Social Transformations in Contemporary Society, 2019 (7)
ISSN 2345-0126 (online)

VIDEO SURVEILLANCE AND THE GDPR

Aurimas Šidlauskas

Mykolas Romeris University, Lithuania
aurimas868@gmail.com

Abstract

Purpose – to present some recommendations that would help organizations to compliance video surveillance under GDPR.

Design/methodology/approach – analysis and synthesis of scientific literature and legal documents, generalization.

Finding – after analyzing the theoretical aspects of video surveillance compliance under GDPR, there were introduced the main recommendations that would reduce the risk of GDPR non-compliance.

Research limitations/implications – The main limitation of this study is that the research is based on scientific literature review.

Practical implications – the present research allows to identify the challenges of GDPR implementation for video surveillance.

Originality/Value – On May 25, 2018, the General Data Protection Regulation or GDPR officially took effect, requiring better protection of personal data across the EU region. In this regard, making video surveillance GDPR compliant has become critical.

Keywords: video surveillance, GDPR,

Research type: general review.

Introduction

In the world of today's information technologies, data may spread through cyber space at the speed of lightning (Limba, & Šidlauskas, 2018). 2018 is a big year for data privacy and data processing regulation. On July 27, 2018, India published a draft bill for a new, comprehensive data protection law to "be called the Personal Data Protection Act, 2018," only a few weeks after the European Union General Data Protection Regulation (GDPR) took effect on May 25, 2018 and California enacted the California Consumer Privacy Act of 2018 at the end of June. Brazil already followed with a new General Data Protection Law (Law No. 13,709/2018) only a few weeks later, on August 14, 2018. The new Indian Personal Data Protection (PDP) Act adopts and further develops many existing principles of EU-style data processing regulation and some aspects of U.S.-style data privacy laws. Global companies can, and should try to, address the requirements of the new Indian Data Protection Law, the GDPR, the California Consumer Privacy Act (CCPA) and other privacy regimes simultaneously and holistically, in the interest of efficiency (Determann, & Gupta, 2018).

The PDP Act is along the lines of the GDPR, it largely regulates all processing of personal data with the prohibitive character by providing for a blanket data protection law. It aims at instituting a data protection authority and subjecting companies to numerous administrative duties which include the appointment of data protection officers, local representatives, data

protection impact assessments, record keeping, privacy by design and frequent audits among other things (Determann, 2016). The CCPA also provides for blanket protection, but the intention is not to replace existing data privacy laws at the U.S. Federal and California State level. As a result, it does not create any such administrative obligations and is implemented to address the specific risks for individual privacy created by data trading. While the PDP Act and GDPR secure any information related to an identifiable individual, CCPA takes one step further to additionally includes information relating to households (California Civil Code).

If companies collect or process personal data from or in any of the three above mentioned territories, they will be subject their respective data protection laws. In order to avert the consequences of non-compliance, the companies would have to stop doing business in each jurisdiction (Bahl, & Bharsakle, 2018).

Privacy and protection of personal data (or more aptly, the lack thereof) has become a topic of concern for the modern society. GDPR defines the privacy of personal data as a fundamental right of all the European people, and accordingly regulates the entire lifecycle of personal data. Thus, any company dealing with EU people's personal data is legally bound to comply with GDPR (Banakar et al., 2019). One of the GDPR goals is to protect the fundamental rights and freedoms of the data subjects by creating a protective regiment with regards to the processing of personal data. This is because new technologies and organisational models both in the private and public sector have made it easy to gather, use, combine, aggregate or otherwise process a vast amount of personal data without sufficient controls or oversight (Kotsios et al., 2019). The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts (Vojkovic, 2018).

Interdisciplinary approaches are mandatory to ensure that legal problems are not overlooked. In addition to economic, ethical and social aspects, technical aspects play an increasingly important role in the law, with technical infiltration into daily human life being reflected in the relevant laws. However, there is often a great deal of uncertainty as to whether technical innovations are compatible with existing legal standards (Bretthauer, 2016). In addition to technological advancement of surveillance systems, there are also concerns about the potential trade-off with human rights and freedoms of citizens. Thus, there is a need for means that allow for the protection of freedoms and human rights, while also ensuring security (Wurster et al., 2018). One particular form is data protection law; this was created as a reaction to technology specific hazards and is based on a risk analysis of data processing. Authors Limba and Šidlauskas (2018) states that the data subject should be involved as an active participant in the personal data protection process in order to avoid violations related to the personal data.

