

Journal Scientific and Applied Research, Vol. 31, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

COMPLIANCE OF VIDEO SURVEILLANCE SYSTEMS WITH PERSONAL DATA PROTECTION REQUIREMENTS: ANALYSIS OF PROVIDER PRACTICES

Deyan P. Ivanov[1], Donika V. Dimanova[2]

[1]Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: deqn.plamenov@abv.bg
[2]Department of Communication and Computer Engineering and Security Technologies, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: d.dimanova@shu.bg

Abstract: *Video surveillance is widely used as a security measure, but its operation is directly associated with the processing of personal data and the need to comply with data protection requirements. This paper analyzes the main criteria for assessing the compliance of video surveillance systems with the General Data Protection Regulation (GDPR) and the applicable national legislation, with particular emphasis on their practical implementation by companies operating in the video surveillance sector. An exploratory survey was conducted among representatives of six companies to examine the existence of internal policies, the technical protection measures applied, the organization of access to video data, staff training, and the main difficulties encountered in meeting personal data protection requirements. The results are interpreted as indicative of the surveyed group and reveal both positive practices and gaps in organizational preparedness and the implementation of compliance measures. On this basis, guidelines are formulated for improving personal data protection in the use of video surveillance systems.*

Key words: *Video surveillance, Personal data, GDPR, Compliance, Exploratory survey, Technical measures, Organizational measures.*

1. Introduction

Video surveillance systems are increasingly used in public spaces, commercial facilities, administrative buildings, industrial sites, and other environments where security and monitoring are required. The development of digital and IP-based technologies has significantly expanded the possibilities for collecting, storing, and analyzing video data, while at the same time increasing the risks associated with unauthorized access, excessive surveillance, and interference with personal privacy. In this context, video surveillance should be regarded not only as a technical security measure, but also as a form of personal data processing that must comply with the applicable legal requirements.

The main regulatory framework in the European Union is established by the General Data Protection Regulation (GDPR), which sets out the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, as well as accountability of the controller [1]. These principles are directly applicable to the use of video surveillance systems where recorded images enable the direct or indirect identification of natural persons.

At national level, the requirements of the GDPR are supplemented by the Personal Data Protection Act, which regulates the obligations of controllers and processors of personal data and defines the role of the Commission for Personal Data Protection as the supervisory authority [2]. In the context of video surveillance, particular importance is attached to the existence of a lawful basis for processing, prior information of monitored individuals, restriction of access to recordings, determination of retention periods, and implementation of appropriate technical and organizational measures.

The specialized guidelines of the European Data Protection Board emphasize the privacy risks associated with video surveillance and the need to ensure proportionality, data minimization, and transparency [3]. A similar approach is reflected in the practical guidance of the Commission for Personal Data Protection, which draws attention to internal access rules, retention periods, accountability of processing operations, and the performance of a Data Protection Impact Assessment where processing is likely to result in a high risk [4, 5].

Assessing the compliance of video surveillance systems cannot be limited solely to the formal existence of a lawful basis. It is also necessary to evaluate the specific organizational and technical practices through which data protection principles are implemented. Key assessment criteria include the lawfulness of processing, clarity of purpose, data minimization, access restriction, defined retention periods, information provided to data subjects, and the performance of an impact assessment where high-risk processing is involved [1, 3].

The practical implementation of these requirements, however, is not always consistent. Common weaknesses include insufficient transparency, inadequate access control, failure to observe defined retention periods, the absence of a DPIA for high-risk technologies, and insufficiently developed internal procedures and staff training.

The aim of the present paper is to analyze the extent to which key personal data protection requirements are implemented by companies operating with video surveillance systems and, on this basis, to identify major gaps and directions for improving compliance.

To achieve this aim, the study applies analysis and systematization of regulatory and methodological sources, comparative analysis, and an exploratory survey among representatives of companies supplying and implementing video surveillance systems.

2. Regulatory and Methodological Framework for Compliance Assessment

The assessment of compliance of video surveillance systems with personal data protection requirements should be based both on the regulatory principles applicable to the processing of personal data and on practical criteria that make it possible to determine the extent to which these principles are implemented within a particular organization. In this sense, compliance assessment should not be limited to verifying the formal existence of a lawful basis, but should also include an analysis of the purposes of surveillance, the scope of the data collected, access arrangements, retention periods, information provided to data subjects, and the technical and organizational measures applied [1, 2].

