



PHARE PROGRAMME TWINNING PROJECT NO. LV/2002/IB/OT-01
DATA STATE INSPECTION

Document 26

Activity 4.3

Creation of material for an awareness campaign among data controllers and workshops / training for data controllers

Processing of Personal Data by means of Video Surveillance - Information Sheet -

written by

Dr. Philipp Scholz, Gregor Scheja

August 2005



**Ludwig Boltzmann Institut für Menschenrechte
Mandated Body**



DATU VALSTS INSPEKCIJA

This publication has been produced with the assistance of the European Union. The contents of this publication can in no way be taken to reflect the views of the European Union.

Introduction

Public and private bodies have been having increased recourse to image acquisition systems in Latvia for the past few years. This circumstance have raised a lively debate in public on the prerequisites and limitations applying to the installation of equipment giving rise to video surveillance as well as the necessary safeguards for data subjects.

When private entities and public authorities use video cameras, for example to protect individuals or prevent material damage, this is subject to the Personal Data Protection Law when the images filmed show identified or identifiable individuals (see Section 2, Number 2 PDP Law). This applies irrespective of whether the images are stored or not. The processing of the images – such as acquisition, release, immediate or subsequent viewing or archiving – must comply with the general principles of data protection.

Criteria for making data processing legitimate

First of all, it is necessary for the processing of personal data by means of video surveillance to be grounded on at least one of the prerequisites referred to in Section 7 PDP Law. Apart from the less frequent cases in which a legal obligation is to be fulfilled or where processing is necessary to protect vital interests, it often happens that a system controller is required to perform a task in the public interest or in the exercise of official authority possibly by complying with specific regulations. Alternatively, the data controller may pursue a legitimate interest which is not overridden by the data subject's interests or fundamental rights and freedoms.

In both cases, though especially in the latter one, the sensitive nature of the processing operations requires careful consideration of the scope of the tasks, powers and legitimate interests concerning the data controller. Superficiality and the groundless extension of the scope of such tasks and powers should be absolutely banned in carrying out this analysis.

Please notice that additional measures and arrangements might result from the preliminary assessment of the processing in accordance with the prior checking mechanism, if video surveillance carries specific risks for individuals' rights and freedoms (see Section 22b PDP Law).

Basic Principles of Data Processing

In addition the basic principles of data processing pursuant to Section 10 must be complied with when installing and operating a video surveillance system: Images must be processed fairly and lawfully as well as for specified, explicit and legitimate purposes. Images must be used in accordance with the principle that data must be adequate, relevant and not excessive, and not further processed in a way that is incompatible with those purposes. Images must be kept for a limited period and no longer than is necessary for the purposes for which the data were collected and processed.

Example: The data may be used for the protection of persons or property or because of logistical or administrative reasons. E.g. a sales outlet may not use security footage for marketing purposes.

Example: The identity of the persons filmed may not be disclosed except a violation of the protected object is obvious. E.g. a sales outlet may not either give or sell filmed images to third parties.

The proportionality principle entails that video surveillance systems may be deployed if other prevention, protection and/or security measures, of physical and/or logical nature, requiring no image acquisition – e.g. the use of armoured doors to fight vandalism, installation of automatic gates and clearance devices, joint alarm systems, better and stronger lighting of streets at night etc. – prove clearly insufficient and/or inapplicable with a view to the above legitimate purposes.

The same principle also applies to the selection of the appropriate technology, the criteria for using the equipment in concrete, and the specification of data processing arrangements as also related to access rules and retention period.

Example: The video camera must be set up in a way that only the images absolutely necessary for the express purpose appear in its filming range. In the surveillance of an apartment block, it should not be possible to see which individual enters which flat.

Example: The images taken with a camera must be deleted within a short time. Normally, a violation of the protected object is established immediately or within a few hours.

Sensitive Data

As far as sensible personal data would be obtained video surveillance is generally forbidden, except the data subject consents.

Example: The observation of a medical practice, a church, the building of a trade-union or a political party or a sex-shop by means of video surveillance is generally inadmissible.

Information to Data Subject

Openness and appropriateness in the use of video surveillance equipment entail the provision of adequate information to data subjects pursuant to Section 8 and 9 of the PDP Law. Data subjects should be aware of the fact that video surveillance is in operation. The information should be visible and may be provided in a summary fashion, on condition that it is effective; it may include symbols that have already been proved useful in connection with video surveillance information – which may differ depending on whether the images are recorded or not. The purposes of the video surveillance and the relevant controller should be specified in all cases. The format of the information should be adjusted to the individual location.

Example: At the entrance to a residential block notice about video observance must be clearly visible to everyone entering the house.

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders.