides to close the file without follow up.
- However, files on the basis of which an administrative enquiry or disciplinary procedure are opened (even if they are non-case) should be kept in line with the retention periods provided for within the Frontex Disciplinary Procedure.
- Conservation: personal data processed as part of the whistleblowing procedure is to be deleted within four months of its conclusion according to Article 7 of the rules.
-Where the information in the internal report is not within the scope of these rules, then personal data contained therein is to be deleted within four months after the Line Manager informs the whistleblower about the outcome of the evaluation of the report (made under Article 3, 4 and 5) pursuant to Article 7.

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

The Legal Affairs Unit is accountable for litigation/pre-litigation: such cases present a high litigation risk and the Head of Legal Affairs would like to keep a longer retention period. An overriding possibility to retain for up to 6 months following the end of the procedure in Article 7: (i) Only the Head of Legal Affairs Unit (and his/her designate) would have access; (ii) only where it is justified by the need to process a potential court case.
(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.

N/A

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

N/A

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

PROCESSING OF DATA THROUGHOUT THE WHISTLEBLOWING PROCEDURE MAY INVOLVE ALL PROVISIONS IN YELLOW BELOW.

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,

17/ COMMENTS

Enclosure:
Annex I: draft rules
Annex II: draft privacy statement

In drafting the rules, privacy statement and this notification for prior checking we have abided by advice given by the EDPS to other EU institutions/agencies to the greatest extent possible.
This is a true prior-notification. Data processing did not start yet since no respective MB-Decision has been adopted yet.

PLACE AND DATE: WARSAW, 10 JANUARY 2017
DATA PROTECTION OFFICER: ANDRZEJ GRAS
INSTITUTION OR BODY: FRONTEX