Mednarodno inovativno poslovanje
Journal of Innovative Business and Management

Video surveillance legislation in the EU and Slovenia: privacy rights, security needs, and data protection challenges

Benjamin Lesjak*, Mateja Savić**

*doc. dr,
University of Primorska,
Faculty of Management,
benjamin.lesjak@fm-kp.si

**Odvetniška pisarna Stefanovič,
mateja.savic@gmail.com

Abstract: This paper describes the legal framework of video surveillance in the European Union (EU), with an emphasis on the legislation of the Republic of Slovenia. We are analyzing the legal intricacies inherent in balancing privacy rights and security needs. The purpose of the paper is to examine the legislative instruments in the EU and Slovenia, especially regarding the legal basis for processing data of video surveillance. The research methodology combines qualitative analysis and legislative review and case studies from selected Slovenian Information Commissioner opinions and decisions. The findings reveal a dynamic and complex landscape, where technology often outpaces regulatory frameworks, leading to potential privacy infringements. The paper shares the idea that harmonizing legislation across the EU helps ensure the balance between security and privacy rights, with significant practical implications in the creation of standardized policies and guidelines for the operation of video surveillance systems regarding European Data Protection Board opinions. The originality of this paper lies in its selected analysis of EU legislation and its practical application in Slovenian legislation. It distinguishes itself by offering a practical view in ensuring data protection compliance and security technologies regarding video surveillance.
Keywords: video surveillance, GDPR, personal data protection
JEL: M31

DOI 10.32015/JIBM.2023.15.2.3

Mednarodno inovativno poslovanje =
Journal of Innovative Business and Management

ISSN 1855-6175

Zakonodaja o videonadzoru v EU in Sloveniji: pravice posameznika, varnostne potrebe in izzivi varstva osebnih podatkov

Povzetek: Članek opisuje pravni okvir video nadzora v Evropski uniji (EU) s poudarkom na zakonodaji Republike Slovenije. Analiziramo pravne vidike, v povezavi z uravnoteženjem pravice do zasebnosti in varnostnih potreb. Namen članka je pregledati zakonodajne instrumente v EU in Sloveniji, še posebej glede pravnih podlag za obdelavo osebnih podatkov videonadzora. Raziskovalna metodologija združuje kvalitativno analizo, pregled zakonodaje ter študije primerov na podlagi izbranih mnenj in odločitev slovenskega Informacijskega pooblaščenca. Ugotovitve razkrivajo dinamično in kompleksno okolje, kjer tehnologija pogosto prehiti regulativne okvire, kar vodi do morebitnih kršitev zasebnosti. Članek predstavlja idejo, da usklajevanje zakonodaje po vsej EU pomaga zagotavljati ravnotežje med varnostjo in pravicami do zasebnosti, s pomembnimi praktičnimi posledicami pri ustvarjanju standardiziranih politik in smernic za delovanje sistemov videonadzora glede na mnenja Evropskega odbora za varstvo podatkov. Izvirnost tega članka je v izbrani analizi zakonodaje EU in njeni praktični uporabi v slovenski zakonodaji. Odlikuje se z praktičnim pogledom na zagotavljanje skladnosti med varstvom osebnih podatkov in varnostnimi tehnologijami v zvezi z videonadzorom.
Ključne besede: videonadzor, GDPR, varstvo osebnih podatkov

INTRODUCTION

The use of a video surveillance system often plays a key role in ensuring security and control in various environments, such as public spaces, office buildings, shopping centers or medical institutions. Before introducing video surveillance, the controller who implements video surveillance must think about the purposes for which he wants to establish video surveillance and make sure that the implementation of video surveillance will be legal. Due to the intensity of the interference with the individual's privacy, it is advised that before establishing video surveillance and before installing cameras, the controller thoroughly consults with his data protection officer or personal data protection expert.

