

VIŠJA STROKOVNA ŠOLA ACADEMIA
MARIBOR

**TEHNIČNO VAROVANJE – VAROVANJE
OSEBNIH PODATKOV, PRIDOBLENIH Z
VIDEONADZOROM**

Kandidat: Timotej Rotovnik

Vrsta študija: študent izrednega študija

Študijski program: Varovanje

Mentor predavatelj: Jakob Demšar, univ. dipl. prav.

Mentor v podjetju: Bernard Majhenič, dipl. ekon.

Lektor: Petra Hercog, univ. dipl. nov.

Maribor, 2025

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Timotej Rotovnik sem avtor diplomskega dela z naslovom Tehnično varovanje – varovanje osebnih podatkov, pridobljenih z videonadzorom, ki sem ga napisal pod mentorstvom Jakoba Demšarja, univ. dipl. prav.

S svojim podpisom zagotavljam, da:

- je predloženo delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia Maribor,
- se zavedam, da je plagiatstvo – predstavljanje tujih del oz. misli, kot moje lastne kaznivo po Zakonu o avtorski in sorodnih pravicah (Uradni list RS, št. 16/07 – uradno prečiščeno besedilo, 68/08, 110/13, 56/15 in 63/16 – ZKUASP); prekršek pa podleže tudi ukrepom Višje strokovne šole Academia Maribor skladno z njenimi pravili,
- skladno z 32.a členom ZASP dovoljujem Višji strokovni šoli Academia Maribor objavo diplomskega dela na spletnem portalu šole.

Piran, september 2025

Podpis študenta:

ZAHVALA

Iskrena hvala podjetju Aerodrom Portorož in vodstvu, ki mi je omogočilo, da sem ob delu uspešno opravljal študijske obveznosti. Posebna zahvala gre direktorju Bernardu Majheniču, ki je bil pobudnik in podpornik moje izobraževalne poti ter je vedno verjel v moje sposobnosti.

Zahvaljujem se tudi svojemu mentorju, Jakobu Demšarju, ki me je z zaupanjem sprejel pod svoje okrilje ter z jasnimi usmeritvami pomagal oblikovati moje diplomsko delo.

Velika zahvala gre tudi sodelavcu Emanuelu Letici, s katerim sva skupaj stopala po izobraževalni poti. V trenutkih, ko sem se spopadal s pomanjkanjem motivacije za študij, je bil prav on tisti, ki me je s svojo odločnostjo in vztrajnostjo spomnil, zakaj vztrajamo. Hvala, ker si verjel v skupni cilj in si pomagal, da sva ga dosegla!

Največja in najgloblja zahvala pa gre moji družini, ki je bila moja opora na prav vsakem koraku te poti. Brez vaše podpore, potrpljenja in razumevanja bi bilo marsikaj težje ali celo nedosegljivo. Hvala, da ste verjeli vame, tudi takrat, ko sam v sebe nisem bil povsem prepričan.

Iz srca se zahvaljujem svoji ženi Kim, moji življenjski sopotnici, najmočnejši zaveznici v vseh obdobjih negotovosti. Njena brezpogojna podpora, neizmerna skrb za najine tri male zaklade in potrpežljivost v vseh dolgih večerih, ko sem bil z mislimi in časom drugje, so mi dali prostor, da sem rasel kot študent, kot mož, kot oče in kot človek. Bila si moja tiha moč, moj kritik in moje varno zatočišče. Ta dosežek je najin in morda še bolj tvoj kot moj.

"Uspeh ni naključje. Je rezultat trdega dela, vztrajnosti, učenja, študija, odrekanja in kar je najpomembneje, ljubezni do tega, kar počneš."

-Pelé

POVZETEK

Videonadzor je eden ključnih elementov sodobnih sistemov tehničnega varovanja in je široko uporabljen v javnem in zasebnem sektorju. Namenjen je zagotavljanju varnosti ljudi, premoženja in nadzoru nad dostopi. Zaradi možnosti identifikacije posameznikov pa takšni sistemi obdelujejo osebne podatke, kar pomeni, da morajo biti usklajeni s pravnimi predpisi, zlasti Splošno uredbo o varstvu podatkov (GDPR) in Zakonom o varstvu osebnih podatkov (ZVOP-2). Neupoštevanje teh pravil lahko vodi v resne kršitve pravic posameznikov ter izpostavi organizacijo pravnim in nenazadnje tudi uglednim tveganjem.

Diplomsko delo obravnava ključne pravne, tehnične in organizacijske vidike videonadzora ter analizira, kako zagotoviti skladnost z zakonodajo pri obdelavi osebnih podatkov. V prvem delu naloge so predstavljena osnovna načela GDPR in ZVOP-2, s poudarkom na zakonitosti, sorazmernosti, omejitvi namena, varnosti obdelave in pravicah posameznikov. Posebna pozornost je namenjena tudi pomenu ocene učinka (DPIA) ter obveznostim informiranja javnosti.

V nadaljevanju so analizirani tehnični vidiki, kot so vrste sistemov, vloga umetne inteligence in oblačnih storitev, pa tudi tehnični ukrepi, kot so šifriranje, nadzor dostopa in evidentiranje. Organizacijski ukrepi vključujejo usposabljanje zaposlenih, notranje politike, nadzor nad dostopi in obvladovanje tveganj.

Empirični del naloge temelji na analizi notranjih dokumentov podjetja ter primernih iz prakse v Sloveniji in tujini. Ugotovitve kažejo, da so najpogostejše napake pomanjkanje jasnih postopkov, prekomerna hramba posnetkov in nezadostna ozaveščenost zaposlenih. Na podlagi analize so oblikovana praktična priporočila za izboljšanje skladnosti z zakonodajo.

Diplomsko delo potrjuje, da je skladna in varna uporaba videonadzora mogoča, če organizacija deluje premišljeno, usklajeno in sistemsko.

Skozi celostni pristop naloga poudarja pomen sodelovanja med tehničnim, pravnim in organizacijskim osebjem. Le s povezovanjem teh področij je mogoče vzpostaviti trajnostne sisteme videonadzora, ki ne ogrožajo zasebnosti, temveč jo ustrezno varujejo, hkrati pa izpolnjujejo svoj temeljni namen, ki je zagotavljanje varnosti.

Ključne besede: videonadzor, osebni podatki, GDPR, ZVOP-2, tehnično varovanje, zakonitost, varnost, zasebnost.

ABSTRACT

Technical security – Protection of personal data obtained through video surveillance

Video surveillance is one of the key components of modern technical security systems and is widely used in both public and private sectors. Its primary purpose is to ensure the safety of people, property and to control access. However, due to the ability to identify individuals, such systems involve the processing of personal data, which must be carried out in accordance with legal regulations – primarily the General Data Protection Regulation (GDPR) and the Slovenian Personal Data Protection Act (ZVOP-2). Failure to comply with these regulations may result in serious violations of individuals rights and pose legal and reputational risks to organisations.

