To be filled out in the EDPS' office

REGISTER NUMBER: 1403

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 30/09/2016
Case number: 2016-0894
Institution: EEAS
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

Controller:
European External Action Service (EEAS)

Directorate/Division responsible for managing the personal data processing operation:
Mr Gianmarco Di Vita
Director General Budget and Administration, EEAS.BA

Delegated Contact Person/Team:
Security Investigations Sector (Head of Sector: Carine Hanssens)
EEAS.BA.IBS.3 HQ Security & EEAS Security Policy

2/ Organisational parts of the institution or body entrusted with the processing of personal data

EEAS.BA.IBS.3 HQ Security & EEAS Security Policy

3/ Name of the processing

Security verifications on employees of external contractors requiring access to EU Institutions & Bodies

4/ Purpose or purposes of the processing

In accordance with the Memorandum of Understanding between the government of the Kingdom of Belgium and the EEAS (and other EU Institutions and Bodies, namely the European Parliament, European Council, Council of the European Union, European Commission, European External Action Service, European Economic and Social Committee, Committee of the Regions of the European Union, European Defence Agency) personal data from employees of external contractors will be processed as follows:

PURPOSE of the Processing

In order to safeguard the security interests of EU institutions and bodies pursuant to the arrangement of 31 December 2004 and the Article 4(3) of the Treaty on European Union and Article 18 of the Protocol on the Privileges and Immunities of the European Union of 8 April 1965, the Belgian Authorities will facilitate the implementation of security verifications consisting of the consultation and evaluation of data transmitted by the intelligence and security services as well as of judicial data transmitted by the police services, if appropriate. The security verification requests will be managed by the competent Administrative Authority of the Belgian State (SPF Affaires étrangères, Commerce extérieur et Coopération au développement - Direction Protocol, Rue des Petits Carmes 15, 1000 Bruxelles). Security certificates will be issued or withdrawn by the Belgian National Security Authority.

Rationale

On request of the European Institutions and Bodies, the Administrative Authority agreed that the access to EU premises for employees of external contractors would benefit from security verification as determined by section 22quinquies of the Act of 11 December 1998. This verification shall be carried out by the authority referred to in section 15, subsection 1 of the same Act.

The permission by the Administrative Authority is legally justified as per the grounds mentioned in article 22quinquies of the Act of 11 December 1998. Inappropriate access to EU premises could cause damage to the protection of the external security of the State and the international relations of Belgium, in particular if the physical security or the reputation of the European Institutions and Bodies were harmed.

5/ Description of the category or categories of data subjects

Data are processed from the following individuals or group of people:

- Employees of concerned EU Institutions and Bodies' external contractors
- The parties of the Memorandum of Understanding, i.e. concerned EU Institutions and Bodies as well as the Government of the Kingdom of Belgium who acknowledge that the security advice is based on information available to the Belgian security authorities as described in Point 3.5* of the Memorandum of Understanding. Given the legal timeframe provided by the Act of 11 December 1998, information on persons who do not reside in Belgium or who are not of Belgian nationality will generally be limited to internationally available data from sources such as the Schengen Information System or Interpol.

*MoU Point 3.5 The security verification consists of the consultation and evaluation of the data referred to in Article 22sexies of the Act of 11 December 1998 on classification and security clearances, security certificates and security advices, from the information collected in the context of the Act of 30 November 1998 on regulation of the intelligence and security services.

6/ Description of the data or categories of data*(including, if applicable, special categories of data (article 10) and/or origin of data)*

Data (category or type of data) processed may be the following:

- Last name, first name, address, e-mail address, date and place of birth, nationality, national number or ID number if the employee has no BE nationality, the employer (details of contractor), the function of the employee of the external contractor, place of employment, photo; contractor's contract number and coordinates. Data will be managed through a datasheet (e.g. excel sheet) as agreed by the parties of the MoU.

- Outcome of the security verification: The EEAS will only receive a positive or negative outcome. The employee will be informed by the Administrative Authority in a well-reasoned letter in case the security advice is negative.