1. Legal basis for video surveillance according to the General Data Protection Regulation (GDPR)

General data Protection Regulation (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, and repealing Directive 95/46/EC or GDPR,OJ L 119, 4.5.2016, p. 1–88, also GDPR) does not apply to the performance of a completely personal or domestic activity, which is specifically stipulated by Article 2(2)(c) of the GDPR (EDPB, 2020). The exception of processing for domestic needs is interpreted narrowly in accordance with the position of the Court of Justice of the European Union and is limited to the private and family life of individuals, therefore it does not include publication on the internet, where recordings become accessible to an indefinite number of persons, nor should it include public space (ECJ, 2003). The Information Commissioner of the Republic of Slovenia (in original: Informacijski pooblaščenec Republike Slovenije), the supervisory authority of the Republic of Slovenia explained that video surveillance carried out by an individual from his private facility or from one's private property is generally considered as processing personal data for personal use and domestic needs, except as highlighted by the 18th opening clause of the GDPR, when an individual would carry out video surveillance while performing a professional or commercial activity. Use for personal or domestic needs would also be exceeded, if an individual would forward the recordings to an unauthorized third party or publish them on the Internet. The Information Commissioner of the Republic of Slovenia could introduce an inspection procedure regarding the implementation of video surveillance by an individual (because it would be, for example, the publication of a recording on the Internet) only if concrete evidence was provided that the individual is actually recording surfaces that are not owned by him or other people also move on them. The proof would be for example a screenshot of the camera recording on the internet (Informacijski pooblaščenec, 07121-1/2023/1054, 2023).

GDPR provides the fundamental legal basis for the establishment and implementation of video surveillance, while national legislation complements the general regulation of the GDPR. In the Republic of Slovenia, GDPR is supplemented by the national act Zakon o varstvu osebnih podatkov (ZVOP-2, Uradni list RS, št. 163/22), which was last amended on January 26, 2023 and contains provisions regarding the legality of video surveillance. As a result, the rules regarding the legality of establishing and implementing video surveillance in the EU differ slightly between different national jurisdictions, but are always based on the provisions of the GDPR.

Croatia generally regulated the processing of personal data through the implementation of video surveillance in the act Zakon o provedbi Opće uredbe o zaštiti podataka (ZPOUZP, NN 42/18 na snazi od 25.05.2018). This stipulates that video surveillance can only be carried out for a purpose that is necessary and justified for the protection of persons and property,

if this is not overridden by the interests of individuals who oppose data processing with video surveillance (Article 26(1) of the ZPOUZP). In Austria, video surveillance is generally regulated by the Datenschutzgesetz (DSG, BGBl. I No. 165/1999 idgF.), which allows video surveillance of public or non-public areas if it is necessary in the vital interest of a person, if it is ordered or permitted by special statutory provisions, there are overriding legitimate interests of the controller or a third party in a particular case, and proportionality is given and also if the data subject has consented to the processing of the data subject's personal data (Article 12(1-2) of the DSG). The German Bundesdatenschutzgesetz (BDSG, Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097)) allows video surveillance of publicly accessible premises to fulfill the tasks of public authorities, to enforce the right to housing or to protect legitimate interests for specifically defined purposes, when this is necessary and not overridden by the interests of individuals. The law specially stipulates that publicly accessible facilities of a larger scale, such as especially sports, gathering and entertainment facilities, shopping centers or parking lots or vehicles and publicly accessible large facilities of public railway, ship and bus transport are considered to be of particularly important interest from the point of view of protecting the life, health or freedom of the individuals who reside there (Article 4(1) of the BDSG).

The Article 6(1) of the GDPR stipulates that the processing of personal data is legal if the data subject has given consent to the processing of his or her personal data for one or more specific purposes, if processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, if processing is necessary for compliance with a legal obligation to which the controller is subject, if processing is necessary in order to protect the vital interests of the data subject or of another natural person, if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller of if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. In practice, controllers must often refer to Articles 6(1)(f) and 6(1)(e), i.e. to legitimate interest and the need to perform a task carried out in the public interest or in the exercise of official authority.