This thesis addresses the core legal, technical and organizational aspects of video surveillance and analyses how to ensure compliance with data protection legislation. The first part focuses on the key principles of GDPR and ZVOP-2, such as lawfulness, proportionality, purpose limitation, security of processing and the rights of data subjects. Special attention is given to the importance of Data Protection Impact Assessments (DPIA) and the obligation to inform individuals.

The technical section explores the types of surveillance systems, the role of artificial intelligence and cloud technologies and technical safeguards such as encryption, access control and activity logging. The organizational measures include staff training, internal privacy policies, access management and risk mitigation practices.

The empirical part of the thesis draws on internal company documents and case studies from Slovenia and abroad. It identifies common issues such as unclear procedures, excessive data retention, and low employee awareness. Practical recommendations are provided to enhance legal compliance and overall system security.

The thesis confirms that lawful and secure use of video surveillance is achievable when an organization adopts a thoughtful, systematic and well documented approach.

Through a comprehensive approach, the thesis highlights the importance of collaboration between technical, legal, and organizational staff. Only with coordinated efforts across these areas can sustainable video surveillance systems be established – systems that protect privacy while effectively fulfilling their primary role of ensuring security.

Keywords: video surveillance, personal data, GDPR, ZVOP-2, technical security, legality, privacy, data protection.

KAZALO VSEBINE

1	UVOD	10
1.1	Opis področja in opredelitev problema	10
1.2	Namen, cilji in osnovne trditve	10
1.3	Predpostavke in omejitve	11
1.4	Uporabljene raziskovalne metode	11
2	PRAVNI OKVIR VAROVANJA OSEBNIH PODATKOV	13
2.1	GDPR in ključna načela	13
2.1.1	Ključna načela varstva osebnih podatkov	13
2.1.2	Smernice in praksa	15
2.2	ZVOP-2 in nacionalna ureditev	15
2.2.1	Ključne določbe ZVOP-2 v povezavi z videonadzorom	15
2.2.2	Poudarek na evidencah in odgovornosti	16
2.2.3	Sankcije	17
2.2.4	Praktična uporaba v slovenskem podjetju	17
2.3	Pomen zakonitosti pri izvajanju videonadzora	17
2.3.1	Zakonska podlaga in zakoniti interes	17
2.3.2	Jasnost in omejen namen snemanja	18
2.3.3	Transparentnost in obveščanje posameznikov	18
2.3.4	Načelo sorazmernosti in minimalnega posega	19
2.3.5	Skladnost s tehničnimi in organizacijskimi ukrepi	20
2.3.6	Kazenske posledice in nadzor	20
3	TEHNIČNI VIDIKI VIDEONADZORA	21
3.1	Vrste in značilnosti videonadzornih sistemov	21
3.1.1	Analogni sistemi (CCTV)	21
3.1.2	Digitalni IP sistemi	22
3.1.3	Pametni videonadzorni sistemi z analitiko	22
3.1.4	Telesne kamere (Bodycams)	22
3.1.5	Videonadzor v oblaku (Cloud VMS)	23
3.2	Osnovni gradniki videonadzornega sistema	23
3.2.1	Kamere	24
3.2.2	Objektiv	24
3.2.3	Slikovni pretvornik (senzor)	24
3.2.4	Prenosni mediji	24
3.2.5	Napajanje	25

3.2.6	Enote za snemanje (DVR/NVR)	25
3.2.7	Programska oprema (VMS – Video Management Software)	25
3.2.8	Ohišje in okoljski pogoji	25
3.3	Vpliv tehnološkega napredka na videonadzor.....	26
3.3.1	Visoka ločljivost in digitalna obdelava slike.....	26
3.3.2	Uporaba umetne inteligence (UI) in videoanalitike	26
3.3.3	Povezljivost in dostopnost prek oblakov	27
3.3.4	Mobilnost in oddaljen nadzor.....	27
3.4	Tehnični ukrepi za varovanje osebnih podatkov	28
3.4.1	Šifriranje posnetkov	28
3.4.2	Nadzor dostopa.....	29
3.4.3	Samodejno brisanje po izteku roka hrambe	29
3.4.4	Zapisovanje dnevnikov dostopov (logi).....	30
3.4.5	Ločevanje pravic uporabnikov	30
3.4.6	Redno testiranje in posodabljanje programske opreme.....	31
4	ORGANIZACIJSKI IN VARNOSTNI UKREPI.....	32
4.1	Nadzor dostopov in vodenje evidenc	32
4.2	Politike in usposabljanje zaposlenih	33
4.3	Ozaveščenost in upravljanje s tveganji	34
5	PRAKTIČNE SMERNICE IN PRIPOROČILA	36
5.1	Primeri dobrih praks v Sloveniji in tujini.....	36
5.1.1	Slovenija.....	36
5.1.2	Tujina	38
5.2	Sinteza dobrih praks izvajanja videonadzora v Sloveniji, Franciji, Nemčiji in Združenem kraljestvu	40
5.2.1	Skupne točke	41
5.2.2	Posebnosti po državah	41
5.2.3	Sklepna ugotovitev	42
5.3	Najpogostejše napake izvajalcev videonadzora	42
5.4	Smernice za skladnost z GDPR in ZVOP-2	43
5.4.1	Predhodna ocena tveganj (DPIA).....	44
5.4.2	Oblikovanje jasnih politik in postopkov	44
5.4.3	Transparentnost in označevanje	44
5.4.4	Načelo minimizacije in sorazmernosti	44
5.4.5	Tehnična zaščita posnetkov.....	44
5.4.6	Nadzor dostopov in revizijska sledljivost	45
5.4.7	Usposabljanje zaposlenih in redni pregledi.....	45

6	SKLEP.....	46
7	VIRI IN LITERATURA.....	50
8	PRILOGE	52

KAZALO TABEL

<i>Tabela 1: Povzetek Posebnosti po državah</i>	<i>42</i>
---	-----------

KAZALO SLIK

<i>Slika 1: Primer opozorilne nalepke za videonadzor</i>	<i>19</i>
<i>Slika 2: Osnovni gradniki videonadzornega sistema</i>	<i>23</i>

OKRAJŠAVE IN KRATICE

AES-256 (Advanced Encryption Standard – 256 bit) – močan šifrirni algoritem, pogosto uporabljen za zaščito videoposnetkov pred nepooblaščenim dostopom.

ANPR (Automatic Number Plate Recognition) – tehnologija za samodejno prepoznavanje registrskih tablic vozil s pomočjo kamer.

CCD/CMOS (Charge-Coupled Device / Complementary Metal-Oxide Semiconductor) – tipa slikovnih senzorjev, ki se uporabljata v videonadzornih kamerah za zajem slike.

CCTV (Closed-Circuit Television) je tradicionalni sistem videonadzornega zaprtega kroga, pogosto uporabljen za nadzor nad objekti in površinami.

CNIL (Commision Nationale de l'Informatique et des Libertés) je francoski nadzorni organ za varstvo osebnih podatkov.

DPIA (Data Protection Impact Assessment) ali ocena učinka v zvezi z varstvom podatkov je postopek, s katerim upravljalec podatkov oceni vpliv obdelave na pravice posameznikov.

