

# VIDEO SURVEILLANCE IN THE WORKPLACE UNDER THE CROATIAN ACT ON IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION

Assist. Prof. Nina Gumzej, Ph. D. \*

Prof. Dražen Dragičević, Ph. D. \*\*

UDK: 342.738:349.2(497.5)

342.738:331.108.2(497.5)

DOI: 10.3935/zpfz.69.3.01

Izvorni znanstveni rad

Primljeno: prosinac 2018.

*The authors critically evaluate the legislation and practice in Croatia on video surveillance in the workplace, focusing in particular on the recently adopted GDPR Implementation Act. This act prescribes rules on the processing of personal data through video surveillance systems, as well as its own maximum administrative fines for violations of some of those rules. Additionally to the new rules on video surveillance of work premises, the authors examine the new general rules on data processing by video surveillance and the related rules on administrative fines, as well as the earlier acts on which the GDPR Implementation Act relies. The goal of this research is to establish if the new rules provide the necessary clarity and legal certainty in relation to existing legislation and practice, as well as compatibility thereof with the GDPR. With the disclaimer that the analysis of the legal bases for processing workers' personal data and of corresponding case law is excluded from the scope of this paper, the authors also briefly point to GDPR rules which the employers, human resources personnel and legal professionals ought to consider when assessing legal compliance of workplace video monitoring. Concluding critical remarks will also deliver de lege ferenda proposals towards amendment of certain examined rules of the GDPR Implementation Act so as to ensure greater legal clarity and legal certainty as well as consistency with the GDPR.*

*Keywords: Croatian Act on Implementation of the General Data Protection Regulation, General Data Protection Regulation, Video Surveillance, Personal Data, Workplace*

---

\* Nina Gumzej, Ph. D., Assistant Professor, Faculty of Law, University of Zagreb, Trg Republike Hrvatske 14, Zagreb; ngumzej@pravo.hr;

ORCID ID: [orcid.org/0000-0002-7434-3538](https://orcid.org/0000-0002-7434-3538)

\*\* Dražen Dragičević, Ph. D., Professor, Faculty of Law, University of Zagreb, Trg Republike Hrvatske 14, Zagreb; drazen@pravo.hr;

ORCID ID: [orcid.org/0000-0001-7364-8439](https://orcid.org/0000-0001-7364-8439)

## 1. INTRODUCTION

With the aid of information and communication technology, the nature and extent of surveillance of persons has significantly proliferated over the past years globally. Where video surveillance (video monitoring) is concerned, in European legal terms a person's recorded image constitutes *personal data* inasmuch as it makes it possible to identify that person, and video surveillance systems entail the *automatic processing of personal data*.<sup>1</sup> While ensuring that security of property and persons is a common purpose for which video surveillance is carried out, when used by employers for work control (measuring efficiency, productivity, etc.), they will, due to potential consequences for employees' position and their fundamental right to personal data protection, be scrutinized under European data protection legislation and often also be subject to labour rules.

With the EU General Data Protection Regulation<sup>2</sup> (hereinafter: GDPR) and its "sound system for the protection of individuals"<sup>3</sup>, the criteria for workplace monitoring in compliance with data protection became more challenging to fulfill. Added to this complexity are the different national rules that may be adopted, since personal data processing in the employment context is one of the areas (Chapter IX) in which the Member States are free to prescribe their own rules. Those rules must, however, follow relevant GDPR provisions. First of all, they must include suitable and specific measures to safeguard employees' dignity, legitimate interests and fundamental rights, with particular regard to, *inter alia*, transparency of processing and *workplace monitoring systems* (Article 88). Next, in all cases of non-compliance with the national rules adopted on the basis of the GDPR, the data protection supervisory authorities may issue a maximum administrative fine of up to 20 million EUR, or in case of an undertaking up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83 para. 5d). The GDPR specifies only the upper limits of administrative fines, which are to be issued with very careful consideration of each and every individual case in line with the prescribed criteria

---

<sup>1</sup> Court of Justice of the EU, judgment, C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, EU:C:2014:2428, points 22-25.

<sup>2</sup> Regulation (EU) 2016/679 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, Official Journal of the European Union L 119, 4.5.2016, pp. 1-88.

<sup>3</sup> de Hert, P.; Papakonstantinou, V., *The new General Data Protection Regulation: still a sound system for the protection of individuals?*, Computer Law & Security Review, vol. 32, no. 2, 2016, pp. 179-194.

and there is ample guidance<sup>4</sup> for supervisory authorities on their application, *inter alia* where natural persons and not legal persons are in breach (Article 83 and recitals 148, 150, 151). Also, Member States are to prescribe rules on other penalties (including criminal) applicable to GDPR violations, especially those not subject to administrative fines, which must be effective, proportionate and dissuasive (Article 84 and recitals 149, 152).

Of other GDPR provisions relevant for the area of video surveillance, it is also important to have in mind Member States' discretion to implement *restrictions* on certain obligations and rights (*e.g.* on the data protection transparency principle), when that restriction respects the essence of fundamental rights and freedoms and where it is a necessary and proportionate measure in a democratic society, in order to safeguard *inter alia* the protection of data subjects or rights and freedoms of others, public security, prevention, investigation, detection or prosecution of criminal offences, *etc.* (Article 23).

