Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection
Privacy International

Project office:
Directorate for Personal Data Protection
10, Samoilova, room nr. 7 ,1000 Skopje
Tel: (+389) 2 3244 761
Email: ipa_dzlp@dzlp.mk

Document 2.1.8 – 2

PROPOSAL of

THE DPDP's OPINION REGARDING DATA PROTECTION IN VIDEO SURVEILLANCE SYSTEMS

Component 1
Activity 2.1.8 - 2

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union

Introduction

Due to fast progress of modern technology, increasing digital memories capacity, development of digitalisation also processing of images and sounds by recording devices is growing. Various sectors apply video surveillance techniques without adequate knowledge of level of interference to privacy of citizens. The relevant institutions shall evaluate video surveillance system from a general privacy protection viewpoint to minimize the risk of negative affect to private life of citizens. The Directorate for Personal Data Protection (DPDP) issues recommendations and advice to everyone who has interest to process personal data in line with the Law on Personal Data Protection and with other principles of European data protection best practice.
This Draft of Opinion aims to help operators to carefully assess their intention of the use video surveillance system and eliminate conflicts with data protection Law. It is not exhaustive list of rules which shall be applied. This document reminds a core privacy protection principles which must be taken into account when deciding about installation of video camera system in the institution.

D R A F T

The opinion of the Directorate for Protection of Personal Data

Operating Video Surveillance Camera Recording Systems in the Light of the Law on Protection of Personal Data 2005 (as amended of 2008 and 2010)

Operation of a video recording system is considered personal data processing, if besides the video surveillance itself the captured images are recorded, or information stored in the recording device and at the same time the recordings, or selected information serve to the purpose of identification of individuals in context with a certain conduct.

Data stored in a recording device, either images or sounds, are always personal data on condition an individual might be identified directly or indirectly on the ground of these recordings (i.e. information from the image or sound recordings enable, if indirectly to identify a person). The Law on Protection of Personal Data defines personal data as “any information relating to an identified or identifiable natural person”. The Law also specifies that “an identifiable person is one who can be identified, directly *or indirectly*, in particular by reference to an identification number or one or more factors specific to his or her physical, psychological, mental, economic, cultural or social identity.”

Before deciding to install a new system the institution must first establish the purpose of the video-surveillance and must make sure that this purpose is legitimate. In accordance with the LPDP and the Rulebook the designation of the purpose must be clear, specific and explicit and it must be put down in writing. Vague, ambiguous, or simply too general descriptions are not sufficient. The institution must aware that decision to use video-surveillance systems should not be taken lightly and requires a careful assessment of both (i) the potential benefits and (ii) the impact that the surveillance may have on the rights to privacy and other fundamental rights and legitimate interests of those in the area of coverage.

What does this mean in practice?

First, recognizable facial images always constitute personal data. This is the case even if the individuals are not known to or not identified by the operators of the system.
An individual is identifiable, if the image on which is he recorded reveals his distinctive marks (especially his face) and the full identification of a person is possible, if these characteristics are matched with other data at disposal. A personal data in its complexity then consists of those identifiers that make it possible to link the respective person with a certain conduct captured on the video taping.

It must be also reminded that not only permanent video camera systems come under the DPDP Rulebook but also if the camera systems are used on an ad-hoc basis.

Personal data processing by means of a video surveillance camera recording system is legitimate:

a) in fulfilling the tasks imposed by the special law (e.g. the Law on the State Police); in these cases it is necessary to observe the provisions of the law in question,

b) with the data subject's consent; it is virtually feasible only in very limited cases when it is possible to identify explicitly the group of persons frequenting within the reach of the camera,

c) without the data subject's consent under application of Articles 9-a, 9-b, 9-c of the Law on Protection of Personal Data (hereinafter the Law).