Video surveillance systems are becoming ubiquitous. They are widely deployed in many strategic places such as airports, banks, public transportation or busy city centers. While people usually appreciate the sense of increased security brought by video surveillance, they often fear the loss of privacy which comes along (Dufaux, & Ebrahimi, 2006). Video footage is included in the GDPR as personal data. With this in mind, it is vital for those collecting and

processing the data produced by video surveillance are ensuring they do so in line with guidelines.

GDPR Overview – Principles, Key roles, Data Processing Lawfulness, Security

Apparently, the GDPR does not contain an express regulation on video surveillance. However, this is a false representation, as the GDPR does not expressly regulate every circumstance or situation governed by its provisions. In order to understand its scope, it is necessary to define the key-element. Personal data is any information relating to an identified or identifiable natural person (data subject):

1. Any information is subjective or objective information.
2. Information in term of its content.
3. Information format.
4. Regardless the modality of capture, storage or presentation.

The principles of the GDPR are focused on the privacy rights of every person when it comes to collecting and processing their data (see Table 1).

Table 1. Six Basic Principles of the GDPR

The Principles	Definition
Lawfulness, Fairness, and Transparency	These dictate that the personal data needs to be processed in a way that is lawful to the subject
Purpose Limitation	The data processors can only use the data for the objectives they've explicitly described and justified
Data Minimization	The information that is required has to be relevant for its purpose and limited to what is necessary
Trueness, Accuracy	If some of the data is inaccurate, it should be removed or rectified
Storage Limitation	Data is kept in a form which permits identification of persons for no longer than is necessary for the purposes for which the personal data is processed
Integrity and Confidentiality	This principle stands for taking all required measures to ensure all the personal data is protected

Compliance with the spirit of these key principles is a fundamental building block for good data protection practice (Šidlauskas, 2019).

On the most fundamental level data protection offers a binary system of two opposed actors: a controller and a data subject. A person processing personal data and the person to whom this data is relating. A data subject is any person whose personal data is being collected, held or processed (see Figure 1).

Source: Ahmed Badr, 2018

Figure 1. Data controller vs data processor

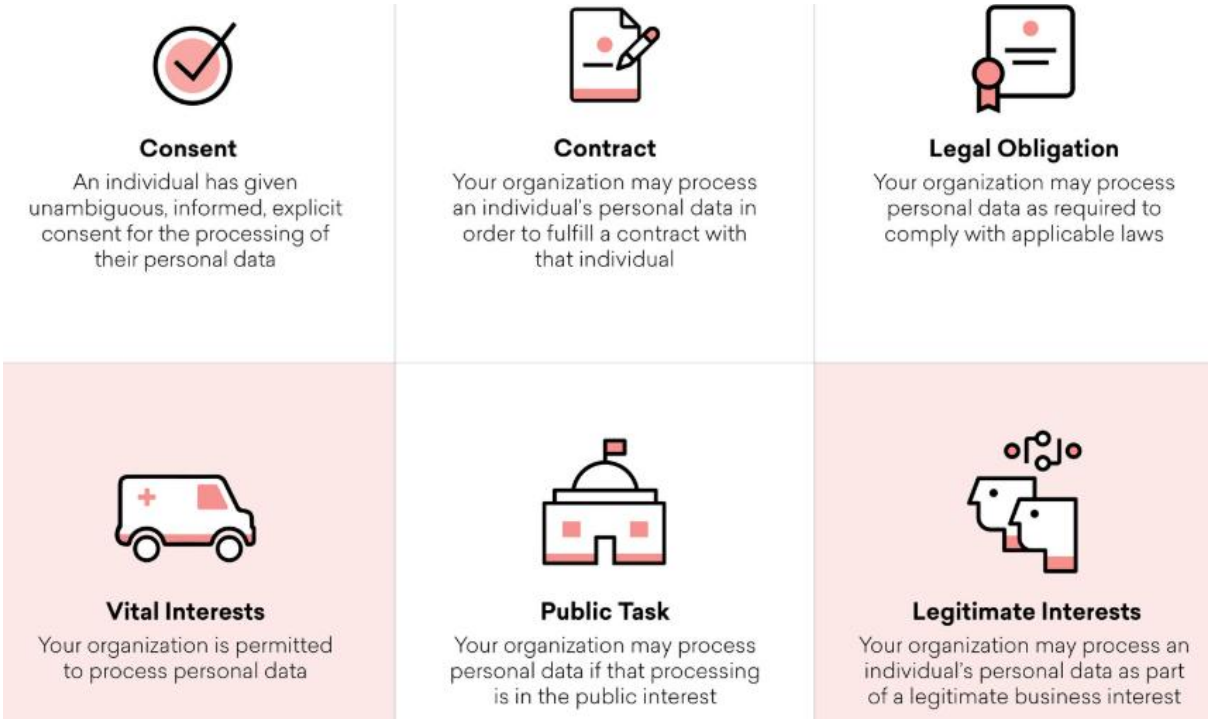
ISSN 2345-0126 (online)