In this paper we will critically assess the legislation and practice in the Republic of Croatia on the topic of workplace video surveillance, with a special focus on the recently adopted GDPR Implementation Act, which contains several rules on video surveillance data processing and sets its own maximum administrative fines for their breach. In addition to the rules on surveillance of work premises, we will also closely examine the new general rules on data processing by video surveillance and existing laws, which the former rules rely on. The aim of this research is to assess if the new rules introduce the needed clarity and legal certainty in this area in relation to existing legislation and practice, and especially in light of the directly applicable GDPR rules, including those on administering fines. We will next briefly point to key GDPR rules that the Croatian employers, human resources personnel and legal practitioners should consider to ensure compliance with the GDPR and the local legislation in implementing future (or existing) employee video surveillance systems. Due to the limited scope of this paper we will not be dealing with the legal bases for processing employees' data and the related judicial and regulatory case law. The results of the overall analysis will serve to deliver concluding critical remarks with *de lege ferenda* proposals towards amendment of the act in order to ensure better legal clarity and certainty of the analyzed new rules, alignment with the GPDR, and proposed local regulation of an important topic of employee monitoring.

---

<sup>4</sup> Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 17/EN, WP 253, 3.10.2017.

## 2. NATIONAL LEGISLATION AND PRACTICE

### 2.1. Sector-specific legislation

Workplace privacy and data protection is, in addition to general data protection rules, regulated in Croatia also by sector-specific laws, in particular the *Labour Act*<sup>5</sup> and the *Occupational Safety Act*<sup>6</sup>. Mandatory video surveillance may be governed by special laws due to industry or job peculiarities, such as in relation to monetary institutions.<sup>7</sup>

Data protection provisions in an employment context are generally stipulated in the Labour Act. Workers' personal data may be processed and delivered to third parties only if so specified by this or another act or if necessary for the exercise of rights and obligations from or relating to employment. Incorrectly recorded personal data must be immediately rectified and the data for the retention of which there are no longer legal or actual reasons must be erased or otherwise removed. If the data are required to be processed or delivered to third parties to exercise rights and obligations arising from or relating to employment, the employer must determine such processing beforehand in work regulations, *i.e.*, by-laws. Only the employer, or a formally appointed representative, may process and deliver such data to third parties. Employers who employ at least twenty workers must appoint a person who enjoys workers' confidence and who is, apart from the employer himself, authorized to monitor if workers' personal data are processed and provided to third parties in accordance with the law (Article 29). This person may be also the data protection officer.<sup>8</sup>

It is important to point here also to the relevant rules of the Labour Act on mandatory involvement of the Workers' Council (or a trade union representative if there is no Council). To be more specific, the employers must seek Workers' Council's (prior) approval before adopting a decision on the processing and transfer of employees' personal data (Article 151, para. 1, point 7). In particular, they must consult with the Council before adopting a decision *relevant for employees' position* that includes *inter alia* decisions on measures related to health

---

<sup>5</sup> Zakon o radu, Official Gazette of the Republic of Croatia Nos. 93/14 and 127/17.

<sup>6</sup> Zakon o zaštiti na radu, Official Gazette of the Republic of Croatia Nos. 71/14, 118/14 and 154/14.

<sup>7</sup> Act on the Protection of Monetary Institutions (Zakon o zaštiti novčarskih institucija), Official Gazette of the Republic of Croatia no. 56/15.

<sup>8</sup> Bet Radelić, B., *Zaštita osobnih podataka u radnim odnosima*, Radno pravo, no. 9, 2017, pp. 3-10, at p. 7.

and safety at work, and introduction of new technology and changes in the organization and mode of work (Article 150, paras. 1 and 3). In a well-publicized judgment on video surveillance in the working area for bottling beverages, where employees who performed the bottling were directly monitored, such monitoring was prohibited as its introduction was in fact the employer's decision important for employees' position, for which the employer failed to consult with the Workers' Council.<sup>9</sup>

Video surveillance for work safety and security purposes is regulated by the *Occupational Safety Act* (Article 43). Use of surveillance is allowed only for the purposes of: (1) controlling entries into and exits from work premises and (2) reducing exposure of workers to risk of robbery, burglary, violence, theft and similar events at work or in connection with work. Monitoring cannot cover areas intended for personal hygiene and changing rooms. The employer may not use recorded material for purposes other than those prescribed in the act, may not broadcast them in public or to persons who are not authorized to supervise general safety and health at work, and is obliged to ensure that the recordings are not made available to unauthorized persons. Employers must notify the employees on the monitoring in writing at the time of hiring. Furthermore, employers may only use video surveillance upon *prior consent of Workers' Council* (or trade union representative if there is no Council in line with the Labour Act<sup>10</sup>) in case of continuous monitoring of all movements of employees during their work or if devices are placed so that the employees are in their field of vision at all times during work (evidently the highly intrusive nature of such monitoring warrants stricter requirements than the Labour Act). A breach of these rules is not subject to monetary fines under this act, though monitoring may be prohibited in inspection proceedings, *e.g.* until shortcomings such as failure to inform the employees have been removed (Article 91).<sup>11</sup>

According to earlier practice of the Personal Data Protection Agency (*i.e.*, prior to the GDPR and under the Personal Data Protection Act<sup>12</sup>), data obtained

---

<sup>9</sup> County Court in Zagreb, judgment, Gžr-389/07-2, 22.4.2008.