The fundamental principles established by the GDPR include lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability [1]. In the context of video surveillance, these

principles have direct practical implications. Surveillance should pursue a specific and legitimate purpose, cover only the spaces and individuals necessary for achieving that purpose, avoid unjustifiably prolonged retention of recordings, and be organized in such a way that access to video data is restricted to authorized persons.

The lawfulness of processing requires the existence of a valid legal basis. In video surveillance practice, legitimate interest or compliance with a legal obligation are among the most commonly applicable grounds. The selected legal basis should be justified in advance and capable of being demonstrated in accordance with the principle of accountability [1, 2].

Transparency is of particular importance. Individuals subject to surveillance should be informed about the existence of video monitoring, the identity of the data controller, and the purposes of processing. The use of clear information notices and easily accessible information concerning the rights of data subjects is among the main practical requirements for the lawful use of video surveillance systems [2, 3, 4].

Another key criterion is data minimization. The field of view of cameras should be limited to areas that are genuinely necessary for achieving the stated purpose, while avoiding the recording of irrelevant or sensitive areas. The same principle applies to retention periods, which should be defined in advance and limited to the minimum period necessary [1, 3].

The security of video data is another essential element of compliance. Appropriate technical and organizational measures should be implemented, including access control, encryption, authentication, activity logging, and traceability of access to recordings. Such mechanisms are important not only for reducing the risk of unauthorized access, but also for demonstrating accountability during internal or external audits [1, 5, 6].

For systems that may present a high risk to the rights and freedoms of natural persons, particularly in cases of large-scale video surveillance or the use of biometric recognition, a Data Protection Impact Assessment (DPIA) is of particular importance. Its purpose is to identify risks in advance, assess their severity, and determine appropriate measures for their mitigation. A DPIA is directly related to the principles of Privacy by Design and Privacy by Default and represents an instrument for proactive risk management [1, 3].

On this basis, several key criteria for assessing compliance can be identified for the purposes of the present paper, as presented in Table 1.

Table 1. Main Criteria for Compliance Assessment

Criterion	Main practical indicator
Lawfulness	Defined and documented lawful basis
Transparency	Visible notice and information about the controller and purposes
Purpose limitation	Clearly defined purpose of video surveillance
Data minimization	Limited camera coverage and collection of only necessary data
Storage limitation	Defined retention period and deletion mechanism
Access control	Access restricted to authorized persons
Security	Encryption, authentication, logging, and other protective measures
Accountability	Internal policies, procedures, and demonstrable traceability
Data Protection Impact Assessment (DPIA)	Assessment conducted for high-risk video surveillance

These criteria reflect the applicable regulatory principles and provide a basis for the subsequent analysis of the practices of the surveyed companies.

Within the present study, this regulatory and methodological framework is used as the basis for interpreting the empirical results. In this way, the responses of the participating companies are considered not in isolation, but in relation to specific indicators concerning the

existence of internal policies, technical protection measures, staff training, access control, and organizational readiness to comply with personal data protection requirements.

3. Survey Methodology

For the purposes of the present study, a survey was conducted among representatives of companies operating in the field of video surveillance systems. The respondents were selected from organizations involved in the development, supply, installation, or maintenance of video surveillance systems and, due to the nature of their activities, have direct practical experience with personal data protection requirements.

The analysis includes six validly completed questionnaires submitted by representatives of companies operating in the video surveillance sector.

The survey aims to determine the extent to which regulatory requirements related to personal data protection are implemented in the practical activities of companies in the sector. Particular attention is given to the existence of internal policies, the technical protection measures applied, the organization of access to video data, staff training, and the main difficulties encountered in complying with GDPR requirements.

The questionnaire is structured into six thematic areas:

- General company information – types of video surveillance systems offered and organization size;
- Data protection policies – existence of internal rules and the main elements of the policies applied;
- Technical measures – use of encryption and methods for managing access to video data;
- Training and awareness – provision of staff training and the main topics covered;
- Challenges – difficulties in complying with personal data protection requirements and opportunities for improving compliance;
- Examples and practices – sharing successful approaches and actions taken in response to personal data breaches.

The survey includes both closed-ended and open-ended questions. Closed-ended questions allow the quantitative summarization of results and comparison between individual practices, while open-ended questions provide respondents with the opportunity to describe specific organizational approaches, difficulties, and good practices. In this way, quantitative and qualitative elements of analysis are combined.