DPO (Data Protection Officer) – pooblaščen oseba za varstvo osebnih podatkov, odgovorna za skladnost z zakonodajo o varstvu podatkov.

DVR (Digital Video Recorder) pomeni digitalni snemalnik, ki shranjuje posnetke iz analognih kamer.

EDPB (European Data Protection Board) – Evropski odbor za varstvo podatkov, organ EU za usklajevanje uporabe GDPR v državah članicah.

ENISA (European Union Agency for Cybersecurity) – agencija EU za kibernetско varnost, ki pripravlja priporočila in smernice za zaščito informacijskih sistemov.

GDPR (General Data Protection Regulation) – označuje Splošno uredbo o varstvu osebnih podatkov, ki jo je sprejela Evropska unija in velja neposredno tudi v Sloveniji.

HTTPS (Hypertext Transfer Protocol Secure) – varna različica spletnega protokola za prenos podatkov med uporabnikom in strežnikom.

ICO (Information Commissioner's Office) je britanski neodvisni nadzorni organ za varstvo osebnih podatkov.

IP RS – je kratica za Informacijskega pooblaščenca Republike Slovenije, ki je neodvisni nadzorni organ za področje varstva osebnih podatkov.

ISO – označuje Mednarodno organizacijo za standardizacijo, ki izdaja globalno priznane standarde, tudi na področju informacijske varnosti.

LAN (Local Area Network) – krajevno računalniško omrežje, ki povezuje naprave znotraj omejenega območja.

NIS2 (Network and Information Security Directive) – označuje evropsko direktivo, katere cilj je izboljšati kibernetiko varnost držav članic.

NVR (Network Video Recorder) je snemalnik, ki deluje v omrežju in shranjuje videoposnetke z IP-kamer.

OS (operacijski sistem) je programska oprema, ki upravlja osnovne funkcije strojne opreme nadzornega sistema.

SIEM (Security Information and Event Management) predstavlja sistem za upravljanje varnostnih informacij in dogodkov, ki omogoča centralizirano beleženje in nadzor nad dostopi.

UI pomeni umetno inteligenco, ki v kontekstu videonadzora omogoča napredne funkcije, kot je samodejno prepoznavanje obrazov ali gibanja.

UPS (Uninterruptible Power Supply) – naprava za neprekinjeno napajanje, ki zagotavlja delovanje sistema tudi ob izpadu elektrike.

UTP/FTP (Unshielded Twisted Pair / Foiled Twisted Pair) – vrsti omrežnih kablov, ki se uporabljata za prenos podatkov med komponentami VNS.

VMS (Video Management System) – programska oprema za upravljanje videonadzornih sistemov, snemanja, pregledovanja in shranjevanja posnetkov.

VNS (Videonadzorni sistem) – sistem za zajem, prenos in shranjevanje videoposnetkov z uporabo kamer.

VPN (Virtual Private Network) – navidezno zasebno omrežje, ki omogoča varen oddaljen dostop do videonadzornih sistemov.

WLAN (Wireless Local Area Network) – brezžično krajevno omrežje, ki uporablja Wi-Fi za povezovanje naprav brez kablov.

ZVOP-2 – pomeni Zakon o varstvu osebnih podatkov, ki v nacionalnem okviru dopolnjuje določbe GDPR in določa podrobnosti, specifične za slovenski pravni red.

1 UVOD

1.1 Opis področja in opredelitev problema

Videonadzor je danes nepogrešljiva tehnologija, ki se uporablja v različnih okoljih, od trgovskih centrov, bolnišnic, javnih ustanov, industrijskih kompleksov, do letališč, šol in nenazadnje tudi v zasebnih stanovanjih. Namen videonadzora je običajno varovanje ljudi, premoženja, nadzor nad dostopi ter zaznavanje in preprečevanje kaznivih dejanj. Ob vse večji dostopnosti videonadzornih tehnologij in napredku umetne inteligence postaja uporaba teh sistemov vse bolj razširjena, kompleksna in v določenih primerih tudi sporna.

Video nadzor omogoča identifikacijo posameznikov, pogosto pa zajema tudi podatke, ki omogočajo profiliranje, sledenje gibanju in posredno razkrivanje občutljivih podatkov. Zaradi tega videonadzor vedno posega v pravico do zasebnosti in predstavlja obliko obdelave osebnih podatkov v smislu Splošne uredbe o varstvu podatkov (GDPR). Zakonodaja tako postavlja jasna pravila in pogoje za zakonito izvajanje videonadzora.

Problem, ki ga obravnava ta naloga, je pomanjkljiva implementacija zakonitih, tehnično ustreznih in organizacijsko nadzorovanih videonadzornih sistemov v praksi. Kljub jasnim pravnim zahtevam v številnih organizacijah še vedno prihaja do napačne uporabe, prekomernega snemanja, nezadostnega informiranja posameznikov ter nezavarovane obdelave posnetkov. To lahko vodi v kršitve človekovih pravic, izrek glob s strani nadzornih organov ter izgubo zaupanja zaposlenih in strank.

Naloga zato obravnava videonadzor z vidika zakonitosti, sorazmernosti, varnosti ter učinkovitega upravljanja obdelave osebnih podatkov.

1.2 Namen, cilji in osnovne trditve

Namen diplomskega dela je celostno predstaviti in analizirati pravne, tehnične in organizacijske vidike varovanja osebnostnih podatkov, ki se zbirajo z uporabo videonadzora. S tem želimo prispevati k boljši ozaveščenosti izvajalcev nadzora ter omogočiti boljšo skladnost s predpisi, hkrati pa zaščititi pravice posameznikov.

Cilji naloge so:

- predstaviti zakonske okvire videonadzora z vidika GDPR in ZVOP-2;
- analizirati tehnične možnosti videonadzornih sistemov in njihov vpliv na varstvo podatkov;
- prikazati organizacijske ukrepe za varno in zakonito uporabo nadzora;

- pregledati primere dobrih in slabih praks v Sloveniji in tujini;
- oblikovati praktične smernice za izvajalce videonadzora.

Temeljne raziskovalne trditve (hipoteze):

- **H1:** Organizacije pogosto izvajajo videonadzor brez popolne skladnosti z zakonodajo zaradi pomanjkanja znanja in notranjih politik.
- **H2:** Tehnična zasnova sistema pomembno vpliva na tveganja za zasebnost posameznikov.
- **H3:** Učinkovita organizacijska ureditev (evidence, dostopi, usposabljanje) bistveno zmanjša možnost kršitev in poveča zaupanje uporabnikov.

1.3 Predpostavke in omejitve

Raziskava temelji na predpostavki, da so izvajalci videonadzora dolžni zagotoviti skladnost z vsemi zakonodajnimi zahtevami, ne glede na velikost organizacije ali namen snemanja. Prav tako predpostavlja, da se s pravilno kombinacijo tehničnih in organizacijskih ukrepov lahko učinkovito zmanjša tveganje za zlorabe ali kršitve varstva osebnih podatkov.