<sup>10</sup> Amendments to Occupational Safety Act were recently proposed to specify also union representatives in this rule in line with the Labour Act: Ministry of Labour and Pension System, *Draft Act on Amendment of the Occupational Safety Act*, May 2018, <https://vlada.gov.hr/UserDocsImages//Sjednice/2018/05%20svibnja/96%20sjednica%20VRH//96%20-%203.pdf> (2 July 2018).

<sup>11</sup> Gović Penić, I., *Povreda privatnosti radnika kao žalbeni razlog u radnom sporu*, IUS-info, 20.7.2017.

<sup>12</sup> Zakon o zaštiti osobnih podataka, Official Gazette of the Republic of Croatia nos. 103/03, 118/06, 41/08, 130/11 and 106/12.

by use of video surveillance may constitute personal data.<sup>13</sup> Also, according to its earlier opinions employee video surveillance must be regulated with by-laws, so that the data protection transparency principle towards employees is met prior to the collection of their data. To be more exact, as argued already early in Croatian literature, any autonomous legal act on workplace surveillance (e.g. company by-laws) should be clear and easy to understand and it should include the scope of application, goals and reasons for introducing monitoring systems<sup>14</sup>. Furthermore, according to the Agency, employers, as data controllers, must take all necessary technical and organizational measures to ensure data confidentiality, including designation of persons authorized to access the data, and the retention period. It is necessary to clearly and unambiguously mark, by image and text, that work premises are monitored. All these requirements were also explicitly confirmed by the Ministry of Economy, Entrepreneurship and Crafts.<sup>15</sup> To be noted here is also the relatively recent decision of the Agency by which it prohibited invasive video surveillance systems that continuously monitored movements of employees in a public authority, where the nature of work itself did not require such invasive monitoring of closed work offices and job positions. The Agency found no legitimate purpose and no legal basis for such monitoring and hence found that the employees' rights to privacy and dignity in the workplace were gravely violated.<sup>16</sup>

---

<sup>13</sup> Personal Data Protection Agency, Opinions, *Video nadzor u poslovnim prostorijama*, <https://azop.hr/upotreba-videonadzora/detaljnije/video-nadzor-poslovnim-prostorijama>, 14.10.2015; *Privacy protection in the workplace-Guide for employees*, 2014, [https://azop.hr/images/dokumenti/252/guide\\_for\\_employees.pdf](https://azop.hr/images/dokumenti/252/guide_for_employees.pdf), p. 23 (2 July 2018). See also Decision of 31.10.2008, class: 004-02/08-01/138, reg. no.: 567-04/02-08-2 and Opinion of 31.1.2013, in: Gotovac, V. *et al.*, *Komentar Zakona o radu*, TEB-Poslovno savjetovanje, Zagreb, 2014, pp. 131-132.

<sup>14</sup> Bodiroga Vukobrat, N.; Martinović, A., *Izazovi novih tehnologija na radnom mjestu*, Zbornik Pravnog fakulteta u Rijeci, vol. 30, no. 1, 2009, pp. 63-89, at p. 87.

<sup>15</sup> Ministry of Economy, Entrepreneurship and Crafts, *Opinions and Interpretations*, 4.3.2015, Ius-Info.

<sup>16</sup> Personal Data Protection Agency, Decision of 9.12.2016, <https://azop.hr/images/dokumenti/490/videonadzor-radno-mjesto.pdf>; *Report on Work for 2016*, June 2017, <https://azop.hr/images/dokumenti/217/godisnje-izvjesce-o-radu-za-2016-godinu.pdf>, p. 9.

## 2.2. The GDPR Implementation Act

The recently adopted *Act on Implementation of the General Data Protection Regulation*<sup>17</sup> (hereinafter: national implementation act, national act or act) replaced the earlier Personal Data Protection Act as of its entry into force on 25.5.2018. The act contains only a few substantive legal norms implementing the GDPR, of which most regulate the processing of personal data by video surveillance (general provisions, video surveillance of work premises, residential buildings and public areas, which co-exist with the sectoral legislation analyzed above (Articles 25-32)).

According to the general provisions on video surveillance, such monitoring refers to the collection and further processing of personal data that involves the making of recordings forming or intending to form part of the storage system. Unless otherwise prescribed by another act, the processing of personal data by video surveillance is subject to this act. Such processing may only be carried out for a purpose that is *necessary and justified for the protection of persons and property* unless there are prevailing interests of data subjects contravening such processing. Monitoring may only cover rooms, parts of business premises, outer surface of the building as well as the interior of public transport vehicles, the surveillance of which is necessary for the above mentioned purposes. The act prescribes a retention period of up to six months for video recordings, unless other acts provide for a longer period or if they are used as evidence in court, administrative, arbitration or other equivalent proceedings. Competent state bodies may access personal data collected by video surveillance in the performance of their statutory duties.

The act specifies its own *maximum administrative fines* for certain breaches of general video surveillance rules, which amount to up to 50,000 HRK, which is approx. 6,770 EUR (Article 51). The first breach falling in the scope of these fines is where the data controller and processor fail to indicate the object, premises, parts of the premises and outer surface of the building *as prescribed in this act*. To be more specific, relevant Article 27 of the act prescribes that the controller (or processor, where applicable) must indicate that the building, or a particular space in that building and the building's outer surface is under video surveillance, and that this notice must be visible at the latest when entering the monitored area. This article also stipulates that the notice must contain all information under Article 13 of the GDPR (transparency principle), and in

---

<sup>17</sup> Zakon o provedbi Opće uredbe o zaštiti podataka, Official Gazette of the Republic of Croatia no. 42/18.

particular a simple and easily understandable image with the information: (1) that the space is monitored, (2) details on the data controller, and (3) contact information so that data subjects may exercise their rights.

