EUROPEAN DATA PROTECTION SUPERVISOR

GIOVANNI BUTTARELLI
SUPERVISOR

...
Head of Security
Directorate for Logistics
European Economic and Social Committee
Committee of the Regions
JDE0003
Rue Belliard 99-100
10 40 Bruxelles

Brussels,
WW/UK/ktl/D(2017) 1654 **C 2017-0662**
Please use edps@edps.europa.euu for all correspondence

Subject: **Prior-checking Opinion regarding the video-surveillance system of the European Economic Social Committee and the Committee of the Regions (EDPS case 2017-0662)**

Dear ...,

On 23 June 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") of the video-surveillance system of the European Economic and Social Committee (EESC) and the Committee of the Regions (CoR) from the Data Protection Officers (DPOs) of both institutions.[2] On 7 July 2017, the European Data Protection Supervisor (EDPS) received confirmation that this is intended as ex-post notification for prior checking due to processing of special categories of data in the sense of Article 10 of the Regulation.

The EDPS has issued Guidelines concerning the processing of personal data for video-surveillance[3] ("the Guidelines"). Therefore, this Opinion analyses and highlights only those practices which do not seem to be in conformity with the principles of the Regulation and with the Guidelines. In the light of the accountability principle guiding his work, the EDPS would nonetheless like to highlight that *all* relevant recommendations made in the Guidelines apply to

[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. The case was suspended between 4 and 7 July 2017. This case has been dealt with on a best-effort basis.
[3] Available on the EDPS website: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf.

the processing operations put in place for video-surveillance at the EESC and the CoR. This regards in particular the use of covert surveillance (see below section 1.1), which for ad hoc measures by the CoR has been the topic of two previous cases[4].

1. Facts and analysis

1.1. Covert surveillance: "the use of concealed cameras"

The EDPS takes note that, under section 4.4 of the Committees' CCTV policy, entitled "*Ad hoc* surveillance", the Committees reserve the right to resort to "***the use of concealed cameras***"[5] under certain conditions ("*...when previously authorised by the Secretary-General, after conducting a data protection impact assessment and obtaining a positive prior checking opinion from the EDPS...*").

a) This seems to contradict the statement contained in section 4.1 of the Committees' CCTV policy, according to which "*...we do not use covert surveillance*" and the information contained in the "Privacy impact assessment", which on p. 2 expressly states that "*The Committees...de not use covert surveillance...*".

b) The EDPS further notes that covert surveillance has been the topic of a consultation on an ***ad hoc*** **targeted covert surveillance** measure in the framework of an administrative inquiry at the CoR (case 2014-0061).

As highlighted on that occasion and in Section 6.11 of the Guidelines, "*The use of covert surveillance is highly intrusive due to its secretive nature. Further, it has little or no preventive effect and is often merely proposed as a form of entrapment to secure evidence. Therefore, its use should be avoided*".

As already noted in the **EDPS Opinion of 30 January 2014 in case 2014-0061**, "*Under the same Section of the Guidelines, proposed exceptions must be accompanied by a compelling justification, an impact assessment and must undergo prior checking by the EDPS who may impose, as necessary, specific data protection safeguards. Although the Guidelines refer to the prior checking of the use of covert surveillance per se, this should be interpreted as referring to a general procedure on the use of covert surveillance. The EDPS' role referred to in the Guidelines is to ensure that the legal framework surrounding the procedure for the possible use of covert surveillance is compliant with the Regulation. It is not to grant prior authorisation in each and every case."*

As its 2012 predecessor under examination in case 2014-0061, the Committees' CCTV policy does, however, not describe the conditions applying to the future "*use of concealed cameras*", explain the reasons thereof, or outline the necessary implementing measures. As a consequence and as already explicitly noted in the EDPS Opinion of 30 January 2014 in case 2014-0061, "*Failing the existence of a Policy on covert surveillance, any such action even as an ad hoc measure would fall in breach of the Guidelines*".

As in the Opinion in case 2014-0061, the EDPS **recommends** urgently amending the Committees' CCTV policy so as to establish a clear, explicit and transparent legal basis for the

[4] See EDPS cases 2013-1423 and 2014-0061.

[5] "*The Committees may need to use video-surveillance on an ad hoc basis for specific events or during internal investigations. In this latter case, the use of concealed cameras may be used when previously authorised by the Secretary-General, after conducting a data protection impact assessment and obtaining a positive prior checking opinion from the EDPS...*".

use of covert surveillance. The Policy on covert surveillance should be in line with the principles and conditions set in Section 6.11 of the Guidelines.
The EDPS expects to receive documentary evidence of implementation.