For the legal establishment and implementation of video surveillance, it is therefore necessary to specifically define the purposes of the processing according to the needs, since video surveillance is not automatically necessary, as long as there are other means to achieve the same purpose (EDPB, 2020). The controller must therefore be able to justify the purpose of video surveillance for each camera and explain why this purpose or the goal cannot be achieved with milder measures (so-called measures that interfere less with the privacy of individuals).The Information Commissioner of the Republic of Slovenia as milder measures cites a video surveillance system that would be directed and would only monitor what is happening at the entrances to the work premises and locking the premises when there are no employees in them (Informacijski pooblaščenec, 0603-29/2023/6, 2023). A milder measure than video surveillance could also be the provision of protection with security personnel, installation of additional locks, anti-graffiti coating of the wall, bars on the windows, etc.

When video surveillance is carried out with the aim of protecting people and property, the legal basis for the implementation of video surveillance will mostly be a legitimate interest, as determined by Article 6(1)(f) of the GDPR. The legitimate interest of the controller of the video surveillance system must be specifically justified, the controller must also ensure that his legitimate interest is not overridden by the interests or fundamental rights and freedoms of the individual to whom the personal data relate, which require the protection of personal data, especially when the individual is, on data subject, child. In other words, the controller

must clearly determine which asset (e.g. property) he wants to protect with video surveillance, ensure that the implementation of video surveillance does not excessively interfere with the privacy of individuals (or that the rights of individuals do not prevail over his interest), limit the recording area in such a way, to record only the protected property and not to interfere with other areas and to take appropriate measures (e.g. limit the period of storage, take measures to secure the video surveillance system ...). The legitimate interest can be of a legal, economic or immaterial nature, it is important that it actually exists and that the need is current, i.e. based on hardship in real life (injuries, incidents) (EDPB, 2020). When justifying the justification of introducing a video surveillance system, records of incidents that happened in the past are useful, e.g. records of damage to property, thefts, riots, security and other incidents. It is also necessary that the video surveillance is carried out only over those parts that it is supposed to protect. For example, if the video surveillance records the cash register, the recording angle must be limited only to the area around the cash register. For the implementation of video surveillance, non-essential parts should be darkened.

Member States of the European Union may introduce special national legislation for video surveillance, but within the scope of the provisions and principles of the GDPR. The establishment and implementation of video surveillance in the public interest or in the exercise of official authority vested in the controller may be based on health and safety and the protection of visitors and employees.

Ultimately, the legal basis for the legal implementation of a video surveillance system can also be the law, when the processing is necessary to fulfill a legal obligation that applies to the controller. The legal basis can thus be the law of the European Union or individual member states.

2. National regulation on video surveillance

On January 26, 2023, the ZVOP-2 amendment brought the most changes precisely in the field of video surveillance. In the third chapter, it regulates individual issues related to the establishment and implementation of video surveillance in more detail. General provisions and requirements for the establishment of video surveillance are defined in Article 76 of the ZVOP-2. The decision on the introduction of video surveillance is taken by the supervisor, director or other authorized individual of a public sector person or a private sector person as controller. The reasons for introducing video surveillance must be explained in the written decision. Every controller who implements video surveillance must also publish a written notice about it, which must be visibly and distinctly published in a way that allows the individual to become familiar with the implementation of video surveillance and to be able to refuse entry to the controlled area. In addition to the information from the first paragraph of Article 13 of the GDPR, the notice must contain the following information: (1) a written or unequivocally graphical description of the fact that video surveillance is being carried out, (2) purposes of processing, indication of the controller of the video surveillance system, telephone number or e-mail address or web address for the purposes of exercising the rights of the individual in the field of personal data protection, (3) information on the specific effects of processing, in particular further processing, (4) contact details of the authorized person (phone number or e-mail address) and (5) unusual further processing, such as transfers to entities in third countries, live monitoring of events, the possibility of audio intervention in in the case of live monitoring. In his opinion, the Information commissioner defined the concept of "special impact of processing", namely neither from the law nor from the explanation of the bill, it is not clear what exactly the legislator envisaged as "special impact of processing". Based on what has been said, the Information Commissioner explains that he does not yet have practice in this area and that he will be able to assess this provision

only in the context of a specific inspection procedure (Informacijski pooblaščenec Republike Slovenije, 2023).