The results were processed by summarizing the frequencies and relative shares of the responses. For the open-ended questions, thematic grouping was applied to recurring responses related to confidentiality, access control, training, regulatory compliance, and risk management.

The compliance criteria formulated in the previous section were used to interpret the results. This makes it possible to assess the practices of the participating companies not only descriptively, but also in relation to key requirements such as the existence of internal policies, technical protection, restricted access, accountability, and organizational readiness.

Due to the limited number of respondents, the results should be interpreted as indicative of the surveyed group and should not be considered statistically representative of the entire sector.

4. Results and Discussion

The results of the survey indicate different levels of preparedness among the participating companies to implement personal data protection requirements when operating

video surveillance systems. The analysis reveals both positive practices related to technical protection and access control, as well as deficiencies in the areas of internal policies, staff training, and the formalization of organizational procedures.

4.1. Internal Policies and Organizational Readiness

With regard to the existence of an internal personal data protection policy, 66.7% of the surveyed companies report that such a policy is in place, while 33.3% indicate the absence of a formalized internal policy (Fig. 1). This suggests that although the majority of participants have taken organizational steps toward compliance, a substantial gap in this area remains in one third of the surveyed organizations.

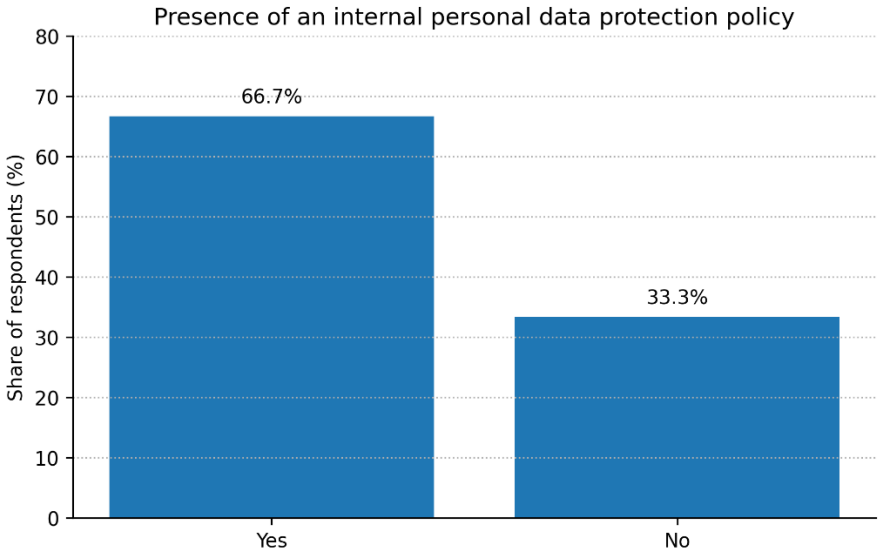


Fig. 1. Presence of an internal personal data protection policy

The content of the internal policies varies in terms of specificity. The principles most frequently identified include confidentiality, lawfulness, fairness and transparency, purpose limitation, accuracy, storage limitation, integrity, and confidentiality of data. Some companies also report structured levels of access to information. At the same time, however, certain responses are limited to general references to applicable regulations and standards without describing specific internal mechanisms.

These findings indicate that the existence of a policy alone is not a sufficient indicator of the actual level of compliance. Of particular importance is the extent to which such a policy is translated into specific procedures, responsibilities, and rules governing access to, storage, and processing of video data.

4.2. Technical Measures and Access Control

The results concerning technical protection are more favorable. A total of 83.3% of respondents indicate that they use encryption for video data, whereas 16.7% do not apply such a measure (Fig. 2).

Within the surveyed group, the high proportion of organizations using encryption indicates a relatively widespread application of this technical measure. At the same time, even the presence of a limited proportion of companies without such protection represents a potential risk to the confidentiality of video data.

With regard to access management, all participants report the use of user accounts and password protection. Some companies apply different levels of access depending on job functions, while one respondent also reports the use of physical access control to the equipment. These practices indicate an effort to combine logical and physical protection mechanisms.

Differentiated access rights are particularly important in video surveillance systems, since different categories of users should not have identical permissions to view, export, delete, or modify recordings. In this sense, access control is not only a technical measure, but also an element of accountability and traceability.

