

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.

For the latest updates, visit www.bna.com

International Information for International Business

Volume 13, Number 2

February 2013

The Hungarian Data Protection Authority's Recommendations for Lawful Surveillance of Employees via CCTV

By Andrea Klára Soós, of Soóslaw, Budapest.

Hungarian employers generally use CCTV surveillance in the workplace to monitor employees' conduct for controlling their work and to promote safety at the workplace. Several types of systems are used, including hidden cameras. Therefore, protecting employee privacy is a top concern of labor lawyers and civil organizations.

There is a general trend in Hungary of watering down employees' fundamental rights, including their rights to privacy, in the workplace. This is why the new Hungarian Labor Code¹ has been heavily criticized by experts. The Labor Code expressly allows the restriction of employees' fundamental rights, provided that such action is necessary and proportionate, and confirms and even strengthens employers' rights to monitor employees (*see analysis by the author at WDPR, January 2012, page 11*).

The view of Hungary's former Data Protection and Freedom of Information Commissioner ("Data Protection Commissioner") was very stringent regarding the monitoring of employees, maintaining that the law prohibited any kind of "aimless monitoring". However, Hungary's new Information Act, which took effect January 1, 2012, eliminated the position of the Data Protection Commissioner and created the new Na-

tional Data Protection and Freedom of Information Authority (DPA)² (*see analysis by the author at WDPR, November 2011, page 4*).

The DPA January 27, 2013, published its official recommendations on the surveillance of employees through the use of CCTV cameras³. In its recommendations, the DPA approves such monitoring in the workplace, provided that certain conditions are met.

This article summarizes the basic principles set out by the DPA for establishing a lawful surveillance system in Hungary.

It should be noted that the DPA's recommendations are not binding for other authorities or courts, including employment tribunals, which means that they might be contested in court, or they might not be accepted by other authorities in individual cases.

Background to the DPA's Recommendations

The former Data Protection Commissioner⁴ published his views on employer monitoring of employees several years ago. He took the position that employees are entitled to privacy, even at the workplace, and that consequently surveillance systems are justified only for safety reasons, *e.g.*, in factories, warehouses and similar places. In his view, it was prohibited to directly monitor an employee during his/her work: "No recorder can

be placed at a place where employees are continuously working and the aim of the surveillance can never be the controlling of their work”⁵. The Data Protection Commissioner noted, however, that there might be valid reasons for surveillance at places where things of high value are stored or where the safety of employees is not fully guaranteed (such as, for example, in the case of processing dangerous materials, or when valuable goods are stored for safekeeping in banks). The conclusions of the Data Protection Commissioner were based on the consistent case law of the Constitutional Court, which acknowledges and respects employees’ fundamental right to privacy, even in the workplace.

In practice, however, the stringent position of the Data Protection Commissioner led some employers to use hidden cameras. Some court decisions even held that hidden cameras could be used by employers, provided that employees had been duly informed about the circumstances of the data processing by the cameras.

The new DPA reassessed the position of the Data Protection Commissioner, and argues that, while employees are entitled to privacy, employers are also entitled to monitor whether their employees are fulfilling their duties or not⁶. The DPA’s conclusions are based on Article 7 (f) of the EU Data Protection Directive (95/46/EC) (“Directive”)⁷. The DPA argues that the Directive shall be directly applied in Hungary in light of the European Court of Justice’s November 2011 decision on the direct applicability of the Directive in EU member states⁸ (*see analysis at WDP, December 2011, page 10*).

No Employee Consent is Required for Surveillance

The DPA argues that, pursuant to the provisions of the Labor Code, employees must work during work time and must follow the employer’s instructions. Moreover, the Code entitles employers to apply sanctions if employees breach their obligations⁹.

In the DPA’s interpretation, the above provisions implicitly signify that there is no need to obtain consent from an employee for surveillance; it is the right of the employer to control whether its employee complies with his/her obligations in the workplace. The DPA maintains that this conclusion is supported by the EU Article 29 Data Protection Working Party in its Opinion 15/2011¹⁰. The Working Party states that “where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent... An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid” (*see analysis at WDP, August 2011, page 4*). According to the DPA, Article 7 in itself can be a valid basis for any action affecting employees’ privacy in the workplace.