1.2. Collection of special categories of data

According to the notification, "*Due to the location of their buildings and in order to fulfil their security needs, the Committees' video-surveillance system might record images of protestors that might contain special categories of data, such as political opinions, religious or philosophical beliefs, trade union membership*" and "*Demonstrators passing in front of the Committees' buildings*" are mentioned as data subjects.

a) Prior-checking

As correctly noted in additional information provided on 7 July 2017, due to this processing of special categories of data in the sense of **Article 10 of the Regulation**, the video-surveillance system of the EESC and the CoR qualifies for prior-checking under **Sections 4.3 and 6.7 of the Guidelines**. Section 6.7 of the Guidelines explicitly states that "*All monitoring processing special categories of data is subject to prior checking by the EDPS*".

The EDPS regrets that, as confirmed on 7 July 2017, the Committees' CCTV policy has been notified to the EDPS ex-post.

b) Data Protection Impact Assessment (DPIA)

Section 6.7 of the Guidelines establishes as a principle that "*...Areas should ... not be monitored where there is an increased likelihood that images revealing special categories of data will be captured on the cameras even if the intention is not to collect such special categories of data*". Under Section 6.7 of the Guidelines, "*An impact assessment must be carried out in case an Institution wishes to derogate from these rules*."

aa) Together with the confirmation of the notification ex-post, the EESC and the CoR provided a document entitled "**Privacy impact assessment: CoR-EESC video-surveillance system**". This document:

- repeats that "*Due to the location of their buildings and in order to fulfil their security needs, the Committees' video-surveillance system might record images of protestors that might contain special categories of data, such as political opinions, religious or philosophical beliefs, trade union membership*";
- notes that "*Images of demonstrators are also retained for 30 days because a security incident could be brought to the attention of the Security Service after a longer period (for example by an individual or by the police).*";
- On the "*Excessive collection of personal data*" identified as "privacy issue" mentions compliance risks regarding the Regulation and the Guidelines;
- On the "*Excessive storage period*" identified as "privacy issue", under compliance risk expressly refer to "*Non-compliance with the...Guidelines, which recommend retention for a week for typical security purposes and of 48 hours in case of surveillance covering member states territory".*
- In the section *"Identify privacy solutions*", expressly notes the following:
  - "*In case of special categories of data collected, cameras do not focus on the faces of individuals and do not seek to identify individuals unless there is an imminent threat to public safety or violent behaviour.*
  - *In the absence of the detection of a security incident, recordings of each peaceful protest are deleted within 2 hours of the end of the protest.*

- *Live monitoring*
- *Images not used for data mining*
- *Appropriate training to operators of the video-surveillance system*".

- In the same section *"Identify privacy solutions*", the column entitled "Evaluation" notes on the above elements that "*The solutions allow for achieving the aims of the project – safeguard Committees' buildings, property, staff and visitors as well as detect and prevent crime – while at the same time avoiding collecting excessive amounts of personal data*";
- In the section "*Sign off and record the PIA outcomes*", the document only refers to the three following points:
  - "*In case of special categories of data collected, cameras do not focus on the faces of individuals and do not seek to identify individuals unless there is an imminent threat to public safety or violent behaviour.*
  - *Images not used for data mining*
  - *Appropriate training to operators of the video-surveillance system*".

bb) The DPIA does not explain why the section "*Sign off and record the PIA outcomes*" does not contain all five elements cumulatively listed in the section *"Identify privacy solutions*". In this context, the EDPS notes that the DPIA does contain the statement (pp. 3/4) that "*Images of demonstrators are also retained for 30 days because a security incident could be brought to the attention of the Security Service after a longer period (for example by an individual or by the police).*"

The EDPS highlights, however, that **the DPIA itself concludes** (column entitled "Evaluation") that all five elements cumulatively listed in the section *"Identify privacy solutions*" "***allow for achieving the aims of the project*** *– safeguard Committees' buildings, property, staff and visitors as well as detect and prevent crime – while at the same time avoiding collecting excessive amounts of personal data*" (emphasis added). Facilitating investigations on behalf of an individual or by the police beyond the "sole purposes of security and access"[6] or "to safeguard its buildings, property, staff and visitors"[7] of the Committees are not part of the stated purposes of the Committees' video-surveillance system, which under Article 5(a) of the Regulation must be limited to the processing that is *necessary* for the performance of a task carried out in the public interest.

cc) Although the Guidelines (p. 29, Section 6.7) explicitly refer to the need to ensure that "the privacy and **other fundamental rights of the participants** caught on the cameras, including, importantly, their **rights to freedom of assembly**, are not disproportionately intruded upon", the DPIA provided does not refer to any risks regarding those rights.

To the understanding of the EDPS, this might explain the omission of identified "*privacy solutions*" as outlined above (under section bb)).