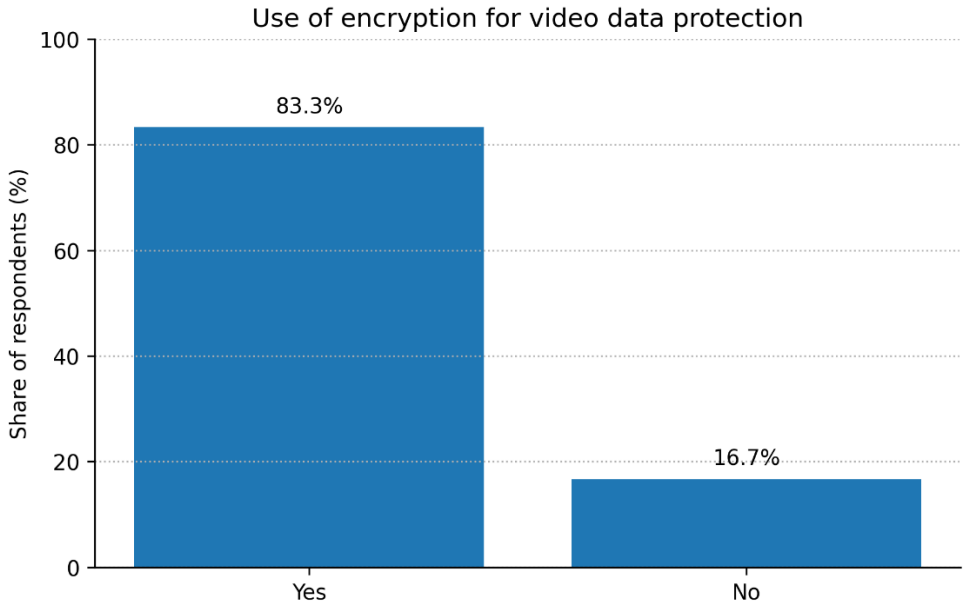


Fig. 2. Use of encryption for video data protection

4.3. Training and the Human Factor

The results regarding staff training indicate a considerably lower level of organizational preparedness. Only 50% of the companies report that they provide staff training related to personal data protection. The remaining half do not systematically apply such a practice.

The content of the training also lacks a unified approach. Some participants identify topics related to regulatory requirements, access to information, and rules for providing data to authorized persons, while others state that no training is conducted or are unable to identify specific topics. This suggests that even where training activities are available, their content is not always sufficiently structured.

This finding is significant, since technical measures alone cannot guarantee compliance. Improper system use, lack of familiarity with procedures, or insufficient awareness may undermine even well-implemented protection mechanisms.

4.4. Main Challenges to Compliance

The responses concerning the main difficulties indicate that the participating companies face both organizational and practical challenges. The issues identified include lack of attention and insufficient engagement on the part of employees and clients, the possibility of leakage of business or customer information, the general nature of some regulatory guidance, and the additional time and resources required for collecting, classifying, and monitoring retention and deletion periods for documentation.

Respondents identify staff training and the provision of more detailed and practically applicable information on personal data protection requirements as the main opportunities for improvement. These responses indicate that the difficulties do not arise solely from technological limitations, but are to a significant extent related to the human factor and to the need to translate regulatory requirements into clear internal procedures.

4.5. Overall Assessment

Comparison of the survey results with the compliance criteria defined in the previous section reveals uneven development across the different elements of data protection.

Within the surveyed group, a higher level of implementation is observed in technical measures, particularly in the use of encryption and basic access control. Lower levels are observed in organizational components, including the existence of formalized policies, systematic staff training, and clearly defined procedures.

The results do not indicate a lack of commitment to personal data protection requirements, but rather varying degrees of their practical implementation. Some companies have introduced the main technical mechanisms, while the organizational framework has not always been developed with the same level of consistency. This highlights the need to treat compliance as an integrated process involving technological, organizational, and training measures simultaneously.

5. Guidelines for Improving Compliance

The survey results indicate that achieving sustainable compliance in the use of video surveillance systems requires the simultaneous implementation of organizational, technical, and training measures. The existence of individual protection mechanisms is not sufficient unless they form part of a clearly defined policy and a consistent personal data management framework.