The law stipulates that the information from points three to five can also be published on websites, if the controller publishes the web address where this information is accessible on the notification from the previous paragraph. Taking into account the principles of Article 5 of the GDPR, video surveillance recordings may be kept for a maximum of one year from the moment the recording was created, but it is recommended that, depending on the purpose of the video surveillance, the retention period be limited to the shortest possible time.

2.1 Where can video surveillance be carried out?

Except for exceptions, video surveillance may not be carried out over public areas. Video surveillance is not permitted in elevators, toilets, changing rooms, hotel rooms and other similar spaces where an individual reasonably expects a higher level of privacy, as stipulated by Article 76(5) of the ZVOP-2. When video surveillance is carried out over a space that is jointly owned, the owners who own more than 70% of the common parts must agree to it (Article 77(4) of the ZVOP-2). ZVOP-2 does not regulate the legality of video surveillance in multi-apartment buildings. In the opinion of the Slovenian Information Commissioner, the appropriate legal basis could thus be the exercise of a legitimate interest based on Article 6(f) of the General Regulation, which is pursued by the controller and whose interests are not overridden by the interests or fundamental rights and freedoms of the individual whose data may be processed. In accordance with the housing legislation, the consent of the owners of the multi-apartment building is also required. A certain condominium owner or manager could be authorized to implement video surveillance (Informacijski pooblaščenec Republike Slovenije, 2023).

Controllers of the video surveillance system may carry out video surveillance of access to official work or business premises, if this is necessary for the safety of people or property, to ensure control of entry to or exit from these premises, or if, due to the nature of the work, there is a possibility of endangering employees (Article 77(1) of the ZVOP-2).

The implementation of video surveillance inside the working premises can only be carried out when it is absolutely necessary for the safety of people or property, the prevention or detection of violations in the field of gambling or the protection of classified information or trade secrets, but these purposes cannot be achieved by milder means. In order to implement video surveillance within the working premises, it is necessary to carry out a consultation process. It is forbidden to use video surveillance to record workplaces where the employee usually works, unless this is absolutely necessary (Article 78 of the ZVOP-2). According to the Slovenian Information Commissioner, a violation was established, as the video surveillance was carried out in such a way that it also covered the area of the public area and the area that was not owned or leased by a legal entity, without there was an appropriate legal basis for the processing. Also, video surveillance was carried out inside the workplaces, while the implementation of video surveillance of these workplaces was not necessarily necessary to ensure the safety of people and property or to protect confidential data and business secrets, since the safety of people and property could be more effectively achieved with milder measures. and more effective means (e.g. with video surveillance, which would only record what happens at the entrances to the premises, with an alarm system, by locking the premises, ...) (Informacijski pooblaščenec Republike Slovenije, 2022). The Slovenian Information Commissioner also dealt with the violation of the illegal implementation of video surveillance inside the premises of the organization. The violator carried out video surveillance inside the work premises, namely, he controlled the production halls, filling stations, passageways and dining areas, but the implementation of video surveillance was not absolutely necessary to ensure the safety of people and property, or to protect classified information and trade secrets. The violator was accused that the

safety of people and property located in restricted spaces could be achieved by gentler and more effective means than with permanent video surveillance, for example: by adopting appropriate organizational measures to ensure the safety of employees and property (instructions to workers), video surveillance, which would cover only entrances to the premises, by locking the premises when there are no employees in them, an alarm system, etc. For violation of the illegal implementation of video surveillance, a fine was imposed on the responsible person of the legal entity (director) and the legal entity (organization). It was also established that the violator carried out video surveillance without publishing a notification, the components of which are determined by ZVOP-2 (Informacijski pooblaščenec Republike Slovenije, 2021).