Under GDPR, businesses must comply as either data processor or data controller, in relation to specific data:

1. Data processors process personal data on behalf of the controller, but they don't decide the purpose or the means.
2. Data controllers determine the purpose of the processing and the means to achieve that purpose. Essentially they decide why and how the processing should take place.

However, the GDPR does not limit itself to this traditional scenario and offers more possible roles. According to the GDPR, a Controller is any (natural or legal) person that, alone or jointly, determines the purposes and means of the processing of personal data. It is a role that is always determined in relation to a specific act or set of acts of processing. These can include the collection, recording, organization, structuring, storage, adaptation, usage, disclosure, cf. In order to limit risks from acts of processing, the GDPR enjoins controllers with certain obligations that are meant to safeguard data subjects' rights. Data Protection Officer (DPO) is a new position implemented in the companies as the GDPR requires certain companies to appoint a DPO to ensure compliance within the company. These officers should inform the organisation on the GDPR and maintain compliance internally.

For every act of processing is in need of a legal basis, making it the controller's duty to make sure that and declare which one of the legal grounds listed in the provision applies. Under GDPR, the processing of personal data is only lawful when it falls under one of six approved justifications (see Figure 2).



Source: Todd Grennan, 2018

Figure 2. Personal data processing under GDPR

Furthermore, certain organizational and technical measures need to be taken in order to ensure that the controller is also in compliance with all the GDPR's specific data protection and data security provisions and is able to prove said compliance at any time. What makes the determination of the scope of these obligations difficult is the rather abstract way in which they are defined. The measures that a controller has to take are dependent on the scope,

context and purpose of the processing and on the severity and the probability of occurrence of the risks for data subjects' rights and need to be "suitable" and "appropriate". In summary, there is no general way of defining measures that every controller can take without taking into account the context and specifics (Kurtz et al., 2019).

The GDPR reinforces the rights of Data Subjects, namely the right to information and access to personal data, their correction or deletion, limiting their processing, data portability, as well as opposing automatic decision including profile definition, thus forcing Organizations to adopt organizational and/or technical procedures so as to comply with the rights of the data subjects. The effectiveness of security measures depends on how they manage to reduce the risk (Šidlauskas, 2017). As the scale and sophistication of attacks grow, the controllers should invest in cyber security compliance within GDPR in order to protect information business systems. The emphasis it given on the fact that they should have to remain vigilant and try to put in place sufficient processes and policies to best protect their businesses and remain in compliance with GDPR. Ultimately, cybersecurity and GDPR are one and the same: the common denominator is data management: designing efficient cybersecurity frameworks in terms of end-point protection – based on privacy by design and also antivirus, malware tools, firewalls – and also designing security policies based on GAP analysis on GDPR with permissions to access data by their employees creating robust governance system with adequately protected personal data belonging to the customers (Boban, 2018). The factors relevant to information security are combined within the strategic, human and technological dimensions of information security management. Information is the greatest asset and the most important security object (Šidlauskas, 2018).