Especially since the GDPR transparency principle (Article 13) was not restricted (Article 23), we see no justifiable legal basis for the adopted national rules on transparency specifically in relation to video surveillance. To be more exact, there is no other possibility to fulfill the transparency principle under the GDPR, *i.e.*, notifying the data subject at the time of collecting their personal data, *without providing them on site with information on video surveillance*. In other words, were the rule not implemented, data protection notices and images on video surveillance would nonetheless be obligatory under existing Croatian legislation and practice regulating video surveillance (prior to the GDPR) and now, of course, the GDPR as properly applied in relation to the specific video surveillance technology. This would imply that the only practical significance of the adopted rule and the related fine lies in a significant reduction of maximum fines for a breach of the transparency principle, for which, under the GDPR, supervisory authorities may issue a maximum fine of up to 20 million EUR, or in case of an undertaking up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83, para. 5b). There is, in any case, a lack of clarity in the adopted provisions as to which infringement of transparency is subject to the national administrative fine, since the national act refers to infringement of its entire Article 27. If that is the case it could be argued that the act provides special (unfair) treatment of operators of video surveillance in relation to other controllers and processors who are obliged by the GDPR's transparency principle in relation to any other personal data processing situation where the data are collected from data subjects, who must be provided with information on the data processing at the time of the collection.

The second infringement subject to national fines is where the data controller and processor *fail to establish an automated record system for recording access to video recordings*. To be specific, video surveillance systems must be protected against access by unauthorized persons and, to that effect, the data controller and processor are obliged to establish an automated record system for logging access to recordings, which includes information on the time and place of access as well as on persons accessing the data.

The third and last infringement targets persons who are, under the act, allowed access to the data collected by video surveillance (responsible person of the data controller or processor and/or person authorized by him/her), and who are prohibited from using recordings contrary to the prescribed purposes.



The question imposing itself is if the prescribed violations in the national act can legally qualify as infringements that are not already covered by maximum administrative fines under the GDPR. In our opinion, from a legal point of view, they cannot or at the very least they should not. Both here mentioned violations of the national act would qualify as breaches of the GDPR requirements: (1) data controller's, *i.e.*, video surveillance operator's accountability in connection with the principles relating to personal data processing (Article 5); (2) data controller's responsibility to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that the processing is performed in accordance with the GDPR (Article 24 para. 1), and more concretely (3) a breach of the duty to implement data protection by design (Article 25 para. 1), and above all (4) a breach of the duty to ensure data security (Article 32 para. 1). Breaches of the above mentioned duties of data protection by design and data security under the GDPR are subject to a fine of up to 10 million EUR, or in the case of an undertaking up to 2 % of total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83 para. 4a). There is, in our opinion, no justification why significantly smaller administrative fines for violations of crucial data security duties of video surveillance operators are prescribed by the national act. Unauthorized access to / use of video records should be punishable equally whether by authorized or unauthorized persons. Next, logging access to video recordings is in fact a technical *sine qua non* measure for observing the GDPR's accountability and security principles, securing monitoring systems/records from unauthorized access and use, and for handling personal data breaches (Articles 5, 32-34). Furthermore, without logging systems, both data subjects and operators of systems are unable to make their case in proving (un)authorized access and/or use of recordings.<sup>18</sup>

Workplace monitoring is specifically regulated by the provision in the new act titled *Video Surveillance of Work Premises* (Article 30). The relevant provision prohibits the monitoring of recreational, personal hygiene and changing facilities, which corresponds largely to the earlier noted rule in the Occupational Safety Act. The new rule also stipulates that the processing of personal data of employees through video surveillance may only be carried out *if in addition to the conditions laid down by this act*, the conditions laid down by the rules governing occupational safety are also fulfilled and if employees have been adequately informed in advance of such measure and if the employer has informed employees before deciding to set up a video surveillance system.

---

<sup>18</sup> In this context see the judgment of the European Court of Human Rights, Case of I v. Finland, Application no. 20511/03, 17.7.2008.

Violations of this rule are not subject to administrative fines in the national act. However, any breach of the general surveillance rules that is subject to the fine and which occurs in the context of the monitoring of work premises could be interpreted as being subject to the national fine. In that sense, we add here the same observations as provided earlier in the paper on those general rules. Also, should this rule qualify as a national rule on employment data processing adopted under the GDPR's Chapter IX, we remind of the applicability of GDPR administrative fines in all cases of violations of such national rules.

The national act did not tackle the important question of whether surveillance can be instituted to monitor employees' efficiency or for disciplinary proceedings (*e.g.* in cases of employees suspected of theft, *etc.*). The only reference to this issue discussed in connection with the act may be found in the Government's replies to comments on an employer's legitimate interest to use personal data from video records in disciplinary proceedings, which it had received during public consultations on the proposed act. It replied that the act does not prevent employers from using records for other purposes as that is regulated by the GDPR (conditions when the data may be processed for a different purpose than that of collection, Article 6 para. 4).<sup>19</sup> This reasoning is, in our opinion, inconsistent with another employment-related rule that we have identified in the act, according to which it is prohibited to use video surveillance in residential buildings for the purposes of monitoring work efficiency of house-keeping personnel (Article 31 para. 3.). No fines are prescribed for a breach of the rule, which we believe could qualify as a rule adopted under the GDPR's Chapter IX.

