(To be filled out in the EDPS' office)
REGISTER NUMBER: 1412

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 16/11/2017

CASE NUMBER: 2016-1056

INSTITUTION: EUIPO

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

INFORMATION TO BE GIVEN

1/ NAME AND ADDRESS OF THE CONTROLLER

SUSANA PEREZ FERRERAS (DIRECTOR OF THE HUMAN RESOURCES DEPARTMENT) - HRD
European Union Intellectual Property Office
Avenida de Europa, 4, E-03008 Alicante, Spain

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

Human Resources Department, EUIPO

3/ NAME OF THE PROCESSING

Procedure for reporting serious irregularities and wrongdoings - "Whistleblowing"

4/ PURPOSE OR PURPOSES OF THE PROCESSING

The implementation of the procedures provided for in Articles 22a, 22b and 22c of Staff Regulations (SR) as well as Articles 11 and 81 of the Conditions of Employment of other servants (CEOS) provide for the rules on Whistleblowing.

The purpose of this data processing is to enable EUIPO's staff members or whistleblowers who are not members of the Office's staff, such as consultants, contractors, etc. to report potential illegal activity, including fraud or corruption, detrimental to the interests of the EU, or other serious professional irregularities at EUIPO.
The processing operation requires establishing reporting channels for whistleblowers, managing and following-up reports. It ensures that staff members who report serious potential wrongdoings or concerns in

[1] OJ L 8, 12.01.2001.

good faith are treated with the utmost confidentiality and greatest degree of protection against any retaliation as a result of their whistleblowing.

Whistleblowing channels will not be used when staff may wish to exercise their statutory rights i.e. by lodging a request or complaint to the appointing authority under article 90 of the SR or for harassment claims and personal disagreements when staff may address themselves to the HRD.

Whistleblowers may proceed anonymously, but they will be encouraged to mention their identity to allow their effective protection against retaliation. This will also allow a better management of the file if further information would be necessary.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

EUIPO's staff members.

Seconded National Experts, trainees, interim agents, contracting parties, subcontractors and their employees can blow the whistle. These persons can also be affected because they might be witnesses, accused persons or third parties mentioned in the whistleblowing report.

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA

(including, if applicable, special categories of data (Article 10) and/or origin of data).

The personal data processed is the data contained in the report submitted by the whistleblower and any subsequent document drawn up in response to that initial report:
These documents may contain:

- identification of the data subject (names, other personal data);
- contact details;
- evaluation of personal aspects of the data subject (e.g.: conduct, activities, working relations and economic or social behaviour);
- administrative data (grade, position and responsibilities, department/service);
- documents produced at work (emails, notes, correspondence, etc.);
- identification of whistleblowers, witnesses, third parties (members of staff or others that are merely quoted) and the person(s) against whom the allegations have been made.

In principle, special categories of data (Article 10 of Regulation 45/2001) should not be included. In any event, the HRD Director should ensure that staff members, and in particular, investigators handling information on potential fraud and other serious wrongdoings, are aware of the following: Data and in particular, special categories of data that clearly are not relevant for the purposes of investigating fraud, corruption or other serious wrongdoings through the whistleblowing procedure, should not be further processed and should be erased. This requires carrying out an initial assessment of the information provided in the whistleblower´s report as soon as possible.

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

Staff members are informed by the information available/disseminated through the relevant page of the HRD in the Intranet and particularly by the specific privacy statement (Annex 4).
Also, all persons affected (whistleblowers, witnesses, third parties, accused person(s)) by a particular whistleblowing procedure will be directly provided with the specific privacy statement as soon as practically possible. In most cases, informing the accused person at an early stage may be detrimental to the investigation and specific information might need to be deferred (see Article 20(1)(a) of Regulation 45/2001). Deferral of information will be decided on a case by case basis where there is substantial risk that such notification would jeopardise the process and possible future OLAF investigation. In that case, the information will be provided to the data subject at a later stage. The reasons for the deferral are to be documented.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

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

The rights of the persons concerned are guaranteed by the rules provided for in Article 12 – *exercise of data subjects' rights* - of the EUIPO's Administrative Decision Nr. 08-40 of 13 November 2008 adopting the implementing rules regarding Regulation (EC) No 45/2001.

Without prejudice to point 7 above and to Article 22(a) and 22(b) of the Staff Regulations, the staff member is informed of his right of access to various documents concerning him in the event of a disciplinary proceeding.

The staff member can request access and copies of all documents directly related to the allegations made against him, except documents for which disclosure could jeopardize the privacy and right to data protection of third parties, or the legitimate guarantees given to the "whistle-blowers". When disclosure of the full document is not possible for the reasons explained above, the staff member should have access, whenever it is possible, to at least an abridged version or excerpts of the documents.

The staff member has the right to rectification in order to ensure completeness of his disciplinary file. This may be done, inter alia, by allowing him to add his comments.

Any exceptions to the right of access of staff members should be strictly applied in light of necessity and they should be balanced in relation to the right of defence.

Particularly, in the case of "whistle-blowers", informants or witnesses, any restriction to the right of access should not be allowed unless such restriction is made in accordance with Article 20 of the Data Protection Regulation. In any case, the identity of "whistle-blowers" should be kept confidential in as much as this would not contravene national rules regarding judicial procedures.

When replying to data subjects' access request, EUIPO should bear in mind that personal data does not only relate to information about an individual's private life in a strict sense, but also to information regarding an individual's activities, such as his or her working relations and economic or social behaviour. Information can relate to an individual because of its content, the purpose of its use and the result of its use.

A case by case assessment of each individual case and document is to be carried out and the status of the requester and the current stage of the investigation are to be taken into account when considering data subjects´ rights.

9/ AUTOMATED / MANUAL PROCESSING OPERATION
(Description of the processing operations)

The procedure for dealing with whistleblowing is based on the rules of the SR and CEOS and on the European Commission Guidelines on Whistleblowing which are applied by analogy to EUIPO.

The processing of the operation is manual. Irrespective of the communication channel used by the whistle-blower, a paper file is prepared by HRD, and stored in a secured cupboard in HRD. Electronic documents related to the procedure are stored on a ShareDOX folder accessible only to authorised staff members of HRD and are password protected.

In order to decide of the appropriate course of action, the Executive Director and the Director concerned may request a paper copy of the file for consultation. All paper copies made by HRD staff are attributed a registration number. The instruction to return the paper copy to HRD and not to make any further copies is written on the paper copy. Upon return of the paper copy, HRD will destroy the copy. Consultation by any other authorised person shall take place in the premises of HRD.

HRD staff keeps a register of all paper copies given out, indicating the registration number of the copy, the name and function of the person who received a copy, date of delivery, return date and destruction date. HRD staff also keeps a register of all consultations taking place in the premises of HRD, indicating the name and function of the person consulting and the date.

The Director of HRD is responsible for granting and reviewing the access to the paper and electronic files, in accordance with the procedures described in this notification. In each case, before providing access to the files, HRD staff actively checks with the Director of HRD whether access could be granted to the person in question. Concerning the access to electronic documents stored on the ShareDOX folder, the Director of HRD annually receives a report from DTD (Digital Transformation Department) on access rights to the ShareDOX folder. The Director of HRD requests necessary changes to access rights, if any, to DTD.
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

Data related to Whistleblowing has restricted access rights. Only authorized staff members working in these files have access to data on a strict need to know basis, only when the information is absolutely necessary for the purpose of the investigation.
Electronic documents are password protected. All records are held securely so as to safeguard the utmost confidentiality and privacy of the data therein.
Paper documents are stored in secure cupboards in the HRD.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Legal basis

- Article 5(a) of Regulation 45/2001;
- Articles 22a, 22b and 22c of the SR and Articles 11 and 81 of the CEOS;
- European Commission's Guidelines on Whistleblowing applied by analogy to EUIPO;
- Communication from the Executive Director to staff for reporting serious irregularities "whistleblowing".

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

Access to data may be granted on a strict need to know basis considering the status of the requester and the current stage of the investigation to the following persons:

- an experienced staff member appointed to offer guidance and support to the whistleblower;
- the hierarchical superior concerned, the Director of the HRD, the Executive Director and the Deputy Executive Director;
- on a need to know basis, recipients could include Directors, Deputy Directors, the President of the Boards of Appeal, and a limited number of authorized staff members of the Legal Service / HRD/ Digital Transformation Department (IT Services) / Infrastructure and Building Department (Security Services) authorized of handling the file, as well as any other staff member responsible for the follow-up action that are to be designed by the Executive Director;
- a limited number of staff members of HRD designated to work in the case;
- the person against whom the allegation has been made, the whistleblower, a witness, third parties) and his/her advisers.

Other recipients on a strict need to know basis:
- authorized staff members of the internal Audit Service, Court of Auditors, Data Protection Officer, European Data Protection Supervisor, OLAF, Court of Justice in case of complaints, other EU Courts and national judicial authorities.

As option of last resort, the staff member who reports serious irregularities can also disclose the data to the President of either of the Council, the European Commission, the European Parliament or the European Court of Auditors or to the European Ombudsman.

Access may also be allowed on a temporary and restricted basis to IT-technicians for compilation of necessary data requested for the investigation.

A declaration of confidentiality/secrecy will be signed by all persons working in whistleblowing files.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Not relevant information:
If special categories of data that clearly are no relevant for the purposes of investigating fraud, corruption or other serious irregularities are collected through the whistleblowing procedure, they will be deleted and not further processed. Staff members in charge of reading and assessing reports will be made aware of this (Article 4(1) of the Regulation).

Cases not relevant to an OLAF investigation or out of the scope of whistleblowing procedures:
If after an initial assessment it is clear that the case should not be referred to OLAF / or cannot be treated within the whistleblowing procedure, the report and personal data will be deleted within 2 months after the conclusion of the preliminary assessment or referred to the right channel (e.g.: alleged harassment).

Relevant information for an OLAF investigation: 15 years

Investigation closed by OLAF without follow-up: 8 years

Case closed by OLAF without investigation: within 2 months after closure of the case

Files on the basis of which an administrative enquiry or disciplinary procedure is opened or files which are reported to OLAF, should be kept in line with the retention periods foreseen for those files.

At the end of the retention period, data are destroyed.

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)

Legitimated requests accepted by the controller are treated immediately and in any case not later than 15 days from the date of receipt of the request.

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

Requirements for transferring data must be assessed on a case by case basis. Personal information will be transferred only when necessary for the legitimate performance of tasks covered by the competence of the recipient. Different obligations will apply depending whether the recipients are EU institutions (e.g.: transfer of data to OLAF) or someone subject to Directive 95/46 (e.g.: national court or other type of recipient).

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

YES.

AS FORESEEN IN: REGULATION 45/2001 & RECOMMENDED IN THE EDPS GUIDELINES WHISTLEBLOWING

17/ COMMENTS
Documents submitted as attachments:

Annex 1 – European Commission's Guidelines on Whistleblowing applied by analogy to EUIPO
Annex 2 – Communication from the Executive Director to EUIPO's staff members
Annex 3 – Data Protection Privacy Statement

PLACE AND DATE: ALICANTE, 16 NOVEMBER 2016

DATA PROTECTION OFFICER: PEDRO DUARTE GUIMARÃES

INSTITUTION OR BODY: EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE