Prior Checking Opinion
"Security clearance procedure at the EFTA Surveillance Authority"

Case 2017-1004

***

The EFTA Surveillance Authority (ESA) processes personal data for granting security clearances. In application of the proportionality principle, the ESA should not keep filled-in security forms, but only forward them to the relevant national security authorities.

***

Brussels, 18 September 2018

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

1. Proceedings

On 17 November 2017, the European Data Protection Supervisor (hereinafter 'EDPS') received from the Data Protection Officer (hereinafter 'DPO') of the EFTA Surveillance Authority (hereinafter 'ESA') a notification for prior checking regarding the data processing operations related to the application of the security clearance procedure.

The EDPS requested complementary information on 30 March 2018. The information was provided on 13 April 2018. The security clearance procedure is already applied (prior to its notification), making the analysis an ex-post control of the processing operation. On 7 August 2018 the EDPS sent the draft Opinion to the DPO of ESA for comments which were received on 27 August 2018.

2. Facts

This prior check concerns the data processing activities, which ESA carries out in order to run security clearance procedures on specific members of staff who are required to have access to classified information.

The overall purpose of the data processing is to determine whether a person is eligible for an authorisation to access classified information. The primary responsibility for the data processing lies within the Administration Unit. In particular, the Authority Security Responsible is competent for granting security authorisations.

The Authority Security Responsible maintains a record of the clearances within the Authority (Article 6.2 of Rules on Security). He collects and retains personal information about staff members in a specific security clearance form issued by the staff members' home country national security authority. The staff members fill in the relevant forms, which are consequently stamped and forwarded to the competent national security authority. Copies of the filled-in forms as well as of the outcome of the vetting procedure are stored by ESA. In the case that the competent authorities issue a positive opinion, the Authority Security Responsible may grant the security authorisation. In the case that a negative opinion is issued, the person concerned may be heard by the Authority Security Responsible. If the latter considers it necessary, he may ask the competent national security authority for further clarifications. However, if the negative opinion is confirmed, the Authority Security Responsible cannot grant an authorisation (Article 20 of the Rules on Security). All the aforementioned documents are kept in a file (hard copies) but also in the ESA database (GoPro). Access is only available to the group Administration Security Clearance Confidential (which consists of the Security Officer and the Assistant in charge of the administration of security clearances).

Data subjects involved in the processing are staff members of the ESA and possibly members of their close family.
The categories of personal data collected vary slightly from State to State, but usually include the following:

- name, name history, date and place of birth, nationality, national identification or social security numbers
- previous and present marital status
- education
- previous and present employment

- criminal record details
- security-related activities (including details of prior security clearance, and details of any activities which could negatively affect security clearance)
- financial situation, interests and history
- past and present address and travel
- health data
- conduct which could provide grounds for pressure or improper influence
- present or past use of, and attitude towards addictive substances (such as drugs and alcohol)

A completed security clearance form may also contain information on the staff member's close family members (parents, in-laws, present and former spouses or partners and children). The categories of people covered also vary depending on which State is issuing the form for security clearance. The information provided contains the following:

- name, name history, date and place of birth, nationality, occupation
- financial situation, interests and history
- details of any activities which could negatively affect security clearance
- financial situation, interests and history
- past and present address and travel

As far as conservation of data is concerned, the paper and digital file is securely destroyed 6 months after the termination/expiration of the staff member's contract.

Personal data are transferred (outside ESA) to EEA member states and to the European Commission in order for the vetting procedure to take place by the relevant national security authorities. Within ESA the Human Resources (HR) department is informed and kept updated by the Security Assistant regarding the security roles of the personnel. The information shared are: the names of the staff members, their titles, the reason for which a security clearance was granted and the stage of the clearance procedure (in process or finalised). The HR department is also informed in the case of a negative outcome of the vetting procedure in order to comply with Rule 19.1 of the Staff Regulations and Rules, according to which the failure to achieve security clearance by a staff member may result in termination of employment.

As far as the right to information is concerned, individuals are provided with a general data protection notice, which informs them of the purposes of the processing, the categories of data processed, the existence of a right of access and rectification, the possibility of recourse to the data protection supervisor and the retention periods. The notice also refers to potential transfers inside the ESA.

Security measures are implemented

3. Legal analysis

3.1. Prior checking

This Opinion relates to the processing of personal data carried out by ESA to support ESA's decision to grant authorisation to specific members of staff in order to access classified information.