Video surveillance in means of transport intended for public passenger transport may only be carried out in parts of the means of transport intended for passengers, for the purpose of the safety of passengers and property, if this cannot be achieved by other measures that interfere less with the rights of the individual (e.g. the right to privacy ...). The controller must destroy the recordings no later than seven days after their creation. The recordings may be used to assert or defend legal claims or to carry out police duties (Article 79 of the ZVOP-2).

Video surveillance on public areas is permitted only when it is necessary due to the existence of a serious and justified threat to the life, personal freedom, body or health of people, the security of the controller's property or the protection of confidential data of the controller or processor in transmission and these purposes cannot be achieved by other means, which interfere less with individual rights. Video surveillance on public areas is also permitted for the purpose of protecting protected persons and special facilities and the surroundings of facilities protected by the police, the Slovenian Army, the competent authorities in the field of national security, the judicial police, or the protection of other premises, buildings or areas that must be protect on the basis of the law, namely only to the extent and duration necessary to achieve the purpose. Viewing, using or transmitting recordings is only permitted for these purposes. Video surveillance can only be carried out in relation to those nearby or connected parts of the public area and to the extent that it is necessary to protect the interests for which video surveillance is carried out. Video surveillance on public areas can be carried out by a person in the public or private sector who manages the public area or legally performs an activity on it. Video surveillance may only be carried out by officials or authorized security personnel for the public sector, and authorized security personnel for the private sector. Persons or personnel from the previous sentence must be expressly authorized to carry out video surveillance. Video surveillance can also be implemented in such a way that live monitoring of the event is carried out while recording. Video surveillance of public areas for the purpose of protecting persons, confidential data in transmission, trade secrets or property of greater value can also be carried out using a body camera, if it is used by a specially trained person. Footage of video surveillance in public areas can be kept for a maximum of six months from the moment the footage was created. The operator of a video surveillance system that performs video surveillance of public areas must immediately notify the police or another competent entity if the video surveillance system records an event that endangers the health or life of an individual. In the area of video surveillance of road traffic, the controller may only perform video surveillance on predetermined sections of roads in his management, so that no systematic monitoring of the movement of individuals or intrusion into the privacy of individuals is carried out. In accordance with the law, the controller must determine those sections of the road in his management, where it is not possible to achieve the necessary and effective protection of road traffic or its management by other means. The controller of the video surveillance system in the field of road traffic must prepare an Data Protection Impact Assessment (DPIA) containing the location of the road sections before finalizing the locations and submit it for a preliminary opinion to the supervisory authority (Article 80 of the ZVOP-2).

According to the Slovenian Information Commissioner, forests should not be considered as areas in which an individual can reasonably expect a higher level of privacy, therefore the implementation of video surveillance by hunting inspectors in legally defined places is legal, taking into account the provisions of the GDPR and the ZVOP-2, which, among other things means that appropriate warning signs must be installed (Informacijski pooblaščenec Republike Slovenije, 2021).

The use of automatic license plate recognition systems and systems that process biometric personal data is prohibited in public areas (Article 80(10) of the ZVOP-2).

2.2 Live monitoring

In addition to recording, many video surveillance systems also allow for live monitoring of what is happening (the so-called extended eye function or live image), which means that certain employees or responsible persons (directors, principals, owners ...) directly monitor what is happening in front of the cameras at that moment. In his opinion, the Slovenian Information Commissioner explained that live video surveillance is considered to be the processing of personal data, provided that the individuals in the recordings or live images are identifiable, or that they can be identified on the basis of the recordings (Informacijski pooblaščenec Republike Slovenije, 2023). According to the current practice of the Information Commissioner, the monitoring of live images is permissible only in cases where it is necessary to protect property and ensure the safety of people, which can only be ensured by constant monitoring of video surveillance by an authorized person, e.g. security guard. In his decisions on the offense, the Information Commissioner has repeatedly emphasized that the monitoring of the live image cannot be left to e.g. to the director or to other authorized persons who can monitor the events when they have time. In the opinion of the Information Commissioner, the transfer of a live image or access to recordings outside the workplace, via laptops or mobile phones, is inadmissible. Before monitoring the live image, it is necessary to judge whether it is legal.