### 3. WORKPLACE SURVEILLANCE AND THE GDPR

#### 3.1. Record-keeping duties

If employers regularly monitor employees by video, they must under the GDPR keep records of such processing *regardless of their size*.<sup>20</sup> No record-keeping duties will apply to employers who undertake only occasional monitoring where

---

<sup>19</sup> Government of the Republic of Croatia, *Final Proposal of the Act on Implementation of the General Data Protection Regulation*, class: 022-03/17-01/171; filing no.: 50301-25/06-18-8, 12.4.2018.

<sup>20</sup> Article 29 Data Protection Working Party, *Position paper on derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19.4.2018, [http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc\\_id=51422](http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422) (2 July 2018).

they are micro, small or medium-sized enterprises and organizations (employing less than 250 persons) if monitoring is not likely to result in risks to employees' rights and freedoms and does not include special data categories or data relating to criminal convictions and offences (Article 30 para. 5 and recital 13).

### 3.2. Data protection impact assessments and profiling

Where video surveillance entails high-risk processing of employees' personal data, employers must carry out *data protection impact assessments* (further also as: DPIA), and if the DPIA shows that in the absence of risk-mitigating measures surveillance would result in a high risk, employers must consult the supervisory authority before such monitoring (Articles 35-36 and recitals 75, 84, 89-96). Of the GDPR-prescribed circumstances for mandatory DPIAs we would highlight the one where surveillance activities entail systematic and extensive evaluation of personal aspects relating to employees, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning them or which similarly significantly affect them. In addition to the prescribed mandatory DPIAs in the GDPR, national supervisory authorities may prescribe further examples. The Croatian Personal Data Protection Agency has accordingly established<sup>21</sup> several circumstances where DPIAs are mandatory, of which we would point to the one where employees' personal data are processed using applications or tracking systems (*e.g.* processing personal data for monitoring work, movement, communication, etc.). This is in line with the GDPR and the European Data Protection Board's criteria for establishing mandatory DPIAs, in particular when taking into account the criterion of employees as vulnerable groups.<sup>22</sup> Also to be noted here is the right of all data subjects, and thus also of employees, not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects concerning them or similarly significantly affect them (*e.g.* advancement, job termination, etc.).

---

<sup>21</sup> Personal Data Protection Agency, *Decision on establishment and publication of the list of types of processing procedures subject to data protection impact assessment requests*, class: 004-04/18-01/01; reg. no.: 567-01/01-18-01, 25.5.2018.

<sup>22</sup> Recital 75 of the GDPR; Article 29 Data Protection Working Party, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN, WP 248 rev.01, adopted 4.4.2017 - as last revised and adopted 4.10.2017; *The Board endorsed Article 29 Working Party's interpretations of the GDPR: Endorsement 1/2018*, 25.5.2018, [https://edpb.europa.eu/sites/edpb/files/files/news/endorsement\\_of\\_wp29\\_documents\\_en\\_0.pdf](https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf) (2 July 2018).

Such processing may *inter alia* consist of profiling to analyze or predict aspects of their work performance (Article 22 and recitals 71-72).

### 3.3. Security of personal data and personal data breaches

Employers operating video surveillance systems must take strict security measures in line with relevant GDPR provisions and implement appropriate technical and organizational measures to ensure security levels appropriate to risks, as well as notify a personal data breach (Article 4 para. 12) to the supervisory authority, as well as to affected data subject(s) in certain cases (Articles 32-34).

### 3.4. Appointing DPOs

Employers carrying out regular and systematic workplace surveillance on a large scale must appoint data protection officers, as must all employers (regardless of nature of monitoring) who are a public authority or body and employers whose core activities entail the processing on a large scale of special categories of data and personal data relating to criminal convictions and offences (Article 37 and recital 97).

## 4. CONCLUDING REMARKS

Despite the already existing sectoral legislation, the Croatian legislator made it a priority to regulate video surveillance also in the act implementing the GDPR. However, the act leaves a number of questions unanswered (in particular) in relation to employee video surveillance. Especially taking into account the discretion afforded to Member States to legislate the processing of personal data in the employment context, regrettably this act shows a missed opportunity to have this area regulated clearly and in detail. While it may be regulated also by other acts, Member States were due to notify the Commission of any such rules by 25.5.2018 and, to the best of our knowledge, no such rules were passed even after this deadline, not even to incorporate references to the GDPR (e.g. in the Labour Act).