Applicability of Decision 235/16/COL: Decision 235/16/COL ('the Decision') of ESA was adopted in order to protect the fundamental right of natural persons to privacy by aligning the data protection rules of ESA with those of the European Union Institutions (EUI) laid down in

regulation (EC) 45/2001[1]. The processing of personal data carried out by ESA is subject to monitoring by the European Data Protection Supervisor (EDPS) in accordance with the Memorandum of Understanding signed in 2017 between ESA and EDPS.

The processing activity under consideration is carried out by ESA in the exercise of activities which fall within the scope of EEA law (Article 3(1) of the Decision) and it is carried out at least partly by automatic means (Article 3(2) of the Decision). Therefore, Decision 235/16/COL is applicable.

Article 27(1) of the Decision subjects to prior checking by the EDPS 'processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes'. Article 27(2) of the Decision contains a list of processing operations that are likely to present such risks.

The EDPS considers that such data processing operation falls under Article 27(2)(a) of the Decision, which establishes that processing operations regarding 'data relating to health and to suspected offences, offences, criminal convictions or security measures' shall be subject to prior checking by the EDPS. In the case at hand, when processing the categories of personal data, referred under point 2 of the present Opinion (Facts), the Authority Security Responsible processes among others information related to health and to criminal convictions.

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operation of ESA has already been established. The recommendations issued by the EDPS should however be fully implemented. As there is no time limit foreseen within which the EDPS must deliver an Opinion pursuant to Article 27 of the Decision, the notification has been treated on a best effort basis.

3.2. Lawfulness of the Processing

Personal data may only be processed if legal grounds can be found in Article 5 of the Decision.

The EDPS considers that the processing operation falls under Article 5(a) of the Decision, pursuant to which data may be processed if the processing is ' necessary for the performance of a task carried out in the public interest on the basis of: the EEA Agreement or legal acts incorporated into that Agreement; the Agreement between the EFTA States on the Establishment of a Surveillance Authority and a Court of Justice; or in the legitimate exercise of official authority vested in the Authority or in a third party to whom the data are disclosed '. In order to determine whether the processing operation in question complies with Article 5(a) of the Decision two elements should be taken into account: a) whether the EEA Agreement or legal acts incorporated into this Agreement or the Agreement regarding the establishment of a Surveillance Authority and a Court of Justice foresee a public interest task that entails the processing of personal data (legal basis) and b) whether the processing operations are indeed necessary for the performance of that task (necessity test).

In the case under consideration, Rule 19.1 of the Staff Regulations and Staff Rules (adopted by ESA) provides that ' The Authority shall designate positions that are subject to security clearance. Failure to achieve security clearance by a staff member in one such position may result in termination of employment in accordance with Regulation 19.1(c)'. Furthermore, the

[1] OJ L 8, 12.1.2001, p. 1.

Rules on Security of ESA state in point 20 the screening procedure resulting in the security clearance of a staff member. Thus, the abovementioned legal framework provides the required legal basis for the processing operations.

As to the necessity of the processing, the EDPS notes that the processing of personal data in the context of granting authorisation to access classified information is considered as necessary in order to prevent unauthorised disclosure of classified information held by ESA.

3.3. Data Quality

Pursuant to Article 4(1)(c) of the Decision, personal data must be 'adequate, relevant and not excessive in relation to the purposes for which collected and/or further processed'.

Taking into account that the background investigation (screening process/vetting process) is conducted by the relevant national security authority, the processing of the data contained in the security clearance form by ESA (in the form of keeping copies) does not comply with the proportionality principle enshrined in the aforementioned Article.

Indeed, ESA is in no position to check the declarations made by staff members in the forms. Only the competent national security authorities can do this. Hence, ESA should only act as a post box and only keep personal data included in the national security authority's opinion in order to grant (or not) an authorisation for access to confidential information.

The European Commission follows a similar procedure. The Security Directorate acts only as a co-ordination point transmitting the application forms to the national security authorities in a sealed envelope and receiving their replies (positive or negative reply without reasoning) for the purpose of granting authorisations allowing access to EU classified information [2].

The EDPS **strongly recommends** not keeping copies of the filled-in forms; instead, ESA should directly forward them to the competent national security authority in sealed envelopes and not take knowledge of their content.