The EDPS **recommends** re-conducting the DPIA taking into account fundamental rights of the participants caught on the cameras, including, importantly, their rights to freedom of assembly. The EDPS expects to receive documentary evidence of implementation.

c) Additional safeguards, in particular retention period in case of peaceful protest

[6] See section 4 of the notification.
[7] See section 1 of the Committees' CCTV policy.

Section 6.7 of the Guidelines stipulates that "*Monitoring may only be carried out subject to additional safeguards. In case of surveillance in order to provide security during demonstrations, these additional safeguards may include, among others, the following:*

- *the surveillance of any peaceful protests could only be carried out in case of demonstrated security needs,*
- *cameras should not focus on the faces of individuals and should not seek to identify individuals unless there is an imminent threat to public safety or violent criminal behaviour (e.g. vandalism or assault),*
- *in the absence of the detection of a security incident, you delete the recordings of each peaceful protest within 2 hours of the end of the protest (or consider live monitoring only),*
- *the images will not be used for data-mining, and*
- *adequate training is provided to the operators of the video-surveillance system to ensure that the privacy and other fundamental rights of the participants caught on the cameras, including, importantly, their rights to freedom of assembly, are not disproportionately intruded upon.*"

aa) Against this background, the EDPS notes that the section "*Sign off and record the PIA outcomes*" of the DPIA (which is Appendix 10 to the Committees' CCTV policy) refers to the three following points:

- "*In case of special categories of data collected, cameras do not focus on the faces of individuals and do not seek to identify individuals unless there is an imminent threat to public safety or violent behaviour.*
- *Images not used for data mining*
- *Appropriate training to operators of the video-surveillance system*".

In addition, the Committees' CCTV policy (section 2.9) notes that

- "*Cameras do not focus on the faces of individuals and do not seek to identify individuals unless there is an imminent threat to public safety or violent behaviour.*
- *Images are not used for data mining*".

bb) The EDPS further takes note of the specificities regarding video-surveillance by the Committees, in particular the location of the buildings on Rue Belliard as a frequently used route for demonstrations. The DPIA notes that "*Due to the location of their buildings and in order to fulfil their security needs, Committees video-surveillance system might record images of protestors that might contain special categories of data, such as political opinions, religious or philosophical beliefs, trade union membership*"..

cc) Regarding the retention period of 30 days mentioned in the notification and the Committees' CCTV policy, the EDPS takes note of the following arguments brought forward:

- Section 8 of the Committees' CCTV policy (and section 13 of the notification): "*The images are retained for a maximum of 30 days, including for special categories of data. ... This retention period is justified by the fact that CoR and EESC members are present on average once a month in the Committees' premises. Therefore, investigating incidents might require accessing records from the previous month...*"
- The DPIA contains the statement (pp. 3/4) that "*Images of demonstrators are also retained for 30 days because a security incident could be brought to the attention of the Security Service after a longer period (for example by an individual or by the police).*"

However, the on average monthly presence of *CoR and EESC members* is not connected to *peaceful protestors* recorded by the CoR and EESC video-surveillance system due to the

location of their buildings. Also, as already noted above (section b)bb)), the DPIA itself concludes (column entitled "Evaluation") that all five elements cumulatively listed in the section *"Identify privacy solutions*" (which include the deletion of the recordings of peaceful protest within 2 hours of the end of the protest) "*allow for achieving the aims of the project – safeguard Committees' buildings, property, staff and visitors as well as detect and prevent crime – while at the same time avoiding collecting excessive amounts of personal data*".

The EDPS **recommends** the re-assessment of the above elements in the context of the DPIA, which should be re-conducted (see also recommendation under Section 1.1 above) also taking into account the specificities regarding video-surveillance by the Committees, including some statistical and/or anecdotal evidence for specific needs justifying deviation from Section 6.7 of the Guidelines.

1.3. Excessive collection of personal data, including special categories of data

Under Article 4(1)(c) of the Regulation, personal data must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*". Section 6.1 of the Guidelines explicitly notes that "*Camera locations should be chosen to minimise viewing areas that are not relevant for the intended purposes*".

The DPIA in the section entitled "*Integrate the PIA outcomes back into the project plan*" (p. 13) mentions two items as "Action to be taken", namely

- "*Mask areas of camera coverage in order to reduce its angle so that areas that should not be under video-surveillance are excluded*" and
- "*Evaluate if all the cameras at the entrance halls in the buildings are necessary so that repeated coverage of persons is eliminated*".

For both actions, the date for completion mentioned in the DPIA is "Summer 2018".