Our analysis showed that the regulated purposes for video surveillance in the national act mainly remained the same as under the Occupational Safety Act. In our opinion, the examined rules in the national act represent no significant development in this area, though certain specific measures, such as the data retention period, are welcome as this would otherwise need to be

interpreted under the GDPR and possibly implemented differently in different sectors. In particular, the act failed to regulate in detail the burning question of whether employee video surveillance can, and if so under which conditions, be instituted for the sole purpose of monitoring workers' efficiency and/or disciplinary proceedings (*e.g.* in cases of suspected theft, *etc.*), and whether workers' personal data processed in connection with video surveillance can be used for that purpose, in cases where surveillance was initially instituted for security reasons. Consequently, in all such cases Croatian employers should, in addition to observing the GDPR and sector-specific laws, carefully assess their particular needs in that respect, consult pertinent case law in this area, and in particular newer decisions of the European Court of Human Rights<sup>23</sup>, any opinions of the Personal Data Protection Agency, as well as important interpretative documents on this subject, such as in particular those issued by the Article 29 Data Protection Working Party (now the European Data Protection Board).<sup>24</sup> While examination of the former as well as of the legal bases for processing personal data by video surveillance goes beyond the scope of this paper, on the basis of our analysis we consider that in such cases the employers should: (1) consult the Workers' Council prior to initiating video surveillance and seek its approval according to sector-specific legislation, and carefully regulate this area in employee by-laws and contracts, advisably so that the workers are regularly reacquainted with those rules; (2) appoint a data protection officer; (3) carry out a DPIA and throughout this process especially consider GDPR requirements in cases of automated-decision making and profiling procedures affecting employees, and (4) apply appropriate security measures with respect to both the video monitoring system and video recordings.

In our analysis of those rules in the national act, infringements of which are subject to maximum administrative fines set out therein, we considered the following GDPR rules: (1) all cases of non-compliance with national rules adopted on the basis of Chapter IX (including rules on data processing in employment) are subject to a maximum administrative fine set out therein; (2) penalties (*e.g.* criminal) may be prescribed in national acts for GDPR infringements, especially for those not already subject to GDPR administrative fines; (3) the GDPR allows Member States to implement restrictions on certain obligations and rights

---

<sup>23</sup> Karin Köpke v. Germany, Application no. 420/07, decision, 05.10.2010; Antović and Mirković v. Montenegro, Application no. 70838/13, judgment, 28.11.2017 (final: 28.2.2018); López Ribalda and Others v. Spain, Applications nos. 1874/13 and 8567/13, judgment, 09.1.2018 (not final - referred to the Grand Chamber).

<sup>24</sup> Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, 17/EN, WP 249, 8.6.2017.

under prescribed conditions. As regards the latter, we found no restrictions were implemented in the act in respect of the analyzed provisions. Next, all or at least most of the examined infringements of the national act subject to an administrative fine set out therein may legally qualify as infringements that the GDPR already covers, which is further aggravated by the fact that the act imposes significantly smaller maximum fines in relation to the GDPR. One exception could be a violation of the rule on the image on video surveillance with three basic sets of information, which, in our opinion, may be subject to an individual penalty in the act even in the form of an administrative fine. However, due to the wording of the relevant rule that points to violations of the entire principle of transparency (GDPR), such interpretation would either require an amendment of the act to that effect, or at the very least a corresponding authoritative interpretation. In other words, a clear delineation could be made between a notice with image and the three sets of minimum information (subject to a national fine), and a detailed notice containing all required information in Article 13 of the GDPR (subject to a GDPR fine). Considerations of legal certainty in any case call for an appropriate amendment of the relevant rule on fines (Article 51) and on transparency (Article 27).

Considerations above apply also to the rule on video surveillance in work premises, as general rules on surveillance also apply to it. The situation here is more complex, however, as it could also be argued that rules on video surveillance of work premises (including the rule on prohibited use of video surveillance in residential buildings to monitor work efficiency of house-keeping personnel) fall within the scope of national rules adopted in the employment context (Chapter IX of GDPR), the breach of which is subject to GDPR fines. However, any breach of the general video surveillance rules that are, under the act, subject to the maximum fine prescribed therein, when occurring in the context of the monitoring of work premises, could be interpreted in practice as being subject solely to the national administrative fine. This precarious situation is even further aggravated in all cases of video surveillance conducted by public authorities in violation of the GDPR and/or the national act, due to the introduced *exoneration of public authorities* (state administration bodies and other state bodies as well as units of local and regional self-government) *from administrative fines both under the GDPR and the act* (Articles 3 para 2. and 47 of the act, Article 83 para. 7 of the GDPR, respectively). To be more specific, in the context of infringements of both the GDPR and the act, while exoneration or lessening of fines towards public authorities and bodies is indeed allowed under the GDPR (Article 83 para. 7), complete exoneration from fines represents a shift away from the rule on effective, proportionate and dissuasive fines (Article 83 para. 1) as regards public authorities, from which the general public normally expects high regard

for legal norms and fundamental rights and freedoms. While the goal of the new data protection framework (GDPR) is certainly not that of imposing (significant) fines in all cases, effective deterrence from non-compliant behavior is its crucial element in order for it to “survive”. However, what we have here is legislated blanket maximum tolerance for even the gravest and persistent violations conducted by public authorities. Of the published decisions of the Personal Data Protection Agency on illegal video surveillance, the one examined in the paper that stands out for its overly intrusive nature towards employees, concerned in fact the responsibility of a public authority.

Despite negative comments on the proposed complete exoneration of public authorities (as opposed to the option of a possible reduction of fines), the Government persistently justified it by quoting that collecting fines from public authorities would only result in transfers of budgetary resources from one budgetary item to another.<sup>25</sup> According to available information on GDPR implementation acts adopted in other Member States, a similar legislative initiative was made in Ireland. However, following a parliamentary debate<sup>26</sup> the finally adopted act introduced only a reduced maximum administrative fine of up to (still significant) 1 million EUR for public authorities and public bodies that do not compete with the private sector.<sup>27</sup> At the very least the Croatian act should have, in such cases, prescribed corrective powers, such as the publishing of non-anonymized findings and decisions in all cases of established irregularities where video surveillance is operated by a public authority. That would require an amendment of the already existing rule in the act, which requires similar publishing in other circumstances (Article 48).