2.3 The consultation into the footage of the video surveillance system

The consultation, use, or transmission of video surveillance system footage is permissible only for purposes that legally existed or were stated in the notice at the time the footage was captured (Article 76(11) of the ZVOP-2). The Slovenian Information Commissioner addressed violations concerning the transfer of recordings. In one instance, the director of an organization was fined for capturing images from surveillance camera recordings and sending them via email (in a blind copy) to multiple addresses without possessing an appropriate legal basis for such use and disclosure by forwarding or processing the personal data of recorded individuals (Informacijski pooblaščenec Republike Slovenije, 2022). The Information Commissioner also asserted that, even in scenarios of direct monitoring of events captured by cameras, it is imperative to document insights in the processing log (Informacijski pooblaščenec Republike Slovenije, 2023). The controller of the video surveillance system must ensure, for every review or use of recordings, the capability of subsequently identifying which recordings were processed, when and how they were utilized, to whom they were sent, who conducted these processing actions, and the purpose or legal basis of such actions. The controller maintains data on recorded consultations in the processing log for two years following the year they were documented (Article 76(12) of the ZVOP-2).

3. Rights of the data subjects regarding video surveillance

By using the video surveillance system, personal data of individuals is processed, as a result of which they are guaranteed certain rights under the GDPR. The data subject has the right of access to the personal data, the right to erasure ('right to be forgotten') and the right to object.

The individual to whom the personal data relates has the right to find out from the controller of the video surveillance system whether his personal data is being processed, i.e. stored or transmitted or not. Insofar as the individual's data is processed, he has the right to access his data and obtain information, which is determined by Article 15 of the GDPR - the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; the right to lodge a complaint with a supervisory authority; where the personal data are not collected from the data subject, any available information as to their source and the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. However, there are several restrictions that may limit an individual's right of access in some cases. Article 15(4) of the GDPR foresees a negative impact on the rights of others. An indefinite number of individuals may be recorded in a video surveillance sequence, and familiarizing an individual with such a recording would result in the additional processing of personal data of other individuals to whom the personal data relate. In such a case, the controller could implement appropriate technical measures to fulfill the individual's request, such as blurring other individuals, but the controller is not obliged to implement such measures if he can otherwise respond to the request within the expected time frame. Furthermore, Article 11(2) of the GDPR stipulates that when the controller proves that he cannot identify the individual to whom the personal data relates and the individual does not provide additional information, he does not need to fulfill the individual's request and must also inform him accordingly. Article 12 of the GDPR stipulates that, in the case of excessive and clearly unfounded requests from an individual, the controller may charge a reasonable fee or refuse to act (EDPB, 2020).

In the event that the controller continues to process personal data after performing real-time video surveillance, the individual to whom the personal data relates has the right to have the controller erasure the personal data relating to him without undue delay, and the controller has the obligation to delete the personal data without undue delay deletion of delays if the circumstances from Article 17(1) of the GDPR are met, i.e. when personal data are no longer necessary for the purposes for which they were collected or otherwise processed, when personal data were processed illegally, when the individual to whom personal data are concerned, object to the processing, and there are no overriding legal reasons for their processing, and when the individual to whom the personal data relates revokes the consent on the basis of which the processing takes place and when there is no other legal basis for the processing. The blurring of the image without the possibility of retroactive recovery of personal data is considered the deletion of personal data (EDPB, 2020).