Med ključne omejitve raziskave sodijo:

- dostopnost podatkov: večina realnih primerov videonadzora ni javno dokumentirana zaradi narave zasebnosti;
- subjektivnost interpretacije zakonodaje in smernic v praksi;
- različna stopnja tehnološke razvitosti in skladnosti med organizacijami.

Kljub tem omejitvam se lahko z analizo zakonodaje, internih pravilnikov podjetja in obstoječe literature oblikujejo realna in uporabna priporočila za izvajalce.

1.4 Uporabljene raziskovalne metode

Diplomska naloga temelji na teoretični raziskavi, ki vključuje več znanstvenih in strokovnih pristopov oziroma metod:

- opisna metoda za opis zakonodajnih okvirov (GDPR, ZVOP-2) in njihovih ključnih določil;
- primerjalna metoda za primerjavo domače in tuje prakse videonadzora;
- deskriptivna metoda za preverjanje hipotez na osnovi obstoječih virov;
- analiza dokumentacije notranjih pravilnikov, obrazcev in evidenc izbranega podjetja;
- metoda sinteze za oblikovanje praktičnih priporočil.

Kombinacija pravnega, tehničnega in organizacijskega vidika omogoča celovit pregled in razumevanje izzivov sodobnega videonadzora.

2 PRAVNI OKVIR VAROVANJA OSEBNIH PODATKOV

Videonadzor kot sredstvo tehničnega varovanja predstavlja pomemben poseg v temeljno človekovo pravico do zasebnosti. Ker sodobni videonadzorni sistemi omogočajo prepoznavo posameznikov, njihovo gibanje, nekatere vedenjske vzorce in druge osebnostne značilnosti, se njihova uporaba šteje za obdelavo osebnih podatkov v smislu evropske in slovenske zakonodaje. Pravna ureditev videonadzora zato zahteva posebno pozornost in poznavanje predpisov, ki določajo pogoje za zakonito, pošteno in varno obdelavo takšnih podatkov.

Osrednja pravna akta, ki urejata področje videonadzora, sta Splošna uredba o varstvu podatkov (GDPR), ki velja na ravni Evropske unije in Zakon o varstvu osebnih podatkov (ZVOP-2), ki določa posebnosti obdelave osebnih podatkov v Sloveniji. Ta dva dokumenta skupaj predstavljata pravno osnovo, ki določa pravila glede pravnih podlag za izvajanje videonadzora, namenov snemanja, obveznosti upravljalcev in pravic posameznikov, katerih podatki se obdelujejo.

2.1 GDPR in ključna načela

Splošna uredba o varstvu podatkov (GDPR), sprejeta kot Uredba (EU) 2016/679 Evropskega parlamenta in Sveta, je temeljni pravni okvir za varstvo osebnih podatkov v EU. Uredba je začela veljati 25. maja 2018 in velja neposredno v vseh državah članicah. Namen GDPR je okrepiti pravice posameznikov v zvezi z obdelavo osebnih podatkov ter poenotiti pravila za organizacije, ki te podatke zbirajo in obdelujejo, ne glede na njihovo lokacijo v EU ali izven nje, če obdelujejo podatke državljanov EU (Splošna uredba o varstvu osebnih podatkov (GDPR), 2016).

GDPR jasno opredeljuje, da se osebni podatek nanaša na katero koli informacijo, ki se nanaša na določeno ali določljivo fizično osebo oziroma posameznika. V kontekstu videonadzora to pomeni, da se vsaka oblika zajema podobe osebe, kjer je mogoče njena identifikacija, šteje za obdelavo osebnih podatkov (Board, 2020).

2.1.1 Ključna načela varstva osebnih podatkov

V 5. členu GDPR so določena temeljna načela, ki morajo biti izpolnjena pri vsaki obdelavi osebnih podatkov. Pri videonadzoru so ta načela še posebej pomembna zaradi narave obdelave, ki je lahko vsiljiva, dolgotrajna in pogosto poteka brez neposredne vednosti posameznika.

1. Zakonitost, poštenost in preglednost (lawfulness, fairness and transparency):

Obdelava mora temeljiti na eni izmed pravnih podlag iz 6. člena GDPR. Najpogostejša pravna podlaga pri videonadzoru je zakoniti interes (čl. 6(1)(f)), čeprav mora upravljalec vedno dokazati, da njegov interes prevlada nad pravicami posameznika. V praksi to pogosto zahteva izvedbo ocene učinka (DPIA).

2. Omejitev namena (purpose limitation):

Osební podatki morajo biti zbrani za določene izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni skladen s temi nameni. Videonadzor mora imeti jasno določen namen (npr. zaščita ljudi in premoženja), ki mora biti naveden že ob uvedbi sistema (GDPR, čl. 5 (1)(b)).

3. Minimizacija podatkov (data limitation):

Obdelava mora biti omejena na tiste podatke, ki so ustrezni, relevantni in omejeni na tisto, kar je nujno potrebno za namen, zaradi katerega se obdelujejo. V kontekstu videonadzora to pomeni, da ne smemo zajemati več prostora, kot je potrebno in da je snemanje v prostorih, kjer posameznik pričakuje večjo stopnjo zasebnosti (npr. sanitarije, dvigala), strogo prepovedano (Board, 2020).

4. Točnost (accuracy):

Podatki morajo biti točni in po potrebi posodobljeni. Čeprav to v videonadzoru ni pogosto relevantno, saj gre za posnetke, se nanaša na pravilno označevanje in povezovanje posnetkov z drugimi podatki, kot na primer evidenca dostopa.

5. Omejitev shranjevanja (storage limitation):

Osební podatki se smejo hraniti le toliko časa, kot je potrebno za namen, za katerega se obdelujejo. GDPR ne določa konkretnih rokov, vendar ZVOP-2 v Sloveniji omejuje hrambo posnetkov običajno na 30 dni, razen če je daljši čas upravičen s konkretnim incidentom (Zakon o varstvu osebnih podatkov (ZVOP-2), 2022).

6. Integriteta in zaupnost (integrity and confidentiality):

Obdelava mora potekati tako, da se zagotovi ustrezna varnost osebnih podatkov, vključno z zaščito pred nepooblaščno ali nezakonito obdelavo, izgubo, uničenjem ali poškodbo. To vključuje tehnične in organizacijske ukrepe, kot so šifriranje, omejitev dostopa, ločevanje arhivov, beleženje dostopov do posnetkov, ipd. (GDPR, čl. 32).

7. Odgovornost upravljalca (accountability):

Upravljalec je dolžan izkazati skladnost z vsemi zgoraj navedenimi načeli in mora dokumentirati sprejete ukrepe (GDPR, čl. 5(2)). V primeru videonadzora to vključuje pisno

odločitev o uvedbi sistema, vodenje evidenc dejavnosti, oceno učinka, politiko varovanja osebnih podatkov in jasno označene nadzorovane prostore.

