EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr Juan Ignacio San Millan Maeso
Head of Unit Security
European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels
Belgium

Brussels, 10 September 2013
GB/OL/sn D(2013)2002 **C 2013-0763, 0764**
Please use edps@edps.europa.eu for all correspondence

Dear Mr San Millan Maeso,

On 28 June 2013, the Data Protection Officer (DPO) of the European Defence Agency (EDA) submitted to the EDPS two notifications for prior checking under Article 27 of Regulation (EC) 45/2001 (the Regulation) related to the "management of FSC" and the "management of PSC".

As the processing operations are already in place, the two-month deadline for the EDPS to issue his Opinion does not apply. The cases have been dealt with on a best-effort basis.

The Facts

The notifications relate to the management of Facility Security Clearances (FSC) and Personnel Security Clearance (PSC). Their purpose is the management of security clearances for handling EU confidential information (EUCI).

FSC: When, in the course of EDA's activities, industrial or other entities need to have EUCI transferred to them, both their staff and their facilities need to comply with certain standards. FSC refers to the security standards in facilities (e.g. physical and IT security measures). Compliance with these standards is certified by the relevant National Security Authorities / Designated Security Authorities in the Member States. Personal data processed by EDA in this context are limited to the contact information (name, phone, fax, e-mail) of the Facility Security Officers (FSOs) of such entities. The data may be transferred to the National Security Authorities / Designated Security Authorities which issued the clearance, in order to check the authenticity of the FSC.

PSC: In the course of its activities, EDA handles EUCI. Handling such information is subject to specific security rules, including the obligation for staff handling such information to be security-cleared by the National Security Authorities of their home Member State. In the

present case, this concerns EDA staff (TA, CA, SNEs), other staff working permanently at EDA (interns, other seconded staff, contractors), contractors of EDA needing access to classified areas or IT networks, delegates participating in EDA classified meetings (i.e. from participating Member States, other EU institutions, third countries etc.) and other visitors needing access to EDA secured areas or classified information. For these persons, EDA receives information on the level and validity of the security clearance. Data may be transferred to the issuing National Security Authority in order to check the validity of the PSC.

Information on both FSC and PSC may also be transferred to the Security Offices of third countries and international organisations with which EDA has signed Security of Information Agreements and/or Security Arrangements, if holders of PSC participate in meetings which require a PSC organised by these third parties.

EDA has developed privacy statements for both processing operations. Both statements refer to the Head of the security unit as the controller. Section (c) of both statements read as follows:
"*(a) replies to questions from data controllers: Replies to the questions raised by data subjects to the data controller or the EDA DPO are obligatory within three (3) months from their receipt. Failure to do so, could lead the data subjects to further address their complaints to the European Data Protection Supervisor*.".

Legal analysis
Both notifications referred to Article 27(2)(a) of the Regulation as the ground for prior checking.

The EDPS does not interpret the term "security measures" in Article 27(2)(a) of the Regulation as measures relating to physical protection and security of buildings and staff. Instead, the EDPS considers that this term refers to measures taken against individuals in the context of a criminal (or administrative) procedure (in French "mesures de sûreté", for example forced admission to a psychiatric hospital, asset freezes etc.). This interpretation is in line with the type of information referred to under the same Article 27(2)(a), which includes information regarding suspected offences, offences, criminal convictions.[1] Accordingly, the processing of personal data that takes place in the context of the management of PSC and FSC does not fall under Article 27(2)(a).

The notification on the management of PSC additionally mentioned Article 27(2)(d) (processing operations for the purpose of excluding individuals from a right, benefit or contract) as a ground for prior checking. In the interpretation of the EDPS, this provision refers to processing operations whose sole and specific purpose is to exclude individuals from rights, benefits or contracts.[2] It thus targets processing operations such as exclusion databases or blacklists.[3] Although holding a valid PSC might be a precondition for certain posts at EDA, and failing to obtain one might exclude staff from employment, this exclusion is not the main purpose of the processing operation. Article 27(2)(d) does not apply either.

Therefore, **the notified processing operations are not subject to prior checking by the EDPS**. Nonetheless, the EDPS would like to make several comments on the processing operations notified.

[1] See case 2009-0382.
[2] See case 2007-0561.
[3] See cases 2009-0681and 2010-0426.

Legally speaking, EDA as an agency is the controller of the processing operation, with the security unit being the organisational part entrusted with the processing of personal data. The Regulation never refers to specific individuals as controllers, but always to institutions, bodies, units and organisational entities. This **should be clarified in the privacy statements** - EDA as an agency is the controller.

Section (c) of both privacy statements is drafted in an unclear way and seems to conflate different issues. It seems to be meant to address the requirements of Article 11(1)(c); however, this provision is to be read from the data subject's point of view: e.g. are replies to a questionnaire mandatory (e.g. in application forms)?. The text of section (c) of the privacy statements however refers to situations in which data subjects have addressed queries to the controller or to the DPO. As correctly noted in section (g) of the privacy statements, data subjects can have recourse to the EDPS at any time, not only after having taken up the matter with the controller or the DPO, as might be seen to be implied by section (c). **Section (c) of both privacy statements should be replaced by the appropriate information.**[4]

The privacy statements do not inform data subjects about the (categories of) possible recipients. However, data subjects have to be informed about the **(categories of) recipients** of their data (Articles 11(1)(c) and 12(1)(d)). This item is **missing from the privacy statements and should be added**.

In general, it would be advisable to redraft the privacy statement in a more user-friendly format.

Transfers to recipients (other than Union institutions or bodies) that are not subject to national legislation implementing Directive 95/46/EC are only allowed under the conditions set out in Article 9 of the Regulation. Depending on the respective implementation of Directive 95/46/EC, this can be the case for National Security Authorities in the Member States. It is always the case for third countries and international organisations (other than Union institutions or bodies). Where these countries and/or organisations do not provide an adequate level of protection (see Article 9(1) and (2)), transfers would need to be based on one of the derogations in Article 9(6).[5] **EDA needs to ensure that Article 9 is complied with**.

Conclusion

Although the notified processing operations are not subject to prior checking, the EDPS has made several recommendations. Provided that these are taken into account, there is no reason to believe that there is a breach of the Regulation. Please report back to the EDPS on the measures taken to implement these recommendations within three months.

Yours sincerely,

(signed)

Giovanni BUTTARELLI

Cc: Mr Alain-Pierre Louis, Data Protection Officer, EDA

[4] While indicating the time limits for the controller or the DPO to queries from data subjects is indeed a good practice, this information is already included in section (d) of the statements.

[5] Article 9(6)(d), which allows derogations for transfers that are "necessary [...] on important public interest grounds" would seem to be the most likely case here.