Obligations of a controller who operates a video recording system equipped with a recording device:

a) The images from video camera systems must be processed fairly and lawfully as well as for specified, explicit and legitimate purposes. The processing of such images must conform all data protection principles set up by the Law on Personal Data Protection.

b) Video camera surveillance system must not excessively interfere with one's privacy. A video recording system may basically be deployed, if the intended purpose cannot be achieved in another manner (a property, for instance, can be protected from robbery by a lock). Furthermore, it is not acceptable to install a video recording system in rooms used exclusively for private purposes (e.g. toilettes, showers, cloakrooms). It is, of course, possible to offer the data subjects a choice between alternatives (it is possible, for instance, to monitor the cloakroom of a swimming pool on condition a space is reserved for changing

that is not monitored). Camera locations should be chosen to minimise viewing areas that are not relevant for the intended purposes.

c) Specification of the intended purpose. The purpose of recording must first be specified unambiguously and be in line with the important, legally protected interests of the controller (e.g. protection of property against robbery). The recordings may be used only in connection with investigation of an event harming these important, legally protected interests of the controller. The legitimacy of the usage of recordings for other purpose must be limited to a significant public interest, e.g. fight against street criminality.

d) Retention period for the recordings is to be fixed. The data retention period should not exceed the maximum time limit eligible for fulfilling the purpose of the video surveillance. Data should be stored within a time loop over, for instance, twenty-four hours, if a permanently guarded property is in question, or over a longer period not reaching over several days (30 days as maximum) and they should be erased after this period elapsed. It does not apply for recordings made by the police pursuant a special law. The data controller is oblige to apply the principle of time limitation which requires that personal data may to be kept for the time period which is necessary for fulfilment of the purpose.
Only in case of an existing security incident the data should be kept longer and disclosed to the law enforcement authorities, the court or other entitled subject.

e) Appropriate security measures are to be ensured in order to protect the recording systems, transfer ways and data carriers on which recordings are stored from unauthorized or incidental access, alteration, destruction, loss or other unauthorised processing. The transmission of video surveillance images via a public communication network may only occur if the transmission is legal, confidential and if the said images are encrypted

f) Data subject must be informed in an appropriate manner that a video recording system is in operation (e.g. through a notice placed in the monitored space), see Article 9-a of the Law, except where a special rights and obligations ensuing from a special law are being exercised. As the Law and the Rulebook specify the informative plate shall be placed on easy visible place. It must be placed as such a way that the data subject is informed about monitoring system before entering to monitored area.

g) Other data subject's rights are to be guaranteed, namely the right to access the data processed and the right to object to their processing (see Articles 10-12 of the Law). In replying to the data subject's request for access to the stored data related to him/her the disclosed data may include date related to third parties exclusively if separating the relevant data and eliminating certain items from the processed data makes the personal information related to data subject no longer understandable.
In practice, it is impossible to exercise the right to have data updated, rectified or supplemented as article 5 of the LPDP stipulates. On the other hand, the data subject has right to have the data blocked if such data is processed in violation of the LPDP.

h) Personal data processing is to be notified to the DPDP (as per Article 27 of the LPDP) except where a special rights or obligations ensuing from a special law are being applied.

i) Processing of special categories of personal data (so called sensitive data) is not allowed, in principle. Areas should also 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. If sensitive data is captured by the system, the specific safeguards and security regime shall be adopted.

j) It must be taken into account that some areas are under heightened expectations of privacy. These areas include, as example, individual offices (including offices shared by two or more people and large), leisure areas (canteens, cafeterias, bars, kitchenettes, lunchrooms, lounge areas, waiting rooms, etc), toilet facilities, shower rooms and changing rooms, and should not be monitored.

k) The institution shall pay a special attention to the use of video surveillance at workplace. The use of video-surveillance to monitor how staff members carry out their work should therefore be avoided, apart from exceptional cases where an Institution demonstrates that it has an overriding interest in carrying out the monitoring. The practice whereby an employee is under constant surveillance (continuously in the field of vision of video-surveillance cameras) is also avoided.

References:

1. Law on Personal Data Protection (Official Gazette, No. 7/05, as amended No.103/08 and No. 124/10)

2. Rulebook on the Content and Form of the Act for the Manner of Performing Video Surveillance (DPDP, 05/11 2010)