EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

[…]
Data Protection Officer
European Banking Authority
One Canada Square, Canary Wharf
London E14 5AA
United Kingdom

Brussels, 19 December 2016
WW/OL/ssp/D(2016)2764 **C 2016-1113**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior-checking notification regarding the use of ECAS at EBA (EDPS case 2016-1113)

Dear […],

On 30 November 2016, the European Data Protection Supervisor (EDPS) received your notification for prior checking under Article 27 of Regulation (EC) No 45/2001[1] ("the Regulation") on the use of the European Commission Authentication System / EU Login (ECAS) for EBA staff to be able to access certain application also from outside EBA's network.[2]

1. The Facts

EBA plans to use ECAS / EU Login to allow its staff to access several applications, such as JSIS online (Joint Sickness Insurance Scheme - reimbursement of health expenses) also from outside EBA's network, e.g. from home.

For using ECAS / EU Login from outside the institutions' and agencies' networks, the use of two-factor-authentication is required. In addition to the user name and password combination, a passcode is sent to a mobile telephone number indicated by the staff member (professional or private device). In order to be able to do this, staff members are requested to provide such a mobile phone number to be given to the European Commission, which manages ECAS / EU Login.

The form requesting EBA staff members to provide this mobile phone number asks them to consent to disclosing their phone number to the European Commission for sending the SMS token.

[1] OJ L 8, 12.1.2001, p. 1.
[2] According to Article 27(4) of the Regulation, the EDPS has to provide his Opinion within two months of receiving the notification, not counting suspensions. The EDPS shall thus render his Opinion by 30 January 2017.

The notification form mentioned the processing of health data as the reason for submitting the prior checking notification.

2. Legal analysis

Article 27(2) of the Regulation lists the criteria which make processing operations "likely to pose specific risks" and thus subject to prior checking. Point (a) of that paragraph refers to the "processing of data related to health".

Using ECAS for the purpose of allowing EBA staff members to access JSIS online from outside the agency's network will indeed result in the processing of health data. However, ECAS / EU Login is only the channel used, while JSIS online or other applications accessed via ECAS / EU Login cover the substantive processing of personal data[3].

The use of ECAS as such is thus **not subject to prior-checking** (however, some processing operations supported by applications using ECAS / EU Login may very well be). Nonetheless, the EDPS has a remark about the notified processing operations:

EBA asks staff members to provide their consent to disclosing the mobile phone number to the European Commission. In order to be valid, consent has to be among other criteria "freely given".[4] Given the imbalance of power between employer and employee, consent is difficult to use in an employment context. It should only be used in cases where staff have a genuinely free choice to either agree or not agree.[5] In the case at hand, staff members will only be able to use applications relying on ECAS / EU Login for access control from outside EBA's network if they agree to disclosing their phone number to the EC. On the other hand, staff member will still be able to use the applications from within EBA's network if they do not agree; thus, the use of consent is possible here if staff members are fully informed. EBA should thus make sure that staff members are fully informed about the choice they make and its consequences; the consent form EBA staff are requested to sign, as well as the privacy statement on ECAS / EU Login provide information. The consent form could however more clearly spell out that the only consequence of not consenting is not being able to use the applications supported by ECAS / EU Login from outside EBA's network.

3. Conclusion

As explained above, the notified processing operations **are not subject to prior checking under Article 27** of the Regulation.

Nonetheless, the EDPS recommends amending the consent form to more clearly spell out that the only consequence of not consenting is not being able to use the applications supported by ECAS / EU Login from outside EBA's network. In light of the accountability principle, the EDPS expects EBA to implement this recommendation accordingly and has decided to **close the case**.

Yours sincerely,

[signed]

Wojciech Rafał WIEWIÓROWSKI

---

[3] See the EDPS prior-check Opinion of 10 July 2007 on the management of the Sickness Insurance Scheme regarding the reimbursement of medical expenses (ASSMAL) by the Commission (case 2004-0238).

[4] See Article 29 Working Party Opinion 15/2011 on the definition of consent, notably p. 13, available here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

[5] An example could be the voluntary inclusion of pictures in an internal directory.