GIOVANNI BUTTARELLI
ASSISTANT SUPERVISOR

Mr. Alain LEFÈBVRE
Data Protection Officer of the European Chemicals Agency
Annankatu 18
P.O. Box 400
FI-00121 HELSINKI
Finland

Brussels, 25/10/2011
GB/UK/mch/ D(2011)1867 **C 2011-0012**

Subject: Prior-checking notification case 2011-12 on the video-surveillance system at the European Chemicals Agency (ECHA)

Dear Mr. Lefèbvre,

We reviewed the documents you have provided the European Data Protection Supervisor (EDPS) with on 21 December 2010 concerning the notification for prior checking under Article 27 of Regulation (EC) No 45/2001 (the Regulation) on the processing operations related to the video-surveillance system at the European Chemicals Agency (ECHA).

The EDPS issued Video-Surveillance Guidelines[1] (henceforth: "Guidelines") in March 2010, requesting the EU bodies and institutions to bring their existing practices in compliance with these Guidelines until 1 January 2011. In the present case, in the light of the notification of 21 December 2010, the EDPS will highlight only those ECHA practices which do not seem to be in conformity with the principles of the Regulation and with the Guidelines and will restrict his legal analysis to those practices. It is clear that all relevant recommendations made in the Guidelines apply to the processing operations put in place in the frame of the video-surveillance system at the European Chemicals Agency (ECHA).

Section 4.3 of the Guidelines outlines the situations in which the EDPS considers that a prior checking notification under Article 27 of the Regulation is required to assist the relevant institution in establishing additional data protection safeguards in cases where its activities go beyond the standard operations for which the Guidelines already provide sufficient safeguards.

[1] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

The situations referred to in Section 4.3 of the Guidelines include inter alia:

- video-surveillance proposed for investigative purposes;
- the processing of special categories of data as well as
- the use of high-tech or intelligent video-surveillance.

As noted in the notification submitted, the footage resulting from the video-surveillance system at ECHA "may in exceptional cases also be used for investigative purposes (disciplinary proceedings)" and "the cameras installed at the outer shell of the building can possibly capture images of demonstrations passing the ECHA premises, which might then consequently involve the processing of special categories of data". Section 4.2 of the ECHA Video-surveillance Policy submitted additionally notes that "Infra-red cameras can be used at outdoor entry/exit points if other security measures are not effective". The Guidelines in Section 6.9 list items qualifying as "high-tech video-surveillance tools" or "intelligent video-surveillance systems"; these notably include "*infra-red or near-infrared cameras* ".

The processing operations under examination are thus subject to ex-post prior-checking in conformity with Article 27 of the Regulation.

However, as has been highlighted by the EDPS upon publication of the Guidelines[2], only in exceptional cases will the prior-checking be comprehensive and cover *all* aspects of a video-surveillance system. In most cases, the EDPS will *not* comprehensively review all aspects of the institution's video-surveillance practices. Instead, as in the case at hand, the EDPS will usually focus his recommendations on those aspects of video-surveillance which differ from, or are in addition to, the common practices and standard safeguards set forth in the Guidelines.

1. Proceedings

The procedure was notified for prior checking under Article 27 of Regulation (EC) No 45/2001 on 21 December 2010, suspended by email of 1 March 2011 (D-420) referring to the fact that the Guidelines in Section 15.1 anticipated that "as of 1 January 2011, and upon receipt of the requested documentation, the EDPS will establish a schedule for the processing of the ex-post prior checking notifications. Depending on the number and quality of the prior checking notifications received, the range of issues encountered, and other relevant factors, the EDPS may issue individual opinions or joint opinions with respect to several Institutions and/or issues..."

2. Video-surveillance proposed for investigative purposes (disciplinary proceedings)

Facts: According to the notification and Section 3.1 of the ECHA Video-surveillance Policy, the video footage "shall only be used in disciplinary proceedings in exceptional cases, when the images captured demonstrate that there has been a failure to comply with the obligations incumbent on staff, and more in particular those set forth in the Staff Regulations and its implementing rules, the ECHA Code of Good Administrative Behaviour or the ECHA Security Rules, or when a suspected criminal offence is captured". The impact assessment provided with the notification notes in this respect that "The use of video-footage in disciplinary proceedings naturally has some impact on the privacy of the individual concerned, but the impact does not seem to be disproportional compared to the purpose as

[2] See "Frequently asked questions on video-surveillance: prior checking", Section 5, available under http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_FAQ_videosurveillance_EN.pdf.

only 'accidentally' recorded footage shall be used and the system shall never target a certain individual. Also the fact that there is no covert surveillance supports this point of view".