At a broader level, the analysis of the national act showed uncertainty in establishing “consistent enforcement of the data protection rules”, which is “central to a harmonized data protection regime” under the GDPR.<sup>28</sup> The here established problem of locally prescribed administrative fines and the impact

---

<sup>25</sup> *Records of Comments to the Act on Implementation of the General Data Protection Regulation, E-consultations, 30 days*, in: Government of the Republic of Croatia, Final Proposal of the Act on Implementation of the General Data Protection Regulation, class: 022-03/17-01/171; filing no.: 50301-25/06-18-8, 12.4.2018, pp. 3 *et seq.*

<sup>26</sup> Houses of the Oireachtas, *Data Protection Act 2018 - Debates*, <https://www.oireachtas.ie/en/bills/bill/2018/10/?tab=debates> (2 July 2018).

<sup>27</sup> Irish Data Protection Act 2018, section 141, <http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print#sec1> (2 July 2018).

<sup>28</sup> Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 17/EN, WP 253, 3.10.2017, p. 4.

thereof on consistent enforcement of data protection rules in the EU is rather new. Furthermore, not all EU Member States have yet passed their implementation laws and/or sector-specific legislation in the area, and there is currently little focus on this issue, especially in academic literature. In order to deepen the understanding and intensity of the problem, the results of this analysis will serve as a good starting point for further research into the specifics of local legislation adopted in this area in other Member States.

## BIBLIOGRAPHY

- Bet Radelić, B., *Zaštita osobnih podataka u radnim odnosima*, Radno pravo, no. 9, 2017, pp. 3-10.
- Bodiroga Vukobrat, N.; Martinović, A., *Izazovi novih tehnologija na radnom mjestu*, Zbornik Pravnog fakulteta u Rijeci, vol. 30, no. 1, 2009, pp. 63-89.
- de Hert, P.; Papakonstantinou, V., *The new General Data Protection Regulation: still a sound system for the protection of individuals?*, Computer Law & Security Review, vol. 32, no. 2, 2016, pp. 179-194., <https://doi.org/10.1016/j.clsr.2016.02.006>
- Gotovac, V. et al., *Komentar Zakona o radu*, TEB-Poslovno savjetovanje, Zagreb, 2014.
- Gović Penić, I., *Povreda privatnosti radnika kao žalbeni razlog u radnom sporu*, IUS-info, 20.7.2017.

## CASE LAW

### Court of Justice of the EU

C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, EU:C:2014:2428.

### European Court of Human Rights

- I v. Finland, Application no 20511/03, judgment, 17.7.2008.
- Karin Köpke v. Germany, Application no. 420/07, decision, 05.10.2010.
- Antović and Mirković v. Montenegro, Application no. 70838/13, judgment, 28.11.2017 (final: 28.2.2018).
- López Ribalda and Others v. Spain, Applications nos. 1874/13 and 8567/13, judgment, 09.1.2018 (not final - referred to the Grand Chamber).



## County Court in Zagreb

Gžr-389/07-2, judgment, 22.4.2008.

## Decisions of the Personal Data Protection Agency

Decision of 31.10.2008, class: 004-02/08-01/138, filing no: 567-04/02-08-2, in: Gotovac, V. *et al.*, *Komentar Zakona o radu*, TEB-Poslovno savjetovanje, Zagreb, 2014, pp. 131-132.

Decision of 09.12.2016, <https://azop.hr/images/dokumenti/490/videonadzor-rad-no-mjesto.pdf>

## LEGISLATION

Act on Implementation of General Data Protection Regulation (Zakon o provedbi Opće uredbe o zaštiti podataka), Official Gazette of the Republic of Croatia no. 42/18.

Act on the Protection of Monetary Institutions (Zakon o zaštiti novčarskih institucija), Official Gazette of the Republic of Croatia no. 56/15.

Irish Data Protection Act 2018, <http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print#sec1> (2 July 2018).

Labour Act (Zakon o radu), Official Gazette of the Republic of Croatia nos. 93/14 and 127/17.

Occupational Safety Act (Zakon o zaštiti na radu), Official Gazette of the Republic of Croatia nos. 71/14, 118/14 and 154/14.

Personal Data Protection Act (Zakon o zaštiti osobnih podataka), Official Gazette of the Republic of Croatia nos. 103/03, 118/06, 41/08, 130/11 and 106/12.

Regulation (EU) 2016/679 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, Official Journal of the European Union L 119, 04.5.2016, pp. 1–88.

## PREPARATORY DOCUMENTS

Government of the Republic of Croatia, *Final Proposal of the Act on Implementation of the General Data Protection Regulation*, class: 022-03/17-01/171; filing no.: 50301-25/06-18-8, 12.4.2018.

Houses of the Oireachtas, *Data Protection Act 2018 - Debates*, <https://www.oireachtas.ie/en/bills/bill/2018/10/?tab=debates> (2 July 2018).