2.1.2 Smernice in praksa

Evropski odbor za varstvo podatkov (EDPB) je leta 2019 izdal Smernice 3/2019 o obdelavi osebnih podatkov prek videonadzora, kjer navaja, da je potrebno videonadzor uporabljati le kot zadnjo možnost, če ni blažjih sredstev za doseg ciljev (EDPB, 2019). Poleg tega mora upravljalec oceniti, ali bi na primer fizično varovanje, mehanske pregrade ali druga sredstva zadostovala za enak učinek.

Ob uvedbi sistema mora biti nameščena **obvestilna tabla**, ki vsebuje informacije o upravljalcu, pravni podlagi, namenu, obdobju hrambe ter kontaktu za uveljavljanje pravic (GDPR, čl. 13). Uporaba generičnih obvestil brez vsebine ni skladna z načelom preglednosti.

2.2 ZVOP-2 in nacionalna ureditev

Čeprav je GDPR neposredno veljaven pravni akt Evropske unije, dopušča posameznim državam članicam, da z nacionalnimi predpisi uredijo posebnosti obdelave osebnih podatkov, kadar to ni v nasprotju z uredbo. V Sloveniji ta pravni okvir zagotavlja **Zakon o varstvu osebnih podatkov (ZVOP-2)**, ki je začel veljati 26. januarja 2023 in nadomesti več kot desetletje veljavni ZVOP-1.

ZVOP-2 vsebuje določbe, ki natančneje urejajo izvajanje videonadzora, zlasti v delovnem okolju, stanovanjskih skupnostih in javnih prostorih. Glavni cilj zakona je zagotoviti skladnost z GDPR, hkrati pa omejiti zlorabe in ohraniti sorazmernost med pravico do zasebnosti posameznika ter legitimnimi interesi upravljalcev.

2.2.1 Ključne določbe ZVOP-2 v povezavi z videonadzorom

ZVOP-2 vsebuje posebno poglavje (II. del, 3. poglavje: Videonadzor), ki natančno določa pogoje za uvedbo in izvajanje videonadzora. Pomembnejši členi vključujejo:

- **76. člen – Splošna pravila za uvedbo videonadzora**

Videonadzor je dovoljen zgolj, če je:

- nujen za varnost ljudi ali premoženja;
- uveden na podlagi pisne odločitve upravjalca;
- označen z jasnim in vidnim obvestilom;
- posnetki se hranijo največ 30 dni, razen če so potrebni kot dokaz v postopku.

Poseben poudarek je tudi na preglednosti, kjer mora obvestilo vsebovati podatke o upravljalcu, kontakt za uveljavljanje pravic, pravno podlago in čas hrambe. Obvestilo mora biti nameščeno pred vstopom v nadzorovano območje.

● **77. člen – Videonadzor v poslovnih prostorih**

V poslovnih prostorih, kjer delajo zaposleni, je videonadzor dovoljen samo, če:

- ni mogoče drugače zagotoviti varnosti;
- je namen izključno varovanju oseb, premoženja, tajnih podatkov ali proizvodnega procesa;
- ne posega pretirano v pravico do zasebnosti;
- je bil predhodno opravljen posvet s sindikatom ali svetom delavcev;
- ni nameščen v prostorih kot so garderobe, sanitarije, prostori za odmor ...

Zelo pomembno je, da snemanje ne sme biti sredstvo za stalni nadzor dela zaposlenih, razen v izjemnih in zakonsko opredeljenih primerih (ZVOP-2, 2022, 77. člen).

● **78. člen – Videonadzor v stanovanjskih območjih**

V večstanovanjskih stavbah je dovoljena namestitvev kamer samo:

- s soglasjem vsaj 70 % etažnih lastnikov;
- za nadzor nad skupnimi prostori, kot so garaže, vhodi v stavbe ...;
- če je zagotovljena sorazmernost in minimalen obseg zajema posnetkov.

Zakon tukaj posebej ščiti stanovalce pred morebitno nepooblaščen rabo videonadzora, kar pogosto vodi do prijav informacijskemu pooblaščenču.

● **79. in 80. člen – Videonadzor v javnem prometu in javnih prostorih**

ZVOP-2 ločeno obravnava videonadzor v:

- sredstvih javnega prevoza;
- na javnih površinah;
- v upravnih postopkih javnih organov.

Za te primere veljajo posebni pogoji, kot so ocena učinka na zasebnost (DPIA), registracija dejavnosti obdelave ter nadzorni mehanizmi. Poudarjen je princip sorazmernosti in nujnosti glede na javni interes.

2.2.2 Poudarek na evidencah in odgovornosti

ZVOP-2 (22. člen) nalaga upravljalcem, da vodijo evidence dejavnosti obdelave, vključno s seznamom kamer, lokacijami, področji snemanja, pravno podlago, namenom in časom hrambe. Poleg tega morajo voditi sledljivost dostopov do posnetkov in jih hraniti najmanj 2 leti.

Zakon vpeljuje tudi dolžnost imenovanja pooblaščenega osebe za varstvo osebnih podatkov (DPO) za javne organe in za organizacije, ki redno in sistematično obdelujejo osebne podatke v večjem obsegu.

2.2.3 Sankcije

ZVOP-2 v poglavju (III. del: Kazenske določbe) določa prekrškovne sankcije, ki vključujejo:

- kazni za odgovorne osebe v višini do 20.000 evrov;
- izrek ukrepov s strani informacijskega pooblaščenca, kot so prepoved obdelave, izbris podatkov ali uvedba nadzora (Zakon o varstvu osebnih podatkov (ZVOP-2), 2022).

2.2.4 Praktična uporaba v slovenskem podjetju

Analiza notranjih dokumentov podjetja Aerodrom Portorož kaže, da skladnost z ZVOP-2 vključuje:

- sprejetje pisnega pravilnika o videonadzoru;
- evidentiranje sistema in kamer;
- imenovanje odgovornih oseb za dostop;
- oblikovanje obvestil o izvajanju nadzora za zaposlene in obiskovalce;
- skrb za zavarovanje snemalnih naprav in posnetkov (Aerodrom Portorož, interna dokumentacija o videonadzoru, 2023).

2.3 Pomen zakonitosti pri izvajanju videonadzora

Videonadzor kot sredstvo tehničnega varovanja je z vidika posameznikove pravice do zasebnosti občutljivo področje. Ker gre pri zajemanju slikovnih podatkov za obdelavo osebnih podatkov, mora biti vsaka izvedba videonadzora zakonita, sorazmerna in transparentna. V nasprotnem primeru lahko pride do kršitev temeljnih človekovih pravic, zlasti pravice do varstva osebnih podatkov in zasebnosti, zaščiteneh tako s Splošno uredbo o varstvu podatkov (GDPR) kot z Ustavo Republike Slovenije (čl. 38).