Under Section 1 of the ECHA Video-surveillance Policy, ECHA's video-surveillance system was set up for typical security purposes. Section 5.8 of the Guidelines stipulates that "where a system is set up for typical security purposes, the video-recordings can be used to investigate any physical security incident that occurs, for example, unauthorised access to the premises or to protected rooms, theft, vandalism, fire, or physical assault on a person. However, in principle, video-surveillance systems should not be installed or designed for the purposes of internal investigations beyond physical security incidents such as those noted above."

Against this background, the intended use of footage in cases of "...a failure to comply with the obligations incumbent on staff, and more in particular those set forth in the Staff Regulations and its implementing rules, the ECHA Code of Good Administrative Behaviour or the ECHA Security Rules..." causes concerns as to its proportionality:

- The seriousness of an infringement of an institution's conduct rules is not generally alike to criminal offences or the physical security incidents referred to in Section 5.8 of the Guidelines. Section 5.1.3 of the Guidelines explicitly notes that "When a video-surveillance system is installed for security purposes and was announced as such to staff, recordings should not be used ... as an investigative tool or evidence in internal investigations or in disciplinary procedures, unless a physical security incident or, in exceptional cases, criminal behaviour is involved".

- Section 5.9 of the Guidelines additionally clarifies that "Goals such as...enforcing the Institutions' policies alone generally do not justify video-surveillance of employees in the context of the work of the Institutions" and highlights that overly intrusive monitoring measures can cause employees unnecessary stress and can also erode trust within the organization.

Recommendations:

- In the absence of further specific justifications for using video-surveillance for investigative purposes and procedural safeguards to ensure that an appropriate proportionality assessment takes place in such cases, video footage should not be used by ECHA in disciplinary proceedings in cases of a failure to comply with the obligations incumbent on staff, and more in particular those set forth in the Staff Regulations and its implementing rules, the ECHA Code of Good Administrative Behaviour or the ECHA Security Rules.

- In the absence of further specific justifications for using video-surveillance for investigative purposes and procedural safeguards to ensure that an appropriate proportionality assessment takes place in such cases, Section 3.1 of the ECHA Video-surveillance Policy should be amended accordingly, reserving the use of video footage in disciplinary proceedings for those exceptional cases where the images captured demonstrate a physical security incident or criminal behaviour.

3. Processing of special categories of data (demonstrations)

Facts: According to the notification, video footage might include "in some cases even data revealing political opinions (in case a demonstration that passes the ECHA premises would be recorded)".

The impact assessment provided notes in this respect "... As the premises of the Agency are located in the immediate centre of Finland's capital Helsinki ... it is well possible that a demonstration passes the building and images of the demonstrators are accidentally captured. There might even be an increased security need for video-surveillance to ensure the security of the premises and the staff and visitors during demonstrations. Even if there exists an obvious risk to the privacy of the participants of a demonstration in this respect, the Agency only captures images for its own security needs in the immediate vicinity of the building's exit and entry points. The Video-surveillance Policy furthermore guarantees that no footage of peaceful demonstrations will be transferred to any third party".

Section 4.7 of the ECHA Video-surveillance Policy indeed stipulates that "Footage of special categories of data (e.g. of demonstrations) shall not be transferred if there is no clear indication of any criminal offence". Section 4.7 of the ECHA Video-surveillance Policy, however, does not further specify under which circumstances an indication of a criminal offence is "clear" in that sense and it does not refer to respective procedural safeguards.

Whilst the EDPS is satisfied that, as previously recommended[3], an impact assessment focusing on this particular issue has been provided in a situation where demonstrations are regularly held in the vicinity of the building and demonstrators/protestors may come within the field of vision of the cameras, the impact assessment provided would not seem to meet the standards applicable under the Guidelines:

- As noted in Section 5.6 of the Guidelines, "even if an Institution concludes that there is a clear need to use video-surveillance and there are no other less intrusive methods available, it should only use this technology if the detrimental effects of video-surveillance are outweighed by the benefits of the video-surveillance... the legitimate interests and fundamental rights of the people monitored may need to be balanced very carefully with the benefits that may be achieved by the surveillance". Whilst the ECHA Video-surveillance Policy stipulates that no footage of peaceful demonstrations will be *transferred* to any third party, *recording* video footage is already a processing of data requiring justification. Under Section 7.1.4 of the Guidelines, inter alia live monitoring should be considered when this is necessary to minimize the intrusion into the privacy and other fundamental rights and legitimate interests of those within the range of the cameras.

