**Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003)**

As adopted by the European Committee on Legal Co-operation (CDCJ)
at its 78th meeting (20-23 May 2003)

# INTRODUCTION

The Council of Europe's data protection committees wished to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe therefore asked a consultant, Dr Giovanni BUTTARELLI (Secretary General of the Italian Data Protection Authority), to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context. It was therefore agreed to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account in relation to video surveillance.

After examination of Mr Buttarelli's report and guiding principles, the CJ-PD agreed to re-elaborate and specify some of these guiding principles, and prepared the following text.

Many public and private entities have increasingly been using surveillance systems in different sectors for various purposes, in particular in order to control the movement of persons and goods and access to property, as well as events, situations and conversations – whether by telephone, over electronic networks or at a physical location.

Surveillance systems often result in the collection of personal data even though their collection and/or storage is sometimes not the aim of the surveillance data controller.

A considerable portion of these activities is performed by means of video surveillance devices, which raises specific issues as regards data protection.

Information collected during video surveillance activities often includes data (in the form of images and sounds) which directly or indirectly permit the identification of individuals, and the monitoring of their conduct. Moreover, video surveillance systems are increasingly converging with other technologies that raise new privacy and data protection concerns. These include the recording of sounds, wireless and high-speed computer networks used to transfer images; facial recognition systems integrated with computerised databases which can identify and track individuals; and devices that search under clothing and through walls, for example heat recognition devices or infra-red devices.

Video surveillance activities entailing the processing of personal data fall within the scope of application of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No.108] (hereinafter Convention 108) –which was prepared when it became apparent that in order to ensure the effective legal protection of personal

data it would be necessary to develop more specifically and systematically the general reference to respect for private life in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter ECHR) .

Additional rights and safeguards are laid down in various Council of Europe Recommendations, in particular:

Recommendation No. R(87) 15 on the use of personal data in the police sector;
Recommendation No. R(89) 2 on the protection of personal data used for employment purposes;
Recommendation No. R(95) 4 on the protection of personal data in the telecommunications sector;
Various other recommendations which – though not expressly referring to video surveillance - include safeguards and rules that are relevant in terms of personal data protection as also related to data communication and transborder data flows.

Video surveillance is not expressly covered in these instruments. In view of the increase in the use of and technological developments in video surveillance, this subject needs to be addressed.

These guiding principles, therefore, expand and further specify the safeguards applying to data subjects contained in the provisions of those earlier instruments as regards the processing of personal data collected by video surveillance. They cover any type of video surveillance activity allowing (by means of technical equipment) the systematic observation, collection and/or storage of personal data relating to one or more individuals in particular in respect of their conduct, presence and/or movement. These guiding principles should cover systematic observation, whether permanent or on the occasion of a specific event, whether personal data are processed wholly or partly by automatic means, and whether they form part of an archive system or constitute non-automatic systematic processing.

Some guidelines anticipate new possibilities of information technology that will allow easy access and correction without revealing the personal data of third parties.

Attention should be drawn to the fact that, to the extent that these guiding principles contain safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, as established by Articles 5, 6 and 8 of Convention 108 and Article 8 of the ECHR, derogations from such rights, in accordance with Article 9 of Convention 108, which were elaborated on the basis of Article 8 of the ECHR, are possible where they are provided for by law and constitute a necessary measure in a democratic society in the interests of:

protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
protecting the data subject or the rights and freedoms of others.

These guiding principles are intended for the widest possible dissemination among individuals who may be the subject of video surveillance and the users of video surveillance systems, devices and techniques. They are also addressed to member States, manufacturers, dealers, service and access providers and researchers with a view to developing software and technologies that pay greater

attention to data subjects' fundamental rights with regard to video surveillance. Council of Europe member States should ensure that these guiding principles are applied as consistently as possible.

These guiding principles could also serve as a framework for other surveillance activities that are not based on the use of video surveillance devices.

## GUIDING PRINCIPLES

Any video surveillance activity should be undertaken by taking such measures as are necessary in order to ensure that this activity complies with personal data protection principles, in particular:

1) by ensuring that it is carried out in a fair and lawful manner for legitimate, specific, and explicit purposes. Personal data collected by means of video surveillance should not be further processed in a way incompatible with the purposes for which they were collected;

2) by only using video surveillance if, depending on the circumstances, the purpose cannot be attained by measures which interfere less with privacy, provided that the alternative measures would not involve disproportionate cost.

3) by making use of video surveillance in an adequate, relevant and non-excessive way with regard to the determined and specific purposes sought in the individual cases where there is a demonstrable need, in order to avoid any unintentional and unjustified infringement of the data subject's rights and fundamental freedoms, for example, the freedom of movement, and to ensure in particular respect of his privacy, even in public places;1

4) Video surveillance should be carried out in a way that does not make the persons recorded recognisable if the purpose of the processing does not require their possible identification;

5) by preventing the data collected from being indexed, matched or kept unnecessarily. When it proves necessary to keep data, these data must be deleted as soon as they are no longer necessary for the determined and specific purpose sought;

6) by refraining from video surveillance activities where the processing of the data would result in discrimination against certain data subjects or groups of data subjects exclusively on account of their political opinions, religious beliefs, health or sexual life, racial or ethnic origin;

---

[1] Therefore, those responsible for such systems are invited to assess to what extent the video surveillance systems are adapted to their information requirements in relation to the geographical location of the cameras (which areas of the city, which streets and why), and to choose which technology should be used according to these same requirements (image definition, zoom capacity, camera miniaturization...) without using excessive measures.

7) by making clearly discernible in an appropriate manner that video surveillance is taking place, its purpose and the identity of the controller2 or by informing the data subject beforehand of the above. Other information,3 having regard to the specific circumstances, should be provided to the data subject, where this is necessary to guarantee fair processing of personal data and does not jeopardise the purpose of the surveillance;

8) by ensuring that during the storage period, the right of access to the data, and, where appropriate, the right of rectification, blocking and/or erasure, is granted to the data subject unless this would entail disproportionate effort;

9) by taking all technical or organisational measures necessary to safeguard the integrity of the collected information4;

10) In case of storage by the police of personal data by automatic means resulting from video surveillance, the principles of Recommendation No. R (87) 15 on the use of personal data in the police sector should furthermore be taken into account;

11) by limiting the use of video surveillance systems in the workplace to organisational and production requirements or to occupational safety purposes. This system should not be aimed at the systematic surveillance of the quality and quantity of individual performance in the workplace.

Employees or their representatives should be informed or consulted before the introduction or adaptation of a video surveillance system. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity their agreement5 should be sought. In the event of a lawsuit or counterclaim, employees should be able to ground them on the recording made.

12) If personal data are recorded and kept, this should be done as far as possible in a way that allows data subjects to exercise their right of access, in accordance with data protection legislation, without obtaining information about other people.

---

2 In some cases the purpose and the identity of the controller are clear from the circumstances. However, in certain limited cases (e.g. traffic management) it may not be feasible to make the identity of the controller available beforehand.

3 The information to be provided to the data subject may also include technical specifications of the chosen system.

4 This is of special importance in cases of digitisation since the alteration of data cannot be easily detected. Collected information should only be modified for adequate and justified reasons, the modified information collected should be labelled as such and the original information should be retained.

5 For example, this agreement could be given, in accordance with the relevant domestic law procedures, by trade unions or labour councils.