To be filled out in the EDPS' office

REGISTER NUMBER: **1450**

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 27/03/2017

Case number: 2017-0350

Institution: EUIPO

Legal basis: **Article 27-5 of the regulation CE 45/2001**(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN (2)

(2) Please attach all necessary backup documents

1/ Name and adress of the controller: **EUIPO, 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: Infrastructures and Buildings Department, Common Services, Security Services (contact person Head, Safety, Health & Securty , currently Jean-Louis Dominguez)

Processors: EUIPO will use the Security Service Provider (SSP), duly contracted (level 1 checks); all connection will go over SSL, this is based on a SHA256 bit encryption. This will ensure shifting administrative workload from EUIPO to the back office of contractors and simultaneously reduce complexity for contractor to get possession of an access badge; enforcing that all contractors do comply and stay compliant with EUIPO regulations regarding access to its premises; enforcing that all contractors do comply and stay compliant with EUIPO policies regarding employment of contractors; establishing and maintaining an up to date access control database; implementing ID verification of contractor during the issuing process of access badges, etc. The SSP have the possibility to subcontracts part of the service to a consulting firm specialized in risk management, business intelligence and strategic security (level 2 checks). For level 2, the above objectives are still relevant but a more thorough verification of credentials will be carried out by the security service provider or a specialised company duly subcontracted. Level 2 will not be mandatory for all positions contracted. Level 3 will be used to perfrom extended verification, as required, due to the risk level and duties performed by the external staff, for instance to access restricted areas. The Seconded National Expert will issue request through the official channels at National level (Spaniards) and International level (Foreigners). The data processing will take place within the EU (Holland/Spain).

Currently, the current contract of Security Service Provider is hold by the company Nsecure (framework contract, maximum duration - 5 years, renewed annualy).
This contract (attached as an annex) includes a clause on data protection (page 40/42, 41/42, 8/23).

3/ Name of the processing: **Security Verification of External Resources**

4/ Purpose or purposes of the processing: The EUIPO makes extensive use of external staff (external resources) deployed by private companies providing services (services providers). The current percentage of external resources is approximately 50% (February 2016 data: externals - 959, internals-928) and around 400 new external staff start working at the office each year (2015 data: 484 externals joined the office, among which 411 are completely new and 73 have worked here in previous occasions). External resources could be provided with access to EUIPO premises on regular basis to offer services such as cleaning, security or maintenance. It could also be a contractor, specifically hired by the IT Department, granted with special access right to restricted areas. All those mentioned above could unlawfully get hold, modify, tamper, or steal valuable information.
The absence of a sufficient background screening could severely detrimental to the liability of the EUIPO vis-à-vis of its clients which, thus, would directly impact its core business and irrevocably damage its reputation. As a result, the implementation of a thorough background screening is deemed as critical for the EUIPO to secure the recruitment of person whom could result being a valuable asset for the organisation by service providers.

Pre-employment screening is the foundation of good personnel security. It seeks to verify the credentials of those the EUIPO is seeking to grant access to the premises and information.

A) Benefits of pre-employment check for the detection of:
• involvement in illegal activities;
• unspent criminal convictions relevant to the role, particularly if not volunteered by the applicant and only revealed by other checks;
• false or unsubstantiated claims on the CV or application form;
• unsubstantiated qualifications;
• unexplained gaps in employment history;
• adverse references;
• questionable documentation e.g. lack of supporting paperwork or concern that documents are not genuine;
• evasiveness or unwillingness to provide information on the part of the candidate.

C) The implementation of screening procedure for externals will allow:
• To verify personal information of all external resources prior to the badge handling process,
• To enable for both EUIPO and the service provider an efficient and transparent verification process,

5/ Description of the category or categories of data subjects: **It is compulsory for all external staff of the EUIPO required by their duties to access the Office premises to go through the security verification clearance before the access is granted.**

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: full name, date and place of birth, nationality
Special categories: data related to criminal records
Data regarding health conditions will not be part of the investigation; neither - family background.

In order to perform the vetting process, the **following documents will be requested for each candidate**:

• valid identity documentation;
• good behaviour certificate or criminal records;
• right of abode and work, when required;
• security declaration – confidentiality;
• declaration of authenticity;
• education qualifications;
• professional qualifications;
• professional references.

For some of them the template forms are available (annexed).

7/ Information to be given to data subjects: **The service providers of the EUIPO will be informed about new security procedure to be applied and about the related requirements. Consequently, the upload of personal data and the reference to individual rights realted to privacy and personal data protection will be shared. Each service provider will have to inform any potential candidate about the process and about their respective rights to privacy and personal data protection. The same information will be duplicated on the portal via a data protection statement.**

8/ Procedures to grant rights of data subjects: *(rights of access, to rectify, to block, to erase, to object)*

For access: could be done if email is sent to the functional mailbox, also EUIPO are looking at the possibility to have automated email with the link which could be sent to the applicant through which he/she could verify that the data provided is accurate.

For rectification: could be done if email is sent to the functional mailbox, also EUIPO are looking at the possibility to have automated email with the link which could be sent to the applicant through which he/she could verify that the data provided is accurate and if not ok, could rectify within screening period.

For blocking: could be done if email is sent to the functional mailbox, also EUIPO are looking at the possibility when applicant will receive an automated mail that the right was ensured.

For objecting: The candidate could object the procedure under which the data is processed and the exact manner of processing, nevertheless, he/she will be advised that this will prevent the fulfilling of the screening procedure and thus, accessing the Office premises will not be granted.

For erasure: Erasure of the documents will be done as per specified in the **annexed table**. If the data subject desires to verify that his/her data was erased he/she could send an email to the functional mailbox; EUIPO are looking at the possibility to have automated mail with the link which could be sent to the applicant when the

9/ Automated / Manual processing operation: The **security service provider will provide portal (automated)** which will be used for:

-submitting documents by the service providers
-checking the documents by the security service providers
-authorizing/vetting candidates by the security service providers
-checking the status of candidates documents by the service providers
-verifying the work performed by the security service providers by EUIPO (quality control checks)
-verifying that the original ID provided corresponds to what was submitted through the portal by the

10/ Storage media of data: **all the documents will be uploaded through the portal therefore no paper documents are stored at all. The portal will be hosted by the security service provider, the collected personal data are stored in servers located in secure data centers.**

11/ Legal basis and lawfulness of the processing operation

Article 5(a) of Regulation 45/2001 (“processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof […]”)

There are several internal documents which support legal basis for processing (their copies are attached):

- QSD-0029- Work Instruction Control of Guard Services. Version 5.5 –14/04/2016
- Service Level Agreement: Allocation of Access Cards & Parking Permits. Version 1.1 –28/06/2016
- T-0080-Access Card informacion. Version 1.0 - 08/09/2014
-Strategic plan 2020 project brief "Increasing the security levels"
- the Note to the European Data Protection Superivor: "Security Verification of external resources".

12/ The recipients or categories of recipient to whom the data might be disclosed: **Security services/Common service/Infrastructure and Buildings/EUIPO as controller of the process will have access to data. The security service provider as the processor of the data will have also access to it. The service provider will be informed if candidate is authorised/vetted to enter the Office premises. In case there is a legal investigation then legal authorities (police, court, etc.) could have access to the data.**

13/ Retention policy of (categories of) personal data

TIME LIMITS

For access: please refer to the table "Documents required for different threat levels" for the complete information on each document.

For rectification: please refer to the table "Documents required for different threat levels" for the complete information on each document.

13 a/ Time limits for blocking and erasure of the different categories of data
(on justified legitimate request from the data subject)

For blocking: please refer to the table "Documents required for different threat levels" for the complete information on each document.

For erasure: please refer to the table "Documents required for different threat levels" for the complete

14/ Historical, statistical or scientific purposes:

Only the documents of selected candidates will be retained - each particular document has its own retention period, more details could be seen in "Documents required for different threat levels". Non-selected candidates´ documents are deleted after 3 months, period during whilch any action against the EUIPO can be initiated in relation with candidate refusal. In such case, the EUIPO will store the documents untill two years after the end of the action and then automatically erase them. For the statistical/historical purposes the data will be stored however in a fully unanomised way & no personal

15/ Proposed transfers of data to third countries or international organisations: **n/a**

Processing operations intended to evaluate personal aspects and suspected offences, offences, criminal convictions relating to the data subjects in order to mitigate risks at EUIPO regarding possible attacks and improve physical security at the Office.

AS FORESEEN IN:

X Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

X 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

PLACE AND DATE: **Alicante, 28/03/2017**

DATA PROTECTION OFFICER: **Pedro Duarte Guimarães**

INSTITUTION OR BODY: **EUIPO**