- Under Section 5.7 of the Guidelines, institutions must justify, in a verifiable manner, the existence and extent of security risks alleged (specific dangers, crime rates, etc). The mere “perception” of a risk, speculation or anecdotal evidence is not sufficient to justify the necessity of video-surveillance. This risk analysis should be documented in writing and should identify and assess any existing risks and institutions need to demonstrate the type of security risks in the area under surveillance by showing what security incidents occurred there in the past or are likely to occur there in the future.

- Section 5.7 of the Guidelines also foresees that, before opting for video-surveillance, all other less intrusive alternatives should be carefully considered. These may include, for example, controls by security personnel, upgrading alarm systems, access control systems, armouring and reinforcing gates, doors and windows and better lighting. Only when such solutions are demonstrated to be insufficient, should video-surveillance be used.

[3] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveilllance_followup_EN.pdf

Recommendations:

- In the light of Section 5.7 of the Guidelines, ECHA needs to account for, in a verifiable manner, the existence and extent of the security risks alleged (specific dangers, crime rates, etc. rather than the broad reference to "increased security need for video-surveillance to ensure the security of the premises and the staff and visitors during demonstrations") by demonstrating
  - the type of security risks in the area under surveillance by showing what security incidents occurred there in the past or are likely to occur there in the future and documenting this risk analysis in writing;
  - that all other less intrusive alternatives (for example, controls by security personnel, upgrading alarm systems, access control systems, armouring and reinforcing gates, doors and windows and better lighting) are insufficient to address the security issues identified.

- In the light of Section 5.6 of the Guidelines, ECHA needs to demonstrate that it has balanced very carefully the legitimate interests and fundamental rights of the people monitored with the benefits that may be achieved by the surveillance.

- Should ECHA be able to demonstrate the existence and extent of the security risks alleged and a careful balancing with the legitimate interests and fundamental rights of the people monitored, the EDPS recommends that, in the absence of the detection of a security incident, ECHA delete the recordings of each peaceful protest within 2 hours of the end of the protest at the latest.

- Whilst Section 4.7 of the ECHA Video-surveillance Policy generally refers to transfers to national authorities, the EDPS would like to recall the following stipulated in Section 10.4 of the Guidelines:
  - If national police, a court or other national authorities request the disclosure of recordings, the Institution should insist that a formal written request be made according to the requirements of the applicable national law regarding form and content. The Institution should only disclose the recordings if another organisation established in that country would also have been required or at least permitted to make the disclosure under similar circumstances.
  - Irrespective of the national requirements, whenever possible, the Institution should require a court order, a written request signed by a police officer having a sufficiently high rank, or a similar formal request. The request should specify, as closely as possible, the reason why the video-surveillance footage is needed as well as the location, date and time of the requested footage.
  - No general requests should be accommodated for data mining purposes.

  ECHA needs to ensure that the above safeguards apply to transfers of video footage to national authorities. The EDPS notes in this context that under Section 4.7 of the ECHA Video-surveillance Policy, "The Security Manger *shall* consult the Data Protection Officer of the Agency regarding all transfer requests" (emphasis added). Given the implications for legitimate interests and fundamental rights of the people monitored when transferring footage of demonstrations, the EDPS invites ECHA to procedurally ensure that consultation of the DPO is mandatory in such cases.

4. Use of high-tech or intelligent video-surveillance (infra-red cameras)

Although the notification does not explicitly refer to the issue, Section 4.2 of the ECHA Video-surveillance Policy submitted with the notification notes that "Infra-red cameras can be used at outdoor entry/exit points if other security measures are not effective". The Guidelines in Section 6.9 list items qualifying as "high-tech video-surveillance tools" or "intelligent video-surveillance systems" and explicitly refer to infra-red cameras in that context.

As noted in Section 6.9 of the Guidelines, the introduction of "high-tech video-surveillance tools" or "intelligent video-surveillance systems" is permissible only subject to an impact assessment. The impact assessment provided does, however, not refer to this issue.

Recommendation:
To enable the EDPS to assess the permissibility of the technique used and to impose, if necessary, specific data protection safeguards, ECHA needs to provide the EDPS with an impact assessment covering the intended use of infra-red cameras at outdoor entry/exit points if other security measures are not effective.