7/ Information to be given to data subjects

A Privacy Statement linked to the present Notification contains information provided to the Data Subject(s).

The aforementioned Privacy Statement is to be provided to the external contractors of the concerned EU institutions and Bodies for making it available to data subjects, i.e. employees requesting security verifications, at the time of the verification request ('Demande de vérification ' / 'Verzoek om een verificatie').

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

Data subjects have the right to access their personal data processed by the EEAS and the right to correct any inaccurate or incomplete personal data, as well as to request the removal of unlawful personal data, which will be implemented within 10 working days after the request has been deemed legitimate. If the data subject has any queries concerning the processing of his/her personal data, s/he may address them to the data controller at the following functional mailbox: EEAS SECURITY VERIFICATIONS <eeas-security-verifications@eeas.europa.eu>

Personal data processed for the purpose of the present security verification implemented by the Administrative Authority of the Belgian State is handled and accessed through the *SPF Affaires Etrangères / FOD Buitenlandse Zaken (Address:* Rue des Petits Carmes 15, 1000 Bruxelles, Belgium, Phone: +32 2 501 81 11, Contact through the following webform link: http://diplomatie.belgium.be/en/Contact

9/ Automated / Manual processing operation

Both.

10/ Storage media of data

In accordance with Point 3.4 of the Memorandum of Understanding *"The European Institutions and Bodies are responsible for storing the duly completed and signed original notification documents (=* 'Demande de vérification ' / 'Verzoek om een verificatie')*."*

Database of the Investigation Sector shall be set up for that purpose.

11/ Legal basis and lawfulness of the processing operation

- **Memorandum of Understanding between the Government of the Kingdom of Belgium and the European Parliament, European Council, Council of the European Union, European Commission, European External Action Service, European Economic and Social Committee, Committee of the Regions of the EU and the European Defence Agency on Security Verifications of 18 October 2016.**

Belgian legal and regulatory framework on security verifications:

- Act of 11 December 1998 on classification and security clearances, security certificates and security advices, its
- Act of 11 December 1998 establishing an appeal body on security clearances, security certificates and security advices and its accompanying Royal Decree of 24 March 2000 (hereafter the Appeal body)
- Royal Decree of 4 September 2013 establishing the amount of charges due for issuing a security advice for persons who need to undergo a security verification

Further legal reference:

Good administrative practices in the framework of the Treaty of Lisbon and the Council Decision of 26 July 2010 establishing the organisation and functioning of the European External Action Service (2010/427/EU) available on http://www.eeas.europa.eu/background/docs/eeas_decision_en.pdf

12/ The recipients or categories of recipient to whom the data might be disclosed

- EEAS Security Investigations Sector
- Dedicated members and management of the EEAS HQ Security and Policy Division
- Other concerned EU institutions and bodies' dedicated staff members involved in the verification procedure, including the POC (Point of Contact) of the concerned EU institutions and bodies

(NOT under Point 15. as this is not considered Transfer to Third Countries)

13/ retention policy of (categories of) personal data

I. Data will be retained for the duration of the contract, or in case of prolongation, 4 years or equal to the duration of the contract.

The security advice will be valid for a period of 4 years.

II. Files related to the contracting arrangement and supporting document regarding the security verification are to be kept for up to 5 years from the date on which the European Parliament grants discharge for the budgetary year to which the data relates (i.e. 5+2 years) for control, inspection and audit purposes for control by Internal Audit, Ex-post Control Services and the European Court of Auditors.

When appropriate, in accordance with Article 48(3) of the Rules of Application, personal data contained in supporting documents should be deleted where possible where these data are not necessary for budgetary discharge, control and audit purposes.

13 a/ time limits for blocking and erasure of the different categories of data
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

Justified requests sent to the EEAS are treated within 10 working days after the request will have been deemed legitimate.

Requests concerning the security verification process or the advice shall be dealt directly by the Belgian Administrative Authority.

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,

Not applicable

15/ Proposed transfers of data to third countries or international organisations

None

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

No. EU institutions and bodies, as parties to the Memorandum of Understanding would not process data related to suspected offences, offences, criminal convictions and security measures. Solely the outcome of the security verifications will be handled by concerned EU institutions and bodies. Personal data linked to the security verification itself will be processed by the law enforcement authorities.

Article 27.2.(b)

Not applicable.

Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

Not applicable.

Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

Yes, exclusion from the right of access to EU institutions and bodies; possibility of the establishment of lists on individuals not to be granted access to EU Institutions & Bodies due to the outcome of the security verification or due to the refusal of the individual being subject of the security verification.

Other (general concept in Article 27.1)

Not applicable.

17/ Comments

Description of the processing

Each of the European Institutions and Bodies participating in the MoU on security verification of 18 October 2016 will designate a point of contact (POC) who will be responsible for managing and overseeing the security verification process for their organisation. The POC is also responsible for transferring the security verification requests to the Administrative Authority.

1. Any employee of an external contractor who will be subject to a security verification will give his permission to initiate the verification necessary to obtain a security advice. The POC will transmit to the external contractor the notification document as included in annex 1, to be forwarded, against notice of receipt, to concerned employees. The employee of the external contractor is invited to complete and sign this document and hand it back to the external contractor who will forward it to the POC.

2. If the employee of the external contractor does not wish to be the subject of a security verification, he may express his refusal by crossing out the notification document and sending it back, by registered mail, to the POC of the concerned EU Institution or Body.

3. The POC will transmit to verification@diplobel.fed.be and in copy to sec-check@diplobel.fed.be the following data of the person concerned: last name, first name, address, date and place of birth, nationality, national number or ID number if the employee is not of Belgian nationality, employer and function. To submit these data, the POC must use the template included in annex 2. In the interest of data protection, these personal data will be transmitted in a protected way. Currently the system for transmission foreseen is ACID, until further notice

4. If the employee of the external contractor refuses to submit to a security verification, this person may be refused access to premises of the European Institutions and Bodies.

5. The security officer of the Administrative Authority will notify the concerned employees of the external contractor of the positive decision forthwith and in the fastest way possible. Simultaneously, the security officer transmits the outcome of the security verification to the POC of the European Institution or Body concerned. If the security advice is negative, the Administrative Authority will inform the concerned employee of the external contractor of the advice by registered mail, in a well-reasoned letter, within 8 days. Simultaneously, the security officer transmits the outcome of the security verification to the POC of the European Institution or Body concerned. A negative security advice means for the National Security Authority that access to EU premises by this concerned individual represents a security risk to the European Institutions and Bodies. Consequently, this person may be refused access to premises of the European Institutions and Bodies.

The concerned employee of the external contractor is entitled to lodge an appeal with the Appeal body within a period of 8 days after the receipt of the advice by registered mail as mentioned above.

4. The security advice is valid for a period of 4 years.

5. The National Security Authority is authorised to withdraw a security advice if it considers that, after having received new information, the conditions for granting a positive security advice are no longer met. In this case the requesting Administrative Authority will be notified immediately so that the procedure in point 3.7 of the MoU will be applied.

Two ways of processing

Outgoing data:

The point of contact (POC) of the EEAS will transmit to the Administrative Authority electronically and in a secure way, through a consolidated template (see annex 2), the data of the person involved. The data concerned are: last name, first name, address, date and place of birth, nationality, national number or ID number if the employee has no BE nationality, the employer and the function.

Incoming data:

The POCs of the EU Institutions & Bodies will share the negative outcomes of the screening by the National Security Authority (NSA) of Belgium and the outcome of the security verification into a database for consulting, storing and transmitting to the POC of other EU institutions and bodies in a secure way according to point 4.1 of the MoU.

PLACE AND DATE: Brussels, 30 September 2016
DATA PROTECTION OFFICER: SAVOIA-KELETI Emese
INSTITUTION OR BODY: European External Action Service