First, organizations should develop and maintain internal video surveillance policies that clearly define the purposes of surveillance, the legal basis for processing, the categories of affected individuals, retention periods, and rules governing access to recordings. Such policies should also assign specific responsibilities to employees who administer or use the systems. They should be reviewed periodically and updated whenever changes occur in the technological or regulatory environment.

Limiting the scope of video surveillance to the minimum necessary is also essential. Cameras should be configured to cover only those areas directly related to the specific purpose of surveillance, avoiding unjustified recording of adjacent or sensitive areas. At the same time, clear retention periods for video recordings should be established, together with automated mechanisms for their timely deletion in accordance with the principle of storage limitation [1, 3].

Technical protection should be regarded as a permanent element of system management. Key measures include encryption of video data during transmission and storage, the use of reliable authentication mechanisms, differentiation of user privileges, and application of the principle of least privilege. For systems with remote access, the use of multi-factor authentication is recommended, together with regular review of active user accounts and assigned permissions.

Traceability of actions performed within the system is another key component of compliance. Logging user access, configuration changes, viewing activities, and the export of recordings enable both the timely detection of suspicious activity and subsequent auditing of actions performed. Therefore, systematic logging and periodic log analysis should form part of standard video surveillance management practices [5, 6].

The survey results indicate that staff training is one of the areas with the greatest potential for improvement. Periodic training should cover not only the basic requirements of the GDPR, but also specific rules for operating video surveillance systems, managing access, responding to incidents, and handling requests from data subjects. Such training reduces the risk of human error and contributes to the development of a sustainable organizational culture of personal data protection.

For high-risk systems, including large-scale surveillance, biometric identification, or automated behavioral analysis, a Data Protection Impact Assessment (DPIA) should be carried out. It should be performed before deployment of the system or when significant changes are introduced to its functionality, so that potential risks can be identified and mitigated at the design stage [1, 3].

Organizations should also establish clear procedures for responding to personal data protection incidents. These procedures should define the steps for identifying and documenting the incident, limiting its consequences, assigning responsibilities, and notifying the competent authorities and affected individuals where applicable.

In summary, improving compliance requires an integrated approach in which legal requirements are translated into specific technical and organizational practices. The greatest effect can be achieved through a combination of clearly defined policies, reliable access control, encryption, logging, regular training, risk assessment, and periodic internal audits. Only through such a consistent approach can video surveillance systems fulfill their security function without creating unjustified risks to the rights and privacy of monitored individuals.

6. Conclusion

The analysis shows that compliance of video surveillance systems with personal data protection requirements depends on the combined application of regulatory, technical, and organizational measures. The results of the survey conducted among six companies in the sector indicate that a number of positive practices are already being applied, particularly with regard to the technical protection of video data and access control.

At the same time, several areas with potential for improvement have been identified. The most significant differences concern the degree of formalization of internal policies, the lack of systematic staff training, and the absence of sufficiently detailed organizational procedures. This indicates that technological safeguards alone are not sufficient to ensure sustainable compliance.

The findings confirm the need for organizations to regard video surveillance as a comprehensive personal data processing activity. This process should include clearly defined purposes and legal bases, limitation of the scope of surveillance, control over access to recordings, reliable technical protection, logging of actions, staff training, and periodic risk assessment.

Particular importance should be placed on moving from formal compliance with regulatory requirements toward the consistent implementation of specific organizational and technical practices. In this context, internal policies, training, DPIA, periodic reviews, and traceability of actions can be regarded as key elements for reducing the risk of violations and strengthening accountability.

In summary, effective compliance of video surveillance systems requires an integrated approach in which personal data protection is embedded from the design and implementation stages and maintained throughout the entire system lifecycle. Such an approach makes it possible to achieve security objectives while simultaneously reducing risks to the privacy of monitored individuals.

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR).

[2] Personal Data Protection Act, amended, State Gazette, No. 69, 31 July 2026.

[3] European Data Protection Board. Guidelines 3/2019 on Processing of Personal Data through Video Devices, Version 2.0, 2020.

[4] Commission for Personal Data Protection. Practical Guide on Video Surveillance, 2021.

[5] Commission for Personal Data Protection. Good Practices from the Supervisory Activities of the Commission for Personal Data Protection.

[6] Varbanova, G. The Significance of Electronic Evidence in the Context of Cybersecurity and National Security. Varna: Nikola Vaptsarov Naval Academy, 2024. ISBN 978-619-93016-0-9.