2.3.1 Zakonska podlaga in zakoniti interes

Za zakonitost obdelave osebnih podatkov mora biti izpolnjen vsaj eden od pogojev iz 6. člena (1) GDPR. Pri videonadzoru je najpogosteje uporabljena pravna podlaga zakoniti interes upravljalca (čl. 6(1)(f), GDPR), kadar namen ni določen z zakonom. Pomembno je, da ta interes:

- zasleduje legitimen cilj, kot na primer varnost ljudi in premoženja;

- je nujen (brez blažjih alternativ);
- ne prevlada nad interesi ali temeljnimi pravicami posameznika.

Evropski odbor za varstvo podatkov navaja, da mora upravljalec vedno izvesti test tehtanja interesov, ki mora biti dokumentiran, saj ga lahko nadzorni organ (npr. IP RS) kadar koli zahteva. V primerih, ko obstaja visoko tveganje za pravice posameznikov, pa je obvezna tudi ocena učinka (DPIA) (GDPR, čl. 35).

2.3.2 Jasnost in omejen namen snemanja

Videonadzor mora imeti jasno opredeljen namen, ki je specifičen in zakonit. Na primer, snemanje zaradi zaščite premoženja, preprečevanja vandalizma ali varnosti zaposlenih. Nezakonita je uporaba videonadzora za spremljanje učinkovitosti dela zaposlenih, razen če je to izrecno določeno z zakonom ali kolektivno pogodbo (ZVOP-2, čl. 77). Nadaljnja obdelava posnetkov za drug namen brez nove pravne podlage ni dovoljena.

2.3.3 Transparentnost in obveščanje posameznikov

Zakonitost vključuje tudi transparentnost. V skladu s členoma 13. in 14. GDPR mora upravljalec posameznike jasno obvestiti o:

- identiteti upravljalca;
- namenu snemanja;
- pravni podlagi;
- obdobju hrambe;
- pravicah posameznika (dostop, ugovor, izbris itd.);
-

ZVOP-2 v 76. členu določa, da mora biti obvestilo vidno pred vstopom v nadzorovano območje in vsebovati vse bistvene informacije. Nepopolna, zamegljena ali skrita obvestila se štejejo kot kršitev zakonitosti. Na spodnji sliki (Slika 1) je prikazan primer dobre opozorilne nalepke, ki ustreza zakonskim zahtevam ter zagotavlja transparentno in informirano obdelavo osebnih podatkov z uporabo videonadzora.

!!!POZOR!!!



UPRAVLJALEC:

KONTAKT ZA UVELJAVLJANJE PRAVIC POSAMEZNIKA:

☐ **VIDEONADZOR VHODOV V STAVBO**
NAMEN IZVAJANJA VIDEONADZORA

☐ Varovanje ljudi

☐ Varovanje premoženja

☐ Preprečitev ogrožanja zaposlenih

☐ Zagotavljanje nadzora vstopa v in izstopa iz prostora

☐ **VIDEONADZOR DELOVNIH PROSTOROV**
NAMEN IZVAJANJA VIDEONADZORA

☐ Zagotavljanje varnosti ljudi

☐ Zagotavljanje varnosti premoženja

☐ Preprečevanje in odkrivanje kršitev na področju iger na srečo

☐ Varovanje tajnih podatkov

☐ Varovanje poslovnih skrivnosti

☐ Upravljelec ne spremlja žive slike

☐ Upravljelec spremlja živo sliko in nima možnosti zvočne intervencije

☐ Upravljelec spremlja živo sliko in ima možnosti zvočne intervencije

Kontaktne podatke pooblaščenih oseb za varstvo osebnih podatkov (e-mail/tel./oboje), če obstaja:

PRAVNA PODLAGA: Videonadzor se izvaja na podlagi zakonitega interesa in v skladu z določili 77. in 78. člena ZVOP-2. Podatki se lahko posredujejo pogodbenim obdelovalcem upravljalca ter drugim uporabnikom z ustrezno pravno podlago, npr. policiji. Nadaljnja obdelava osebnih podatkov ne pomeni. Avtomatizirano sprejemanje odločitev ne pomeni. Podatki se ne posredujejo v tretje države ali mednarodne organizacije. Posameznik ima pravico do informiranja, dostopa do podatkov, popravila, izbrisa, omejitve obdelave in ugovora. O pravicah se odloča v konkretnem postopku.

PRAVICA DO PRITOŽBE: Posameznik ima pravico, da se pritoži informacijskemu pooblaščenцу, naslov: Dunajska 22, 1000 Ljubljana, e-mail: gp.ip@ip-rs.si, tel: 01 2309 730, spletna stran: www.ip-rs.si.

IZVAJA SE VIDEONADZOR

Slika 1: Primer opozorilne nalepke za videonadzor

Vir: Lasten vir

2.3.4 Načelo sorazmernosti in minimalnega posega

Poleg zakonitosti mora biti videonadzor tudi sorazmeren. To pomeni, da ne sme posegati v zasebnost bolj, kot je nujno potrebno za doseg namena. EDPB v svojih smernicah opozarja, da mora upravljelec pred uvedbo videonadzora preveriti:

- ali je mogoče cilj doseči na drugačen način (npr. mehanske zapore, varnostnik ...);
- ali je območje snemanja omejeno na minimalno potrebno površino;
- ali se uporabljajo dodatne zaščite (npr. avtomatsko brisanje, zameglitev obrazov, registrskih tablic ipd.).

Sodna praksa Sodišča EU (npr. zadeva Rigas Satiksme, C-13/16) potrjuje, da lahko tudi videonadzor v zasebnih prostorih postane nezakonit, če ni utemeljen s tehtnim interesom (Zadeva Rigas Satiksme, 2017).

2.3.5 Skladnost s tehničnimi in organizacijskimi ukrepi

Zakonitost izvajanja videonadzora se ne zaključi z namestitvijo kamer in obvestil. Uredba GDPR v 32. členu zahteva uvedbo ustreznih tehničnih in organizacijskih ukrepov, s katerimi se varujejo integriteta, zaupnost in razpoložljivost podatkov. Ti ukrepi vključujejo:

- omejitev dostopa do posnetkov po načelu najmanjšega privilegija;
- vodenje dnevnikov o vpogledih;
- šifriranje;
- načrte za odziv ob incidentih (npr. vdor v sistem, kraja opreme);
- periodične revizije o skladnosti.

Informacijski pooblaščenec RS v praksi ugotavlja, da je največ nepravilnosti prav na področju:

- pomanjkljive evidence kamer;
- pretiranega snemanja;
- nedokumentirane pravne podlage;
- nedovoljenega dostopa do posnetkov (Informacijski pooblaščenec (IP RS), 2023).

2.3.6 Kazenske posledice in nadzor

ZVOP-2 in GDPR določata stroge sankcije za nezakonito izvajanje videonadzora. Globe so tako za pravne kot tudi fizične osebe izjemno visoke, informacijski pooblaščenec pa lahko izda tudi prepoved izvajanja nadzora, odredi izbris podatkov ali zahteva odpravo pomanjkljivosti.

Za dokazovanje zakonitosti mora upravljalec voditi:

- pisno odločitev o uvedbi videonadzora;
- oceno učinka;
- evidenco dejavnosti obdelave (GDPR, čl. 30, ZVOP-2, čl. 22);
- sledljivost dostopov do posnetkov.