5. Reminders regarding other aspects of the ECHA Video-surveillance Policy

a) Ad hoc surveillance

Section 4.7 of the ECHA Video-surveillance Policy stipulates that, provided ad hoc video-surveillance is "an effective countermeasure", it may be started if the Security Manager so decides, e.g. because of prominent guests, a temporarily increased security risk or because other physical systems are not functioning, but contains no further specification or guidance. In line with Section 3.5 of the Guidelines, advance plans should be made where an institution contemplates using video-surveillance on an ad hoc basis (for example at times of hosting high-profile events or during internal investigations). In this case the necessary framework and policies for data protection should be established sufficiently before the occurrence of the video-surveillance itself. The ECHA Video-surveillance Policy should be complemented with a framework guiding the Security Manager in making his decision as well as generally outlining the measures to be applied.

b) Number of cameras mentioned in policy

Under Section 6.2 of the Guidelines, the number of cameras must be included in the video-surveillance policy. The ECHA Video-surveillance Policy fails to mention this information and should be complemented accordingly.

c) Retention period

Under Section 4.6 of the ECHA Video-surveillance Policy, the normal retention period is 28 calendar days (4 weeks) and thus longer than recommended in Section 7.1 of the Guidelines "*due to the increased risks posed by the location of the Agency, the value of information processed in its premises and because the premises have many exit and entry points distributed over a number of separate but interconnected buildings. The latter may also cause that security incidents are only discovered after the lapse of a certain amount of time...*"

The EDPS would like to highlight that, as illustrated by the example given in Section 7.1.3 of the Guidelines[4], the fact that an institution is located in a busy downtown area cannot by itself

[4] "Agency B...located in the heart of a busy downtown area with a train station nearby and heavy pedestrian traffic on the pavement of the streets outside its buildings"

warrant an exception to the standard retention period recommended in the Guidelines. This does, of course, not exclude that an institution provides in a verifiable manner proof of the existence and extent of alleged security risks[5], in particular of an increased crime rate in its vicinity, which *inter alia* can contribute to the justification of putting into place a prolonged retention period.

As previously clarified by the EDPS[6], unless institutions provide sufficient justification and adequate safeguards, they should reduce the retention period to seven days or less, as recommended in the Guidelines. ECHA should therefore demonstrate, in a verifiable manner, the existence and extent of the security risks alleged as required under Section 5.7 of the Guidelines.

d) Disposal of no longer useable media

Under Section 7.1.1 of the Guidelines, the ECHA Video-surveillance Policy should further regulate what happens once the media is no longer useable to ensure that it is safely disposed of in such a manner that the remaining data on it is permanently and irreversibly deleted.

e) Register of recordings retained beyond the retention period

Under Section 7.2 of the Guidelines, ECHA needs to establish a register of recordings retained beyond the retention period.

f) Training

ECHA is invited to confirm that the training referred to in Section 4.13 of the ECHA Video-surveillance Policy ("...shall be offered...") has actually taken place.

g) On-the-spot notice and public version of the ECHA Video-surveillance Policy

Section 5.1.2 of the Guidelines foresees that the purposes of the system must be communicated to the public on the spot in a summary form and in more detail, for example, via the public on-line version of the Institution's video-surveillance policy.

The on-the-spot notice mentioned in Section 4.11 of the ECHA Video-surveillance Policy does not meet the content requirements stipulated in Section 11.2 of the Guidelines. ECHA should revise the notice so that it:

- identifies the "controller" (the name of the Institution is usually sufficient),
- specifies the purpose of the surveillance (“for your safety and security” is usually sufficient),
- clearly mentions if the images are recorded,
- provides contact information and a link to the on-line video-surveillance policy.
- Since areas outside the buildings are under surveillance (see above), this should be clearly stated. A notice in such a case merely stating that *the building* is subject to video-surveillance is misleading.

As only the "internal" version of the ECHA Video-surveillance Policy has been provided, ECHA is invited to provide the EDPS with the "summary version" available for visitors at the building reception desk referred to in Section 4.11 of the ECHA Video-surveillance Policy.

h) Attachments to the video-surveillance policy

In the light of the list of attachments to the video-surveillance policy contained on page 63 of the Guidelines, ECHA is invited to provide the EDPS with the following documents:

[5] See Section 5.7 of the Guidelines

[6] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-07-14_Videosurveilllance_followup_EN.pdf

- A map with the locations of the cameras;
- The technical specifications for the cameras and for the video-surveillance system as a whole (including any software and hardware);
- The contract with the outsourced security company;
- Copies of the confidentiality undertakings (see Section 8.3 of the Guidelines);
- The register of retention and transfers (see Sections 10.5 and 7.2 of the Guidelines);
- A processing-specific security policy ("Security Policy for Video-surveillance").

6. Conclusions

The EDPS recommends that the ECHA adopts specific and concrete measures to implement the above recommendations regarding the video-surveillance system.

As concerns the reminders mentioned in this note, the EDPS would like to be informed about the situation regarding the compliance with the Guidelines and receive the requested information.

To facilitate our follow-up, it would be appreciated if you could provide the EDPS with all relevant documents within 3 months of the date of this letter which prove that all recommendations and reminders have been implemented.

Kind regards,

(**signed**)

Giovanni BUTTARELLI