Video Surveillance Under GDPR

GDPR applies to all data processing operations, even if not all of these are expressly regulated. One of these personal data modalities is represented by the video surveillance. Despite not expressly regulated by GDPR, this is one of the most commonly used means of personal data processing. Video surveillance as a data processing method should be assessed very carefully by any organization that has the capacity of controller or processor, in order to be fully compliant with the provisions of the GDPR (Cliza, Olanescu, & Olanescu, 2018). The GDPR raises for companies the question of how they can ensure that operations conform with external data processors according to the regulation (Kurtz, & Semmann, 2018). Organizations that collect, access, store or process personal data are now obliged to inform data subjects about what data they collect and what are their objectives in processing those data in an understandable and transparent way, using clear and simple language (Tesfay et al., 2018). Information Governance in an Organization describes how information is managed and all the procedures involved. The following should be known about the data: their source, how they are processed, reliability in terms f integrity and accuracy, and traceability (Wróbel et al., 2017). In some cases, prior consent of data subjects is now compulsory for the Organization to be able to collect, store and process personal data and, at any moment, data subjects may withdraw their consent (Safari, 2016). Consent must be concise, understandable, easily accessible and written clearly and accurately (Chowdhury et al., 2017).

The use of digital surveillance technology is rapidly growing as it becomes significantly cheaper for live and remote monitoring (Caputo, 2014). The UK is often cited as being one of the most video monitored societies globally, with up to 5.9 million CCTV cameras in operation in 2015 alone (one camera for every eleven people) (Andrew Kuemmerle, 2018). The way CCTV video footage is captured and handled must change to fit with the new GDPR guidelines introduced by EU, ensuring that more stringent rules and regulations are implemented in

ISSN 2345-0126 (online)

order for business owners and organisations looking to install new CCTV systems. A business owner will now need to have a valid reason for CCTV placement within their businesses, which requires viable reasoning. One such reason may be to help protect their stocks or assets, the wellbeing of their employees when it comes to health and safety, or to capture footage of any incidents that may occur within the company. In the workplace, CCTV surveillance could frequently be justified by a claim that it was there to prevent or detect crime, with only notice to employers needed (Edwards, Martin, & Henderson, 2018). There has been an accelerated expansion of Closed-Circuit TeleVision (CCTV) surveillance in recent years, largely in response to rising anxieties about crime and its threat to security and safety (Gong, Loy, & Xiang, 2011).

There are many different types of CCTV systems available – analogue and digital, wired and wireless and their modes of operation vary; however, the basic components are more or less the same: a camera, a lens, a monitor, and (for wired systems) cables that carry the signal from one place to another. Many systems also use video recorders to record the video footage (Murungi, 2009). Video surveillance, closed-circuit TV and IP-camera systems became virtually omnipresent and indispensable for many organizations, businesses, and users. They also became increasingly complex, comprising many communications means, embedded hardware and non-trivial firmware (Costin, 2016).

Surveillance footages are often used merely as passive records or as evidence for post-event investigations. Miss-detections of important events can be perilous in critical surveillance tasks (Gong, Loy, & Xiang, 2011). However, the sensitive nature of the surveillance use case imposes high requirements on privacy/confidentiality, authenticity, and availability of such systems. (Obermaier, & Hutle, 2016). It's an important part of security system because of its visualized, accurate, timely and rich information content. Video surveillance has become the main tool due to its rich, intuitive and accurate information (Xu, Hu, & Mei, 2016).

Recommendations of video surveillance compliance under GDPR

A video recording of an identifiable person naturally forms part of an individual's personal data. The GDPR applies throughout the European Union and has affect camera system operators.

The European Data Protection Supervisor (EDPS) is the European Union's (EU) independent data protection authority which presented the main video surveillance data protection issues:

1. **Data quality** - Cameras can and should be used intelligently and should only target specifically identified security problems thus minimising the gathering of irrelevant footage (data minimisation). This not only reduces intrusions into privacy but also helps to ensure a more targeted, and ultimately, more efficient, use of video-surveillance.
2. **Right of information** - Notices can be found in EU institution buildings informing staff and visitors about the security cameras in place. These signs are mandatory because individuals affected by video-surveillance must be informed upon its installation about the monitoring, its purpose and the length of time for which the footage is to be kept and by whom.
3. **Retention period** - Although the installation of cameras might be justified for security purposes, the timely and automatic deletion of footage is essential. The EDPS requires all EU institutions to have clear policies regarding the use of video surveillance on their premises including on potential storage.

