EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

[…]
Data Protection Officer
European Centre for Disease Control (ECDC)
Granits väg 8
171 65 Solna
Sweden

Brussels, 17 January 2018
WW/OL/sn/ D(2018)0109 **C 2017-1077**
Please use edps@edps.europa.eu for all correspondence

Subject: Prior-checking Opinion on access to premises at ECDC (EDPS case 2017-1077)

Dear […],

On 30 November 2017, the European Data Protection Supervisor (EDPS) received a notification for prior checking under Article 27 of Regulation (EC) No 45/2001[1] (the Regulation) on 'access to premises'.[2]

Having analysed the notification and its supporting documentation, the EDPS considers that 'access to premises' is not subject to prior checking. Nonetheless, we have some remarks and recommendations on the notified processing operations.

1. Need for prior checking

Article 27 of the Regulation subjects a number of processing operations 'likely to present specific risks' to prior checking by the EDPS. Paragraph 2 of that Article lists processing operations likely to do so.

ECDC notified 'access to premises' for prior checking under Article 27(2)(a), which lists the 'processing of data relating to health and to suspected offences, offences, criminal convictions or security measures' as such risky processing.

'Security measures' in this Article do not refer to security measures in the sense of managing access to premises or information security. Instead, the EDPS interprets this as referring to measures taken against individuals in the context of a criminal (or administrative) procedure.[3]

[1] OJ L 8, 12.1.2001, p. 1.
[2] As this is an ex-post case, the deadline of two months does not apply. This case has been dealt with on a best-effort basis.
[3] Cf. also the French and German language versions, using 'mesures de sûrete' (instead of 'mesures de sécurité) and 'Sicherungsmaßregeln' (instead of 'Sicherheitsmaßnahmen'), respectively.

None of the other criteria triggering a need for prior checking under Article 27 appear to apply either. Therefore, 'access to premises' is **not subject to prior checking**.

That being said, the EDPS still has several recommendations to make in order to ensure that 'access to premises' will comply with the Regulation. The analysis below does not cover all aspects of the Regulation, but only those that require improvements or otherwise give rise to comments

2. Facts and analysis

Under Article 4(1)(e) of the Regulation, data are to be 'kept in a form which permits 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'.

According to the notification form, ECDC keeps personal data of visitors for five years after the visit; for long-term permits, ECDC keeps the data for five years after the person has stopped working at ECDC. The notification did not include additional documentation showing ECDC's security needs justifying this period

While it is in the first place for ECDC to establish a retention period in line with Article 4(1)(e), which can be paraphrased as 'as long as necessary, as short as possible', this retention period appears excessive.

By way of comparison, the European Commission keeps identification data for six months following the visit / expiry of the badge.[4] A similar period may be acceptable for ECDC. For the EDPS to accept longer retention periods, EU institutions have to demonstrate their specific needs and obligations, such as in relation to nuclear safety.[5]

The EDPS **recommends** reducing the retention period to a proportionate length.

Under Article 4(1)(c) of the Regulation, personal data must be 'adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed'.

According to the information provided, ECDC takes a 'copy of the relevant pages of the [identification] document' (page 6 internal procedure, for occasional visitors) and a 'copy of the ID/passport of the external worker' (page 15 internal procedure, for access by external workers outside working hours). ECDC also collects information on since when a person is registered at their home address in Sweden or another EU country (page 15 internal procedure).

While the EDPS accepts recording items such as name, date of birth, home address, citizenship and ID document number, EU institutions should not copy entire documents, as doing so may collect irrelevant personal data. By comparison, some EU institutions use or plan to use scanners automatically extracting only the relevant data items from ID documents. Others only record the relevant items without taking a copy of the whole document. It is also not clear why ECDC collects the date since when a person is registered at their residence.

[4] European Commission general physical access control (http://ec.europa.eu/dpo-register/details.htm?id=44001 – last update 30/03/17); OLAF has some specific rules (https://ec.europa.eu/dpo-register-olaf/details.htm?id=966 – last update 26/05/16).

[5] Please see https://edps.europa.eu/sites/edp/files/publication/11-07-15_acs_jrc_en.pdf for an example for such specific obligations. For other precedent cases please see https://edps.europa.eu/data-protection/our-work/publications/opinions-non-prior-check/access-control-premises-eda_en and https://edps.europa.eu/data-protection/our-work/publications/opinions-prior-check/control-system-iris-scan-european-central_en. For a recent notification of an EU agency with heightened security needs and a short retention period, see https://edps.europa.eu/sites/edp/files/register/notification_file/1440-2017-2045_-_notification.pdf.

The EDPS **recommends** that ECDC re-evaluate which data items it needs and cease copying ID documents of visitors / external workers and instead only record the relevant data items, e.g. on a visitors' list.

Under Article 22 of the Regulation, controllers have to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks'.

[…][6].

[…]

3. Conclusion

Although 'access to premises' is not subject to prior checking under Article 27 of the Regulation, the retention periods raise issues of compliance with the Regulation, as analysed above. In light of the accountability principle, the EDPS expects ECDC to implement the above recommendations and has decided to **close the case**.

Yours sincerely,

[signed]

Wojciech Rafał WIEWIÓROWSKI

Cc: […], Head of Section Corporate Services, ECDC

[6] On ISRM in general, see: https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en .