‘Security Verifications of External Contractors requiring access to [certain] EU Institutions & Bodies in Belgium’

Prior Checking Opinion

Case 2016-0894

***

Some EU Institutions and the Belgian State have signed a Memorandum of Understanding setting out the rules to conduct security verifications on employees of external contractors (security agents, housekeeping persons, canteen personnel, etc.) who require access to the said Institutions. The purpose of the processing is to protect theses Institutions’ *staff, physical assets and information* from persons that could be a potential threat.

The Belgian intelligence and police services will conduct a security assessment and provide the requesting institution with a security advice about the individuals that may be granted access to the Institutions in case of a positive outcome. It is important to ensure that there is a specific legal basis to process this information and that the persons concerned are properly informed of the processing of their personal data.

***

Brussels, 30 October 2018

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Note to the reader: at the time of publishing this Opinion, the processing is suspended.

1. Summary of the facts

Certain EU Institutions ('EUIs', 'participating EUIs' or 'Institutions') have signed a Memorandum of Understanding (MoU) with the Belgian State in relation to security verifications on employees of external contractors requiring access to the premises of these Institutions. The purpose is to safeguard the Institutions' *staff, physical assets and information,* and the MoU sets out rules on how this procedure should be implemented.

Upon request of the participating institutions, the Belgian Authorities (i.e. the Belgian intelligence and police services - the 'Belgian NSA') will carry out security verifications of external contractors' employees[1] who have access or request access to the premises of the Institutions.

When the MoU entered into force[2], employees of external contractors already working for the institutions were assessed while they already had access to the premises. Concerning new employees of contractors, the assessment is to be carried out before they start, as a pre-condition for receiving an access badge from the accreditation service.

[…]If an individual receive a negative reply, this information will be provided to the individual by the Belgian NSA. In such case, the MoU foresees that the person may lodge an appeal with the Belgian Appeal body.

2. Legal analysis

On 30 September 2016 the European Data Protection Supervisor (EDPS) received a notification for prior checking under Article 27 of Regulation (EC) No 45/2001[3] ('the Regulation') on 'Security Verifications on Employees of External Contractors Requiring Access to EU Institutions and Bodies' from the Data Protection Officer (DPO) of one of the participating EUIs.

Following email exchanges for additional information, the EDPS requested a meeting[4] with staff in charge of the security verifications and security coordination from the institutions participating in the MoU. The meeting took place 3 May 2017 and was followed by further correspondence by letter.

On 18 April 2018 the EDPS informed the EUI that initiated prior checking of the EDPS, since the case had been pending on the EUI for a long time that the EDPS would like to proceed with the Opinion and requested some final clarifications necessary for finalising the Opinion. On 29 May 2018, the EDPS received some of the requested information and the EUI stated that discussions were still on-going with the Belgian Authorities and that the EDPS would be kept informed about any new developments.

[1] Such as security agents, housekeeping persons, canteen personnel etc.
[2] The EDPS was informed that the MoU has been signed 18/10/2016 and activated as of 01/01/2017.
[3] OJ L 8, 12.1.2001, p. 1.
[4] By letter dated 29 March 2017.

The EUI furthermore provided information to the EDPS on 29 June 2018 by forwarding the templates received by the NSA "Identification des mésures de sécurité du secteur" along with the Risk assessment guidelines. The requirement of the NSA for EUIs to fill in the Risk Assessment template was the result of the publication of the adjustment of the Law of 11 December 1998, published on 1 June 2018. […]

Since it is not clear how long these discussions will be on-going, the EDPS issues a general Opinion with recommendations based on the information provided, focusing on those main aspects which raise issues of compliance with the Regulation or otherwise merit further analysis. These recommendations can be addressed by the EUIs while the discussions are on-going and be useful for the EUIs throughout the process. In this regard, the EDPS reminds the EUIs that they are the controllers for their part of the processing activities and therefore responsible for the compliance with the Regulation. At the same time the Belgian NSA is the data controller for the security screening performed by the latter, the modalities of which the EUIs have no access to or control over.

The main issues for the EDPS are the non-existing justification of the necessity to assess all the external contractors' employees wishing to access the premises of the EUIs, the lack of a sufficient legal basis, the redress mechanisms on the level of the EUIs and the information to the individuals about the outcome of the verifications. These are the main subjects the EDPS will address in this Opinion together with some other considerations.

2.1 The necessity of assessing all employees of the external contractors

The security verifications apply to all external contractors' employees[…]. The EDPS has pointed out the fact that necessity implies the need for the combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is the least intrusive measure compared to other options for achieving the same goal. As mentioned in our Necessity toolkit[5], if there is no objective evidence justifying the need for the proposed measure, or if the existing evidence is not relevant or sufficient, the measure should not be proposed. Therefore, the EDPS requested the background information or statistics used as a basis for the assessment and to decide the implementation of the procedure taking into account practical experiences such as incidents already occurred and the potential threats identified.

The participating EUIs argues that the premises of the EUIs constitute politically sensitive working places with a huge amount of confidential and sensitive information and that threats to security have generally increased over Europe in the last three years and particularly in Brussels[…]. Therefore, the participating EUIs consider a screening of all external personnel necessary.