ISSN 2345-0126 (online)

The Article 29 Working Party (WP29) has issued Opinion 2/2017 on data processing at work, The Opinion closes with a number of conclusions and helpful recommendations:

1. **Fundamental rights**. Based on the current Data Protection Directive employers may only collect the data for legitimate purposes, with the processing taking place under appropriate conditions (e.g., proportionate and necessary, for a real and present interest, in a lawful, articulated and transparent manner), with a legal basis for the processing of personal data collected from or generated through electronic communications.
2. **Consent; legitimate interest**. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer. The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity.
3. **Transparency**. Effective communication should be provided to employees concerning any monitoring that takes place, the purposes for this monitoring and the circumstances, as well as possibilities for employees to prevent their data being captured by monitoring technologies. Policies and rules concerning legitimate monitoring must be clear and readily accessible.
4. **Proportionality and data minimization**. Data processing at work must be a proportionate response to the risks faced by an employer. The information registered from the ongoing monitoring, as well as the information that is shown to the employer, should be minimized as much as possible. Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances. Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies. The information should be stored for the minimum amount of time needed with a retention period specified. Whenever information is no longer needed it should be deleted.

The Article 29 Working Party Opinion 8/2001 on the processing of personal data in the employment context and the 2002 Working Document on the surveillance of electronic communications in the workplace, stated the position and conclusions that when processing employees' personal data:

1. Employers should always bear in mind the fundamental data protection principles, irrespective of the technology used.
2. The contents of electronic communications made from business premises enjoy the same fundamental rights protections as analogue communications.
3. Consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence.
4. Performance of a contract and legitimate interests can sometimes be invoked, provided the processing is strictly necessary for a legitimate purpose and complies with the principles of proportionality and subsidiarity.
5. Employees should receive effective information about the monitoring that takes place.
6. Any international transfer of employee data should take place only where an adequate level of protection is ensured.

Secure Insights (2018) identified how the GDPR affects camera system:

1. No obligation to notify the Office for Personal Data Protection of the installation of the camera system (the CS).
2. Obligation of the administrator to provide more information about the method of data processing with the help of the CS.
3. Obligation of the administrator to keep a written record of CS operation.

ISSN 2345-0126 (online)

4. Obligation of the administrator to report leaks of personal data (or security breach) to the Office for Personal Data Protection.

5. Obligation to develop a Data Protection Impact Assessment (DPIA) with regards to "extensive systematic monitoring of publicly accessible premises."

6. Obligation to appoint a so-called data protection officer (applies to public entities or specialists for the processing of personal data).

How to ensure your video data is compliant. It is a complex balance between making sure that you're protecting people without compromising their privacy. Roobol (2018) gives some things to consider (see Table 2).

Table 2. A suggestion to video surveillance and the GDPR

Suggestion	Explanation
Use a secure system	To significantly reduce the chances of a breach, invest in high-end security software and secure hardware for your video surveillance and connectivity, stay abreast of the latest cybersecurity best practices and make sure your system is regularly updated and maintained in line with patches and guidance from the manufacturer.
Be selective	Check where the major risk/interest points are on the site and focus your strategy on these areas. Also, remember when setting up a new system, there is an obligation to develop a Data Protection Impact Assessment (DPIA) with regards to "extensive systematic monitoring of publicly accessible premises". By making your surveillance targeted, you are only gathering necessary data, meaning you have reasonable grounds to store it, analyse it and catalogue it.
Work with trusted partners	GDPR compliance or instances of breach largely depend on how you are using the services provided by third parties. What type of GDPR obligations that arise – and who owns those obligations – must be examined on an application-specific basis. It is vital to use a reputable company to ensure your footage is managed correctly.

Source: Roobol, 2018

Video surveillance is increasingly omni-present in our everyday life and is a key component of many security systems. Not only is the increasing number of cameras, but also the resolution of visual sensors and the performance of video processing algorithms. This evolution generates some important privacy concerns (Ruchaud, 2015).

Conclusions

GDPR went into effect on May 25, 2018. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world. In addition to economic, ethical and social aspects, technical aspects play an increasingly important role in the law, with technical infiltration into daily human life being reflected in the relevant laws.

Personal data is any information relating to an identified or identifiable natural person (data subject). Video footage is included in the GDPR as personal data. With this in mind, it is vital for those collecting and processing the data produced by video surveillance are ensuring they do so in line with guidelines. Six Basic Principles of the GDPR – Lawfulness, Fairness, and Transparency; Purpose Limitation; Data Minimization; Trueness, Accuracy; Storage Limitation; Integrity and Confidentiality.

