GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr […]
Head of Unit Security
European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels
Belgium

Brussels, 01 October 2013
GB/OL/sn D(2013)2163 **C 2013-0765**
Please use edps@edps.europa.eu for all correspondence

Subject: EDA prior checking notification concerning access control to EDA premises

Dear Mr […],

On 28 June 2013, the Data Protection Officer (DPO) of the European Defence Agency (EDA), Mr Alain-Pierre Louis, submitted a notification for prior checking under Article 27(3) of Regulation (EC) 45/2001 concerning "access control to EDA premises" to the EDPS.

On 15 July 2013, the EDPS requested additional information, which was provided on 6 September 2013. As the processing operations are already in place, the deadline of two months for the EDPS to issue his Opinion does not apply. The case has been dealt with on a best-effort basis.

The notification mentioned Article 27(2)(a) (processing of data related to suspected offences, offences, criminal convictions or security measures) as the reason 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 EDA's access control measures does not fall under Article 27(2)(a) and is **not subject to prior checking**.

[1] See case 2009-0382.

Nonetheless, the EDPS would like to make **several remarks** on the processing operations:

Legally speaking, EDA as an agency is the controller of the processing operations, with the security unit being the organisational part entrusted with the processing of personal data. The Regulation never refers to specific persons as controllers, but always to organisational entities. This **should be clarified in the privacy statement** - EDA as an agency is the controller. The notification also uses the term "processor" in an unclear way. This term is to be understood as referring to entities processing personal data on behalf of a controller - the prime example would be outsourced services. The EDPS discourages using this term to describe the fact that different units within EDA carry out processing operations.

The conservation period of up to five years from the end of contract/last visit for data on badge holder seems excessively long. Other Union institutions have adopted significantly shorter periods in the range of three to six months from the end of contract/last visit.[2] **EDA should reduce the conservation period accordingly or justify the longer period**.

The information on the conservation periods in the privacy statement does not differentiate between administrative data on badge holder and the access logs. For increased clarity, **the two conservation periods should be distinguished in the statement**.

Point (c) of the privacy statement seems to confuse two different aspects: following the design of the statement, it seems as if it refers to the information to be provided under Article 11(1)(d), i.e. whether providing the information is mandatory; the text of this point however refers to the time limits within which the controller will reply to requests for access, rectification, etc. This should be **clarified** by changing the title and providing the relevant information (i.e. that providing the information is obligatory to be granted access to EDA premises) here. Providing information on the time limits within which the controller will reply to requests is a good practice, but would fit better under point (d) of the privacy statement. As correctly noted in section (g) of the privacy statement, data subjects can have recourse to the EDPS at any time, not only after having taken up the matter with the controller, as might be seen to be implied by section (c). In this regard it should also be noted that the information provided in the privacy statement and in the notification form do not match: the statement mentions that the controller will react within three months, while the notification (point 13A) mentions one month. This inconsistency should be remedied.

Please inform the EDPS of the measures taken based on the recommendations of this letter within a period of 3 months.

Yours sincerely,

(signed)

Giovanni BUTTARELLI

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

[2] European Commission: 6 months, see Opinion in case 2010-0427, p.6; European Central Bank (iris scans for access to restricted areas): 3 months, see Opinion in case 2007-0501, p. 8.