Valid Reason for Data Controlling in Line with the Test Introduced by Article 7 (f) of the Directive

Article 7 (f) of the Directive provides:

Member States shall provide that personal data may be processed only if:

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

In the DPA’s conclusion, the employer’s legitimate interest is based on the provisions of the Labor Code, which allow it to monitor and control employees if the following four conditions are met:

- 1) the surveillance is necessary, given the nature of the work (*i.e.*, if there is no other, less intrusive possibility for the employer);
- 2) the surveillance system does not violate human dignity (for example, it cannot be placed in dressing rooms or restrooms);
- 3) the employer properly and duly informs employees about the fact of the surveillance; and
- 4) the employer respects the principles of the privacy law, such as the requirement of fair and legal data controlling.

In the DPA’s view, employers must prepare a monitoring policy regarding the above four conditions, and, in line with the requirement of accountability, the burden of proof is always on employers to show that the above conditions are met.

Technical Requirements for CCTV Cameras

If the conditions of the test described above are fulfilled, the employer must comply with certain technical requirements.

Employers must comply with the requirements of a separate act on the protection of property¹¹. The Property Protection Act states that CCTV cameras (applied by security service providers and private investigators) shall be placed in a manner that does not violate human dignity. With respect to records, the Property Protection Act accepts three days’ storage for any video record (in exceptional circumstances, this can be extended to 30 or even 60 days).

In the DPA’s conclusions, if the conditions for surveillance laid down by the Property Protection Act are met, the surveillance by an employer is considered to be lawful.

In order to facilitate the installation of cameras, the DPA provides some examples. For instance, a camera may not be directed at individual employees. Further, a camera may not influence the work of employees (for example, it cannot be used in order to increase employees’ productivity or effectiveness). Cameras shall not be placed

where employees generally spend their breaks (for example, kitchens). However, after normal working hours, such places can also be monitored.

The DPA also highlights that the cameras can be placed only in a manner which restricts the surveillance solely to the property of the employer. In other words, cameras cannot be directed at public areas or at the property of another company.

The DPA also highlights that separate rules apply if the monitoring is outsourced to a security company.

Administrative Requirements

If the theoretical and technical conditions described above are fulfilled, employers still face certain administrative requirements.

The DPA expects that certain minimum information will be provided to all employees in written policies. Such information shall include the placement of the cameras, the aim of the surveillance and the rules for storage of the records.

The final concern of the DPA is that the fact of monitoring shall be registered in the National Data Controlling Registry, in particular when third persons can also be recorded by the cameras.

Is It Now Safe for Employers to Introduce a CCTV System?

In the author's view, employers can easily comply with the recommendations of the DPA.

However, employers must consider the privacy risks associated with video surveillance and the monitoring of employees in order to mitigate the risks of litigation by data subjects.

Courts are not bound by the DPA's recommendations. Therefore, in practice, a prudent employer should always apply its own test to determine whether or not an action restricts the privacy of employees.

The real question, therefore, is whether a surveillance system that expressly and intentionally violates the privacy of employees can be validly used.

In the author's view, employers should clearly state in their policies which privacy rights employees are guaranteed at a given workplace, and what constitutes an invasion of privacy (for example, in no circumstances can an employer make recordings in dressing rooms, showers, changing rooms, restrooms, smoking areas, kitchens or even employee lounges).

As a final observation, the author notes that the DPA's recommendations seem to run counter to recent international trends, such as the widely accepted view that employees' private life shall be respected even during work hours or while using employers' assets.

NOTES

¹ Available in Hungarian at http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200001.TV.

² Information about the DPA is available, in English, at <http://www.naih.hu/general-information.html>. Note that the status and legitimacy of the DPA are subject to a debate in the European Court of Justice: *See European Commission v Hungary* (C-288/12), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=125053&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=886023>.

³ Available in Hungarian at <http://www.naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf>.

⁴ Dr. András Jóri.

⁵ Available in Hungarian at <http://abi.atlatszo.hu/index.php?menu=aktualis/allasfoglalasok/2009&dok=2900/P/2009-3>.

⁶ In the author's view, this conclusion can be disputed, since employees' right to privacy is granted by the Fundamental Law (Constitution), while employers do not have any such right for monitoring.

⁷ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

⁸ Joined cases C-468/10 and C-469/10.

⁹ Section 11 (1) of the Labor Code.

¹⁰ Opinion 15/2011 (WP 187).

¹¹ Available in Hungarian at http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500133.TV.

The text of the National Data Protection and Freedom of Information Authority's recommendations on the surveillance of employees through CCTV can be accessed, in Hungarian, at <http://www.naih.hu/files/Ajanlas-a-munkahelyi-kameras-megfigyelesr-l.pdf>

Andrea Klára Soós is an Attorney at Law with Soóslaw, Budapest. She may be contacted at andrea.soos@sooslaw.hu.