The principles of the GDPR are focused on the privacy rights of every person when it comes to collecting and processing their data.

ISSN 2345-0126 (online)

On the most fundamental level data protection offers a binary system of two opposed actors: a controller and a data subject. A person processing personal data and the person to whom this data is relating.

For every act of processing is in need of a legal basis, making it the controller's duty to make sure that and declare which one of the legal grounds listed in the provision applies. Under GDPR, the processing of personal data is only lawful when it falls under one of six approved justifications – Consent; Contract; Legal obligation; Vital Interests; Public task; Legitimate interests.

Certain organizational and technical measures need to be taken in order to ensure that the controller is also in compliance with all the GDPR's specific data protection and data security provisions and is able to prove said compliance at any time.

Recommendations of video surveillance compliance under GDPR:

1. Cameras can and should be used intelligently and should only target specifically identified security problems thus minimising the gathering of irrelevant footage.
2. There is a need to notify individuals of surveillance information processing, such as their presence in an area where CCTV is in operation, and their rights of access to recordings/images of themselves.
3. CCTV recordings that no longer serve a purpose need to be deleted. The information should be stored for the minimum amount of time needed with a retention period specified. Whenever information is no longer needed it should be deleted.
4. Organizations may only collect the data for legitimate purposes, with the processing taking place under appropriate conditions, with a legal basis.
5. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.
6. Policies and rules concerning legitimate monitoring must be clear and readily accessible. Clear documentation of the information retention policy which is clearly understood by CCTV system operators.
7. Data processing at work must be a proportionate response to the risks faced by an employer. Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies.
8. The contents of electronic communications made from business premises enjoy the same fundamental rights protections as analogue communications.
9. Any international transfer of employee data should take place only where an adequate level of protection is ensured.
10. Obligation to appoint a so-called data protection officer (applies to public entities or specialists for the processing of personal data).
11. Invest in high-end security software and secure hardware for your video surveillance and connectivity, regularly update and maintain in line with patches and guidance from the manufacturer.
12. It is vital to use a reputable company to ensure your footage is managed correctly.
13. Conduct a Privacy Impact Assessment (PIA) to be sure all CCTV cameras serve a legitimate purpose.
14. Recordings from CCTV systems need to be securely stored and access restricted to authorised personnel.

Video surveillance should be assessed very carefully by any organization, in order to be fully compliant with the provisions of the GDPR.

References

Costin, A. (2016, October). Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. *In Proceedings of the 6th international workshop on trustworthy embedded devices* (pp. 45-54). ACM.

Dufaux, F., & Ebrahimi, T. (2006, June). Scrambling for video surveillance with privacy. *In 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)* (pp. 160-160). IEEE.

Xu, Z., Hu, C., & Mei, L. (2016). Video structured description technology based intelligence analysis of surveillance videos for public security applications. *Multimedia Tools and Applications*, 75(19), 12155-12172.

Gong, S., Loy, C. C., & Xiang, T. (2011). *Security and surveillance*. In Visual Analysis of Humans (pp. 455-472). Springer, London.

Obermaier, J., & Hutle, M. (2016, May). Analyzing the security and privacy of cloud-based video surveillance systems. *In Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (pp. 22-28). ACM.

Working Party 29, *Opinion 2/2017 on data processing at work*, WP249, 8 June 2017, Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

Ruchaud, N. (2015, September). Privacy protection filter using stegoscrambling in video surveillance. *In MediaEval*.

Kurtz, C., & Semmann, M. (2018). Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Information Systems Security And Privacy (Sigsec).

Edwards, L., Martin, L., & Henderson, T. (2018). *Employee Surveillance: The Road to Surveillance is Paved with Good Intentions*.

Murungi, M. (2009). *Video surveillance system design*. University of Nairobi. Retrieved from http://eie.uonbi.ac.ke/sites/default/files/cae/engineering/eie/VIDEO%20SURVEILLANCE%20SYSTEM%20DESIGN.pdf

Vojkovic, G. (2018, May). Will the GDPR slow down development of Smart Cities?. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1295-1297). IEEE.

Working Party 29, *Opinion 8/2001 on the processing of personal data in the employment context*, WP48, 13 September2001, Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

Bretthauer, S. (2016). Law by technology or technology by law?–An illustration using the example of video surveillance. *Interdisciplinary Approach to Law in Modern Social Context*, 69.