[…]

2.2 Legal basis for the processing operation

The EDPS has repeatedly expressed that a stronger legal basis has to be developed and that adapting of the EUIs' security rules or similar in line with the MoU would not be sufficient. In the reply of the EUIs on 9 March 2018, the EUIs describe the specific security rules or similar that the participating EUIs consider as their legal basis. For example, the European Commission has foreseen a legal basis in its Security Rules 2015/443[6], in particular Article 3(6) (to be read

[5] Available at the following link:
https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_1.pdf
[6] Commission Decision (EU, Euratom) 2015/443 of 13 March 2015, available on the following link:

together with the MoU), 7(5) and 12(1)(b). Article 7 covers security measures regarding persons and section 5, same article, refers to background checks that mandated staff may carry out to determine whether giving such persons access to the Commission premises or information presents a threat to security. The article also sets out what information that may be used and that all checks should be in compliance with Regulation 45/2001. The EDPS considers this article to be specific enough to serve as a legal basis regarding the security verifications and recommends the other participating EUIs to adopt a similar legal basis at the equivalent level.

The EDPS **strongly recommends** that the participating EUIs adopt a legal basis similar to Article 7(5) of the Commission Decision 2015/443 and on the equivalent level.

2.3 Redress mechanisms

The EDPS has expressed concerns about the lack of appeal mechanisms on the EU side for individuals that are denied access to the premises of the EUIs. From previous correspondence, it is clear that a decision to deny access is ultimately a decision of an EUI. The EDPS inquired how the right of redress is maintained under EU law and the availability of redress mechanisms in compliance with Article 47 of the Charter of Fundamental Rights of the European Union.

The EUIs explained that the European Commission foresees that the individual has the right to file an administrative review against the act of removal of their access rights and, in addition, the employee of the external contractor can also institute proceedings against the act before the Court of Justice of the European Union according to Article 263 TFEU[7]. Furthermore, the EUIs pointed out that each EUI can foresee other redress mechanisms or mainly rely on the appeal mechanisms provided by the Belgian authorities against their decisions under Belgian law.

In this regard, the EDPS points out that Article 263 TFEU applies to all the participating EUIs.

2.4 Information to be provided to the external contractors

In the initial notification, the EUI that initiated the prior checking stated that a privacy statement is to be provided to the external contractors for making it available to the data subjects at the time of the verification request. The external contractors might be in the best position to individually inform their staff but the EDPS points out that the participating EUIs are the controllers of this processing activity and the external contractors the processor in line with Article 23 of the Regulation. The EUIs should therefore instruct the external contractors how to collect personal information from their employees on behalf of the EUIs and provide the external contractors with a data protection notice that informs the staff in a clear and plain language how their personal information is being processed throughout the whole procedure.

The EDPS **strongly recommends** that the participating EUIs draft a data protection notice with all the required information in Articles 11 and 12 of the Regulation, publish it on their website/intranet and instruct the external contractors to provide the data protection notice to their employees before collecting their personal information for the security verifications.

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015D0443&from=EN

[7] The Court of Justice of the European Union shall review the legality of legislative acts, of acts of the Council, of the Commission and of the European Central Bank, other than recommendations and opinions, and of acts of the European Parliament and of the European Council intended to produce legal effects vis-à-vis third parties. It shall also review the legality of acts of bodies, offices or agencies of the Union intended to produce legal effects vis-à-vis third parties.

2.5 Outcome of the verifications

[…] The EDPS requested information regarding the procedure for informing individuals with a negative outcome, what information they would receive and from whom. The EUIs explained that the individuals with a negative assessment receive this information from the Belgian NSA through registered mail. It is however not clear to the EDPS what this information includes. Even if the decision to deny an individual access is delivered by the Belgian NSA, it is indirectly a decision of the EUIs and the EUIs must therefore ensure that the requirements under Article 11 and 12 of the Regulation are fulfilled. This could be achieved through a data protection notice including information about the possible appeal procedures that the Belgian NSA will provide to the individuals on behalf of the EUIs.

The EDPS **strongly recommends** that the participating EUIs liaise with the Belgian NSA to ensure that the Belgian NSA will provide the information required under Article 11 and 12 to the individuals who will receive a negative reply.

2.6 The new law on security verifications and clearances

A new database
The EDPS requested further information on how the new law on security verifications adopted by the Belgian State would affect the current procedure in place and/or the MoU.

[…]

The EDPS **recommends** that the participating EUIs […]

[*Update of the existing MoU*]
[…]In the light of the new database, the EDPS points out that the procedure described in the MoU is not up to date and would consequently require a review.

[*Replies in specific situations*]
The EDPS has expressed his concerns about those situations when the Belgian NSA [does not provide the reply within the stipulated time frame] to the EUIs and, as a consequence, the individuals [...] would […] not able to work for the EUIs. This concern was based on our interpretation of Article 22quinquies/1 §3 of the amended law on security verifications and clearances. The EUIs noted that individuals are still able to work in the EUIs until an outcome is received and that such situations, when an individual [...] could not access the premises, have not yet been observed. […]

3. Conclusion

In this Opinion, the EDPS has made several recommendations and suggestions to ensure compliance with the Regulation. In particular, the participating EUIs should:

1. Adopt a legal basis for this processing activity, similar to Article 7(5) of the Commission Decision 2015/443 and on the equivalent level;
2. draft a data protection notice with all the required information in Articles 11 and 12 of the Regulation, publish it on the website/intranet of the EUIs and instruct the external

contractors to provide it to their employees before collecting their personal information;

3. The EDPS strongly recommends that the participating EUIs liaise with the Belgian NSA to ensure that the Belgian NSA will provide the information required under Article 11 and 12 to the individuals who will receive a negative reply;
4. […].

The EDPS expects that the EU Institutions and bodies covered by the MoU implement the recommendations accordingly. The EDPS will therefore **close the case**.

Should the participating EU Institutions and bodies however fail to implement these recommendations, the EDPS may take further action under Article 47(1)(f) of the Regulation.

Yours sincerely,

[signed]

Wojciech Rafał WIEWIÓROWSKI