When video surveillance is carried out on the basis of a legitimate interest or for the performance of tasks in the public interest, the individual to whom personal data relates has the right to object to the processing of his personal data at any time, based on reasons related to his special situation. The controller must stop processing personal data, unless it demonstrates imperative legitimate reasons for processing that override the interests, rights

and freedoms of the individual to whom the personal data relates, or for the assertion, exercise or defense of legal claims (Article 21 of the GDPR). In the case of video surveillance, an individual can exercise the right to object upon entering the video surveillance area, while being in the area, or after leaving the area (EDPB, 2020).

CONCLUSIONS

Video surveillance is an important instrument for ensuring security and control in various environments. However, when setting up and implementing video surveillance, laws and regulations must be carefully followed to ensure its legality. It follows from the annual report of the Slovenian Information Commissioner for 2022 that in that year he led as many as 155 inspection procedures in the field of video surveillance, which is the third most common reason for the initiation of the procedure. The GDPR represents the fundamental legal basis for the establishment and implementation of video surveillance, which is also supplemented by national legislation. ZVOP-2 foresees fines of up to EUR 30,000 for violation of the provisions on video surveillance.

In order for video surveillance to be legal, it is necessary to define the purposes of data processing and to prove that video surveillance is necessary and that there are no other less invasive means to achieve the same purpose. The legal interest of the video surveillance controller must be specifically justified, and care must be taken to ensure that the interests and rights of individuals do not prevail. It is also important to limit the recording area, observe storage deadlines and take appropriate safety measures.

By complying with the GDPR and national laws, and by prioritizing the rights and privacy of individuals, video surveillance can be legally established and operated, thereby promoting security and control in diverse settings.

REFERENCES

Bundesdatenschutzgesetz (Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858; 2022 I 1045) geändert worden ist").

Datenschutzgesetz (StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.).

European Court of Justice, Judgment in Case C-101/01, Bodil Lindqvist case, 6th November 2003, para 47.

European Data Protection Board. (2019). Guidelines 3/2019 on processing of personal data through video devices, pp. 5-21. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

Informacijski pooblaščenec Republike Slovenije. (2023). Obvestilo o izvajanju videonadzora ter dnevniki obdelave OP, no. 07121-1/2023/205. https://www.ip-rs.si/mnenja-zvop-2/obvestilo-o-izvajanju-videonadzora-ter-dnevniki-obdelave-op-1676964233

Informacijski pooblaščenec Republike Slovenije, Infringement decision no. 0603-86/2022/7, 29th September 2022.

Informacijski pooblaščenec Republike Slovenije, Infringement decision no. 0603-1/2021/8, 24th March 2022.

Informacijski pooblaščenec Republike Slovenije (2023). Infringement decision no. 0603-29/2023/6, 27th June 2023.

Informacijski pooblaščenec Republike Slovenije, Infringement decision no. 0603-82/2022/6, 15th September 2022.

Informacijski pooblaščenec Republike Slovenije. (2023). Izvajanje videonadzora v naravi, no. 07120-1/2023/318. https://www.ip-rs.si/mnenja-zvop-2/izvajanje-videonadzora-v-naravi-1686554965

Informacijski pooblaščenec Republike Slovenije (2023). Snemanje zasebne hiše in objava na spletu, no. 07121-1/2023/495. https://www.ip-rs.si/mnenja-zvop-2/snemanje-zasebne-hi%C5%A1e-in-objava-na-spletu-1692595828

Informacijski pooblaščenec Republike Slovenije. (2023). Videonadzor v živo, no. 07121-1/2023/200. https://www.ip-rs.si/mnenja-zvop-2/videonadzor-v-%C5%BEivo-1676964328

Informacijski pooblaščenec Republike Slovenije. (2023). Vodenje dnevnika obdelave, no. 07121-1/2023/495. https://www.ip-rs.si/mnenja-zvop-2/vodenje-dnevnika-obdelave-1683869643

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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (OJ L 119, 4.5.2016, p. 1–88).

Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18 na snazi od 25.05.2018).

Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22).