Wurster, S., Kamara, I., Sveinsdottir, T., & Krempel, E. (2018). Certified Video Surveillance Systems for More Resilient Urban Societies. In Urban Disaster Resilience and Security (pp. 313-330). Springer, Cham.

Cliza, C., Olanescu, S., & Olanescu, A. (2018). Video Surveillance: Standpoint Of The EU And National Legislation On Data Protection. *Challenges of the Knowledge Society*, 465-471.

Working Party 29, *Working document on the surveillance of electronic communications in the workplace*, WP55, 29 May 2002, Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

Šidlauskas, A. (2017). *Users electronic data protection features*. Master's Work in Cyber Security Management. Vilnius: Mykolas Romery University.

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). Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Tesfay, W., Hofman, P., Toru, N., Kiyomoto, S. and Serna, J. (2018). PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation. *In ACM Proceedings of the 4th ACM on International Workshop on Security and Privacy Analytics* (pp. 15-21). https://doi.org/10.1145/3180445.3180447

Šidlauskas, A. (2019). Opportunities For DPO (Data Protection Officer) Occupational Training And Improvement. INTED2019: *13th International Technology, Education and Development Conference*, Valencia, Spain, 11-13 March, 2019. (pp. 3413-3419).

Caputo, A. C. (2014). *Digital video surveillance and security*. Butterworth-Heinemann.

Safari, B. A. (2016). Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection. Seton Hall L. Rev., 47, 809.

Chowdhury, M. J. M., Colman, A., Han, J. and Kabir, M. A. (2018). A Policy Framework for Subject-Driven Data Sharing. *In Proceedings of the 51st Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2018.594

Wróbel, A., Komnata, K. and Rudek, K. (2017). IBM data governance solutions. *In IEEE Behavioral, Economic, Socio-cultural Computing (BESC), 2017 International Conference* on (pp. 1-3).

Boban, M. (2018). Cyber Security Foundations For Compliance Within GDPR For Business Information Systems. *Economic and Social Development: Book of Proceedings*, 541-553.

The European Data Protection Supervisor, Video-surveillance, Retrieved from https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

Kotsios, A., Magnani, M., Rossi, L., Shklovski, I., & Vega, D. (2019). *An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research*. arXiv preprint arXiv:1903.03196.

Limba, T., & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook. *Entrepreneurship and Sustainability Issues*, *5*(3), 528-541.

Banakar, V., Shah, A., Shastri, S., Wasserman, M., & Chidambaram, V. (2019). *Analyzing the Impact of GDPR on Storage Systems*. *arXiv preprint arXiv:1903.04880*.

Grennan, T. (2018). 17 Things You Need To Know About GDPR. Blaze. Retrieved from https://www.braze.com/perspectives/article/gdpr-compliance-need-to-know

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., & Böhmann, T. (2019, January). The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems. *In Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Secure Insights (February 27, 2018). Video surveillance and the GDPR. What will change?. Retrieved from https://www.axis.com/blog/secure-insights/video-surveillance-gdpr-guest/

Roobol, E. (August 29, 2018). Faces as data: A guide to video surveillance and the GDPR. Retrieved from https://gdpr.report/news/2018/08/29/faces-as-data-a-guide-to-video-surveillance-and-the-gdpr/

Šidlauskas, A. (2018). Users Electronic Data Protection Features. *In Social transformations in contemporary society: proceedings of annual international conference for young researchers* (pp. 78-88). Mykolas Romeris University.

Kuemmerle, A. (October,2018). Is your CCTV system GDPR compliant?. Opinion, Technology & media. Retrieved from https://www.roydswithyking.com/is-your-cctv-system-gdpr-compliant/

Determann, L., & Gupta, C. (2018). Indian Personal Data Protection Act, 2018: Draft Bill and Its History, Compared to EU GDPR and California Privacy Law. Compared to EU GDPR and California Privacy Law (September 3, 2018).

Determann, L. (2016). Adequacy of data protection in the USA: myths and facts. *International Data Privacy Law*, 6(3), 244-250.

California Civil Code, 1798.140. Retrieved from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml

Bahl, A., & Bharsakle, S. (2018). The Privacy Jungle–comparative Study Of The Indian Personal Data Protection Act, 2018 With Eu Gdpr And California Privacy Law.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.