Ministry of Labour and Pension System Policy, *Draft Act on Amendment of the Occupational Safety Act*, May 2018., <https://vlada.gov.hr/UserDocsImages//Sjednice/2018/05%20svibnja/96%20sjednica%20VRH//96%20-%203.pdf> (2 July 2018).

## OPINIONS AND OTHER DOCUMENTS

Article 29 Data Protection Working Party, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, 17/EN, WP 248 rev.01, adopted 4.4.2017 - as last revised and adopted 4.10.2017.

Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 17/EN, WP 253, 3.10.2017.

Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, 17/EN, WP 249, 8.6.2017.

Article 29 Data Protection Working Party, *Position paper on derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19.4.2018, [http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc\\_id=51422](http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422) (2 July 2018).

European Data Protection Board, *The Board endorsed Article 29 Working Party’s interpretations of the GDPR: Endorsement 1/2018*, 25.5.2018, [https://edpb.europa.eu/sites/edpb/files/files/news/endorsement\\_of\\_wp29\\_documents\\_en\\_0.pdf](https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf) (2 July 2018).

Ministry of Economy, Entrepreneurship and Crafts, *Opinions and Interpretations*, 4.3.2015, Ius-Info.

Personal Data Protection Agency, *Decision on establishment and publication of a list of types of processing procedures subject to data protection impact assessment requests*, class: 004-04/18-01/01; filing no.: 567-01/01-18-01, 25.5.2018.

Personal Data Protection Agency, *Opinion of 31.1.2013*, in: Gotovac, V. et al., *Komentar Zakona o radu*, TEB-Poslovno savjetovanje, Zagreb, 2014, pp. 131-132.

Personal Data Protection Agency, *Opinions, Video nadzor u poslovnim prostorijama*, <https://azop.hr/upotreba-videonadzora/detaljnije/video-nadzor-poslovnim-prostorijama>, 14.10.2015.

Personal Data Protection Agency, *Privacy protection in the workplace-Guide for employees*, 2014, [https://azop.hr/images/dokumenti/252/guide\\_for\\_employees.pdf](https://azop.hr/images/dokumenti/252/guide_for_employees.pdf) (2 July 2018).

Personal Data Protection Agency, *Report on Work for 2016*, June 2017, [https://azop.hr/images/dokumenti/217/godisnje-izvjesce-o-\\_radu-za\\_2016-godinu.pdf](https://azop.hr/images/dokumenti/217/godisnje-izvjesce-o-_radu-za_2016-godinu.pdf).

## Sažetak

Doc. dr. sc. Nina Gumzej\*  
Prof. dr. sc. Dražen Dragičević\*\*

### VIDEONADZOR NA RADNOM MJESTU PREMA HRVATSKOM ZAKONU O PROVEDBI OPĆE UREDBE O ZAŠTITI PODATAKA

*U radu autori kritički ocjenjuju zakonodavstvo i praksu u Republici Hrvatskoj o temi videonadzora na radnom mjestu, a posebno se usredotočuju na nedavno usvojen Zakon o provedbi Opće uredbe o zaštiti podataka. U tom se aktu, naime, utvrđuje više pravila o obradi osobnih podataka putem videonadzornih sustava te najviše upravne novčane kazne za slučaj kršenja pojedinih ondje navedenih pravila.*

*Osim novih odredbi o videonadzoru radnih prostorija, u radu se detaljno ispituju nova opća pravila o obradi osobnih podataka putem videonadzora te povezane odredbe o upravnim novčanim kaznama, kao i raniji propisi na koje se ispitivane odredbe Zakona o provedbi Opće uredbe oslanjaju. Cilj ovog istraživanja je ocjena uvodi li se novim pravilima potrebna jasnoća i pravna sigurnost u odnosu na postojeće zakonodavstvo i praksu te ocjena o njihovoj sukladnosti s odredbama same Opće uredbe o zaštiti podataka (uključujući onima o sankcijama). Autori također ukratko upozoravaju na pravila Opće uredbe o zaštiti podataka koja poslodavci, stručnjaci u području ljudskih resursa i pravni stručnjaci, trebaju razmatrati pri ocjeni pravne usklađenosti prakse videonadzora na radnom mjestu, uz napomenu da je iz opsega rada isključena analiza pravnih osnova za obradu osobnih podataka radnika i pripadajuća sudska i regulatorna praksa.*

*Rezultati cjelokupnog istraživanja osnova su za zaključne kritičke primjedbe s de lege ferenda prijedlozima izmjena pojedinih analiziranih odredbi Zakona o provedbi Opće uredbe kako bi se osigurala veća pravna jasnoća i pravna sigurnost te usklađenost s Općom uredbom o zaštiti podataka.*

*Ključne riječi: hrvatski Zakon o provedbi Opće uredbe o zaštiti podataka, Opća uredba o zaštiti podataka, videonadzor, osobni podaci, radno mjesto*

---

\* Dr. sc. Nina Gumzej, docentica Pravnog fakulteta Sveučilišta u Zagrebu, Trg Republike Hrvatske 14, Zagreb; ngumzej@pravo.hr;  
ORCID ID: orcid.org/0000-0002-7434-3538

\*\* Dr. sc. Dražen Dragičević, profesor Pravnog fakulteta Sveučilišta u Zagrebu, Trg Republike Hrvatske 14, Zagreb; drazen@pravo.hr;  
ORCID ID: orcid.org/0000-0001-7364-8439