3.4. Conservation of Data/Data Retention

Pursuant to Article 4(1)(e) of the Decision, personal data may be kept in a form which permits the identification of data subjects for 'no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. Provided that only the result of the vetting procedure is processed by ESA, the EDPS considers the retention period applied by ESA appropriate. Specifically, the destruction of the file containing the result of the vetting procedure 6 months after the expiration or termination of the ESA's staff member's contract complies with the aforementioned provision.

3.5. Transfers of data

According to the facts of the case, personal data may be transferred internally and externally.

[2] See European Commission, Registrer of data processing operations, DPO-93.9 Procédure des habilitations de sécurité, available at http://ec.europa.eu/dpo-register/details.htm?id=43995.

Regarding the internal transfers, Article 7 of the Decision providing that personal data may be transferred 'if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient' applies. In the case under consideration, the transfer of data relating to a negative outcome of a vetting procedure to the HR department, in order for the latter to comply with Rule 19.1 of ESA's Staff Regulations and Rules (failure to achieve security clearance by a staff member may result in termination of the employment relationship) is legitimate according to the abovementioned Article 7. The same stands for the personal data transferred to the HR department regarding the security roles of ESA's personnel, as described under point 2 of the present Opinion.

Regarding the transfer of the security clearance form to the EEA member states and to the European Commission in order for the vetting procedure to take place by the relevant national security authorities, we note that ESA should act only as an intermediary transmitting the data to the national authorities without keeping a copy (see the recommendation in section 3.3 above).

3.6. Information to the Data Subject

Article 11 of the Decision lists the information that must be provided to the data subject before launching a processing operation (identity of the controller, purpose(s) of the processing, recipients or categories of recipients of the data, existence of data subjects' rights, the legal basis of the processing and the data retention period). The data protection notice provided with the employment contract (document 880498) is a general one referring to every processing operation launched by the HR sector. Therefore, it does not include all the necessary elements provided for in Article 11 of the Decision regarding the processing operation aiming at granting an authorisation to access classified information.

The EDPS **recommends** ensuring that data subjects are informed in line with Article 11. It is ESA's choice whether to provide this information as part of a general data protection notice on employment matters or to do it in a separate notice.

3.7. Rights of Access and Rectification

Article 13 of the Decision establishes a right of access and the arrangements for exercising it upon request by the data subject. It encompasses the right to be informed that information relating to the data subject is processed by the controller and to obtain the communication of such data in an intelligible form. Article 14 of the Decision provides the data subject with a right to rectify inaccurate or incomplete data without delay.

The data protection notice (document 880498) explains in plain language the meaning of the aforementioned rights but does not mention a dedicated contact point (e.g. a functional mailbox) for the exercise of these rights. The same stands for ESA's website, where only the DPO's email is available.

The EDPS **recommends** adding a clear contact point in the data protection notice in order to facilitate the exercise of the abovementioned data subjects' rights.

3.8. Security Measures

According to Articles 22 and 23 of the Decision, the controller and the processor must implement the appropriate technical and organisational measures to ensure a level of security

appropriate to the risks represented by the processing and the nature of the personal data to be protected. These security measures must in particular prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration and prevent all other forms of unlawful processing. The technical and organisational measures in place, as described under point 2 of the present Opinion (Facts), appear to be suitable in order to ensure a level of security appropriate to the risks represented by the processing.

4. Conclusion

In this Opinion, the EDPS has made several recommendations to ensure compliance with Decision 235/16/COL. Provided that all recommendations are implemented, the EDPS sees no reason to believe that there is a breach of the Decision.

For the following **major recommendation**, the EDPS expects **implementation and documentary evidence** thereof within **three months** of the date of this Opinion:

1. Ensure that copies of the security clearance filled-in forms are securely destroyed and not kept in the future. ESA should re-evaluate its procedure and provide that the filled-in forms are directly forwarded to the competent national security authority in sealed envelopes without taking knowledge of their content.

For the following **recommendations**, the EDPS expects **implementation**, but does not require documentary evidence:

1. Update the data protection notice in order to ensure that data subjects are informed in line with Article 11 of the Decision.
2. Update the data protection notice by adding a clear contact point in order to facilitate the exercise of the data subjects' rights.

Done at Brussels, 18 September 2018

Wojciech Rafał WIEWIÓROWSKI