Additional information provided by the EESC DPO in an email of 7 July 2017 (in the context of confirming the ex-post notification) contains the following explanation: "*the Committees' Security Service has informed us that the reason is that the Committees' buildings will undergo a refurbishment that will be completed by that date*".

This indicates that (i) current camera angles cover areas that should not be under video-surveillance and (ii) the necessity of all cameras has not been established. No interim measures are foreseen until summer 2018.

Against this background, the EDPS fails to understand how the Committees' CCTV policy can state in its section 2.6 that "*...The decision to use the current video-surveillance system and to adopt the safeguards as described in this video-surveillance policy was made by the Secretary-General of each Committee... During this decision-making process, the Committees:*

- *demonstrated the need for a video-surveillance system as proposed in this policy,*
- *discussed alternatives and concluded that the maintenance of the current video-surveillance system, after the adoption of the data protection safeguards proposed in this policy, is necessary and proportionate for the purposes of the video-surveillance system (see Guidelines, Section 5)...*".

The EDPS **recommends**

- masking areas of camera coverage in order to reduce its angle so that areas that should not be under video-surveillance are excluded;
- evaluating if all the cameras at the entrance halls in the buildings are necessary so that repeated coverage of persons is eliminated;
and expects to receive documentary evidence of implementation.

1.4. Retention period of 30 days

Regarding the retention of recordings, under Article 4(1)(e) of the Regulation, recordings must not be retained longer than necessary for the specific purposes for which they were made (see Guidelines Section 7.1.1).

Under section 8 of the Committees' CCTV policy (and section 13 of the notification): "*The images are retained for a maximum of 30 days, including for special categories of data. ...*".

a) Regarding the need to revise the retention period applicable to **recordings containing special categories of data** in the sense of Article 10 of the Regulation to ensure that, in the absence of the detection of a security incident, recordings of each peaceful protest are deleted within 2 hours of the end of the protest, see above **section 1.1**.

b) For all other recordings, the EDPS takes note that the Committees diverge from the standard one week retention period stipulated for typical security purposes in Section 7.1.2 of the Guidelines. Under section 8 of the Committees' CCTV policy (and section 13 of the notification): "*This retention period is justified by the fact that CoR and EESC members are present on average once a month in the Committees' premises. Therefore, investigating incidents might require accessing records from the previous month...*".

   As explicitly noted in Section 7.1.2 of the Guidelines, "*When cameras are installed for purposes of security and access control, one week should in most cases be more than sufficient for security personnel to make an informed decision whether to retain any footage for longer in order to further investigate a security incident or use it as evidence. Indeed, these decisions can usually be made in a matter of hours. Therefore, Institutions should establish a retention period not exceeding seven calendar days. In most cases a shorter period should suffice*." Also "*If the purpose of the video-surveillance is security and access control, and a security incident occurs and it is determined that the recordings are necessary to further investigate the incident or use the recordings as evidence, the relevant footage may be retained beyond the normal retention periods for as long as it is necessary for these purposes*".

   CoR and EESC members are only part of the data subjects concerned (according to the notification, other groups of data subjects such as Committees' staff and visitors exist and should outnumber them by far). Against this background and in view of communication channels not requiring physical presence to report security incidents, it is not clear in how far the limited *physical presence* of CoR and EESC members should impact on the possibility to identify a security incident as such. Notably, once a security incident has been identified as such, footage can be kept longer than the standard one week retention period in order to allow for further investigation (which may or may not require physical presence of particular data subjects concerned).

The EDPS **recommends** aligning the retention period to the standard one week retention period stipulated for typical security purposes in Section 7.1.2 of the Guidelines.

1.5. Periodic review of the CCTV policy

Section 2.8 of the Committees' CCTV policy stipulates that "*A periodic data protection review will be undertaken by the security service every two years, the next will be in 2020*". Given the adoption of the Committees' CCTV policy and its notification to the EDPS mid-2017, a review in 2020 does not correspond to a review "*every two years"* as stipulated in the (public) policy document.

In line with what is publically stated in Section 2.8 of the Committees' CCTV policy, the EDPS **suggests** conducting the next periodic review of the Committees' CCTV policy in 2019.

2. Conclusions

In this Opinion, the EDPS has made five recommendations to ensure compliance with the Regulation, as well as one suggestion for improvement. Provided that all recommendations are implemented, the EDPS sees no reason to believe that there is a breach of the Regulation.

The EDPS expects **implementation and documentary evidence** thereof within **three months** of the date of this Opinion for the recommendations made in this Opinion.

Additionally, the EDPS **suggests** conducting the next periodic review of the Committees' CCTV policy in 2019. It is for the controller to assess whether or not to implement this suggestion.

Yours sincerely,

(signed)

Giovanni BUTTARELLI

Cc.: ..., DPO EESC
..., DPO CoR