3 TEHNIČNI VIDIKI VIDEONADZORA

Razvoj informacijsko-komunikacijske tehnologije je omogočil razmah naprednih videonadzornih sistemov, ki danes presegajo tradicionalno vlogo zgolj vizualnega nadzora. Sodobni sistemi vključujejo digitalne kamere visoke ločljivosti, pametne analitične funkcije, shranjevanje v oblaku in integracijo z drugimi sistemi za upravljanje varnosti. Takšna orodja ponujajo izjemne možnosti za preprečevanje incidentov, prepoznavanje nevarnosti in podporo pri reševanju kaznivih dejanj.

Vendar pa z zmogljivostjo teh sistemov prihajajo tudi tveganja, zlasti na področju varstva osebnih podatkov. Videonadzor ne zajema več le slike, temveč vse pogostejše omogoča identifikacijo oseb, zaznavanje vedenja, sledenje gibanju in celo avtomatsko prepoznavo obrazov. Te zmožnosti lahko močno posežejo v zasebnost posameznika, zato mora biti njihova uporaba natančno premišljena, zakonita in tehnično zavarovana.

3.1 Vrste in značilnosti videonadzornih sistemov

Videonadzorni sistemi (VNS) se med seboj razlikujejo glede na tehnično zasnovo, način prenosa podatkov, stopnjo avtomatizacije in funkcionalnosti. Njihov uporaba sega od osnovnega vizualnega nadzora do kompleksnih integriranih varnostnih sistemov, ki vključujejo analitiko, biometrične funkcije in obdelavo podatkov v realnem času. Poznavanje različnih vrst videonadzornih sistemov je ključno za razumevanje vpliva njihove uporabe na zasebnost in varstvo osebnih podatkov.

3.1.1 Analogni sistemi (CCTV)

To so tradicionalni sistemi zaprtega kroga (Closed-Circuit Television – CCTV), ki uporabljajo koaksialne kable za prenos videosignala do snemalne enote (Digital Video Recorder – DVR). Glavne značilnosti teh sistemov vključujejo nižjo ločljivost slike, nezmožnost daljinskega dostopa in omejeno funkcionalnost snemanja ter shranjevanja.

Čeprav jih v sodobni praksi postopoma nadomeščajo naprednejši sistemi, so analogne rešitve še vedno prisotne v manjših poslovnih okoljih zaradi enostavnosti uporabe in nizkih stroškov (Lesjak & Savić, 2023). Zaradi odsotnosti napredne obdelave podatkov ti sistemi načeloma pomenijo manjše tveganje za zasebnost, vendar še vedno predstavljajo obliko obdelave osebnih podatkov, zato zanje veljajo zahteve GDPR in ZVOP-2.

3.1.2 Digitalni IP sistemi

Sistemi na osnovi internetnega protokola (IP) omogočajo digitalno obdelavo in prenos podatkov prek omrežij (npr. LAN, WLAN ali internet). Kamere IP omogočajo visoko ločljivost (HD, 4K), oddaljen dostop, digitalno shranjevanje na omrežne snemalnike (NVR) in napredne varnostne funkcije, kot so zaznavanje gibanja, opozorila in integracija z drugimi informacijskimi sistemi (Zhou, 2021).

Zaradi povezave v omrežje IP sistemi prinašajo tudi povečana kibernetiska tveganja, saj so izpostavljeni zlonamernim napadom, nepooblaščenemu dostopu ali vdoru. Zaradi tega je nujna uporaba šifriranja, segmentacije omrežja, požarnih zidov ter močnih gesel in avtentikacije (ENISA, 2022).

3.1.3 Pametni videonadzorni sistemi z analitiko

Najnovejši trendi vključujejo tako imenovane “pametne” videonadzorne sisteme, ki poleg snemanja izvajajo tudi napredno obdelavo videa s pomočjo umetne inteligence (UI) in strojnega učenja. Te funkcije vključujejo:

- zaznavanje gibanja in prepoznavanje obrazov;
- štetje oseb ali vozil;
- zaznavanje nenavadnega vedenja ali zapuščenih predmetov;
- optično prepoznavanje znakov (npr. registrskih tablic).

Takšni sistemi omogočajo avtomatizacijo nadzora in večjo učinkovitost, hkrati pa ustvarjajo visoko tveganje za zasebnost, zlasti pri uporabi biometričnih podatkov. GDPR v 9. členu določa, da je obdelava takšnih podatkov načeloma prepovedana, razen, če obstaja izrecna pravna podlaga (čl. 9, GDPR). (Board, 2020) posebej opozarja, da je uporaba videoanalitike dopustna le ob izvedbi ocene učinka (DPIA) in ustreznem tehtanju interesov.

Raziskava (Mihaescu, 2024) ugotavlja, da številni pametni sistemi niso razviti skladno z načeli “privacy by design”, kar pomeni, da zasebnost posameznika ni zaščitena že na ravni zasnovne tehnologije.

3.1.4 Telesne kamere (Bodycams)

Telesne kamere se uporabljajo predvsem v varnostnih službah, policiji in redarstvu. Njihova prednost je v povečanju transparentnosti in dokazni vrednosti, saj snemajo dogodke iz perspektive uporabnika. Zaradi njihove mobilnosti pa predstavljajo še večji izziv z vidika obveščanja posameznikov in časovne omejitve snemanja.

ZVOP-2 v 80. členu določa, da mora biti uporaba telesnih kamer sorazmerna, da mora biti upravljalce posebej usposobljen za nošnjo le te ter mora zagotoviti obveščanje posameznikov (npr. z vizualno oznako). V praksi pa so ravno ti pogoji pogosto zanemarjeni (Informacijski pooblaščenec (IP RS), 2023).

3.1.5 Videonadzor v oblaku (Cloud VMS)

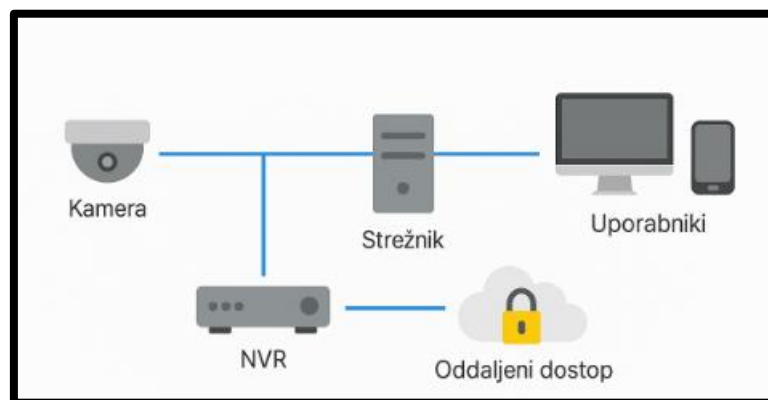
Zaradi nižjih stroškov vzdrževanja in večje dostopnosti se vse več upravljalcev odloča za oblačne rešitve videonadzora. Te omogočajo hranjenje posnetkov na oddaljenih strežnikih, dostop od kjer koli in samodejne varnostne kopije.

Toda uporaba oblačnih sistemov pomeni tudi večjo izpostavljenost kibernetским grožnjam, zato je ključno da upravljalce zagotovi kvalitetno pogodbeno varstvo s ponudnikom, vključno z lokacijo hrambe, protokoli dostopa in šifriranjem (ENISA, 2022).

Zaradi razpršenosti teh sistemov mora biti še posebej jasno, kdo ima dostop do posnetkov, kje se hranijo in kako dolgo – v nasprotnem primeru lahko pride do kršitev določb o čezmernem prenosu podatkov (čl. 44-50, GDPR).

3.2 Osnovni gradniki videonadzornega sistema

Videonadzorni sistem je sestavljen iz več osnovnih tehničnih komponent, ki skupaj tvorijo celoto za zajemanje, prenos, obdelavo, shranjevanje in prikazovanje video vsebin. Delovanje in zanesljivost sistema sta odvisna od pravilnega izbora in integracije teh gradnikov. Sodobni sistemi pogosto vključujejo tudi inteligentne funkcije, vendar osnovna struktura ostaja ključna za tehnično in pravno skladno izvajanje videonadzora (Cehner, 2017).



Slika 2: Osnovni gradniki videonadzornega sistema

Vir: (Lastni vir)

3.2.1 Kamere

Kamera je osnovna komponenta sistema, ki zajema vizualne informacije. Glede na zasnovo ločimo:

- analogne kamere (CCTV) uporabljajo koaksialni kabel, slika se prenaša v analogni obliki;
- IP kamere so digitalne kamere, ki omogočajo prenos slike preko omrežja, pogosto z visoko ločljivostjo (HD, 4K).

Kamere se delijo tudi glede na delovne pogoje:

- barvne kamere delujejo v dobri svetlobi, nudijo realističen prikaz;
- črno-bele kamere so primerne za slabšo osvetlitev;
- dnevno-nočne kamere samodejno preklopijo med barvnim in IR načinom.

3.2.2 Objektiv

Objektiv omogoča usmerjanje svetlobnega signala na slikovni pretvornik (CCD/CMOS).

Njegove ključne lastnosti so:

- vidni kot (širokokotni, ozkokotni);
- zaslonka (f-število), ki določa, koliko svetlobe doseže senzor;
- fokusna razdalja, ki vpliva na povečavo slike.

Objektivi so lahko fiksni ali variofokalni, kar pomeni, da omogočajo ročno ali motorizirano prilagajanje povečave (Cehner, 2017).

3.2.3 Slikovni pretvornik (senzor)

Gre za elektronsko komponento, ki svetlobni signal pretvori v električni signal. Uporabljajo se:

- CCD (Charge-Coupled Device) senzorji – boljši za slabo osvetlitev, dražji;
- CMOS (Complementary Metal – Oxide Semiconductor) senzorji – energijsko učinkovitejši, cenejši, bolj prilagodljivi.

Zahvaljujoč tehnološkemu razvoju danes večina IP kamer uporablja visoko zmogljive CMOS senzorje, ki omogočajo digitalno obdelavo slike že na ravni kamere (Zhou, 2021).

3.2.4 Prenosni mediji

Prenosni medij omogoča prenos video signala od kamere do snemalnika ali strežnika. Glede na sistem razlikujemo:

- koaksialne kable – klasični analogni sistemi;
- UTP/FTP kable (npr. Cat5e, Cat6) – za IP sisteme, z možnostjo PoE (napajanje prek istega kabla);

- optična vlakna – za dolge razdalje, brez elektromagnetnih motenj;
- brezžične povezave – za mobilne, oddaljene ali težko dostopne lokacije (Cehner, 2017).

3.2.5 Napajanje

Kamere in drugi elementi sistema zahtevajo ustrezno napajanje. Možnosti vključujejo:

- ločene napajalnike (12V DC, 23V AC);
- PoE (Power over Ethernet), kjer se napajanje in podatkovni signal prenašata po enem omrežnem kablu;
- baterijsko ali solarno napajanje za oddaljene lokacije.

Za sisteme v kritičnem okolju se uporabljajo tudi rezervni napajalniki (UPS) in prenapetostne zaščite.

3.2.6 Enote za snemanje (DVR/NVR)

- DVR (Digital Video Recorder) – uporablja se z analognimi kamerami;
- NVR (Network Video Recorder) – za IP kamere, pogosto podpira obdelavo signala, analitiko, oddaljeni pristop.

Shranjevanje mora biti prilagojeno zakonitim rokom hrambe (npr. 30 dni v Sloveniji, razen v izjemnih primerih (IP RS, 2023)) in mora omogočati zaščito pred nepooblaščenim dostopom, kot na primer s šifriranjem in/ali avtentikacijo uporabnikov.

3.2.7 Programska oprema (VMS – Video Management Software)

Sistemi za upravljanje videa omogočajo:

- pregled posnetkov v živo in iz arhiva;
- iskanje po dogodkih ali gibanjih;
- integracijo z drugimi sistemi (kontrola pristopa, alarmi);
- analitiko (npr. štetje oseb, zaznavanje nepravilnosti).

VMS mora omogočati tudi upravljanje z uporabniki in revizijsko sledenje, s čimer se izpolnjuje načelo odgovornosti (čl. 5 in 24, GDPR).

3.2.8 Ohišje in okoljski pogoji

Kamere so pogosto nameščene na prostem, zato potrebujejo zaščito pred:

- vremenskimi vplivi (dež, sonce, mraz – IP65/IP66 standardi);
- vandalizmom (IK10 ohišje);
- mehanskimi vplivi (npr. zaščitna kupola).

Določena okolja zahtevajo tudi ATEX zaščito (eksplozijsko ogrožena območja) ali grelnike in ventilatorje za ekstremne temperature.

3.3 Vpliv tehnološkega napredka na videonadzor

Z napredkom informacijske in komunikacijske tehnologije so se videonadzorni sistemi razvili iz preprostih snemalnih naprav v kompleksne digitalne platforme, ki omogočajo zbiranje, obdelavo in analitiko osebnih podatkov v realnem času. Ti razvojni premiki imajo številne pozitivne učinke na varnost, učinkovitost in operativno prilagodljivost, a hkrati pomenijo tudi večje zahteve po skladnosti z zakonodajo in spoštovanju pravic posameznikov.

3.3.1 Visoka ločljivost in digitalna obdelava slike

Ena najpomembnejših sprememb v razvoju videonadzornih sistemov je prehod z analognih sistemov nizke ločljivosti na digitalne rešitve z visoko ločljivostjo. Sodobne IP kamere omogočajo zajem slike v visoki ločljivosti (HD, Full HD, 4K in več), kar zagotavlja bistveno boljše prepoznavnost detajlov, kot na primer obraznih značilnosti, registrskih tablic idr. (Zhou, 2021). Takšne zmogljivosti povečujejo učinkovitost videonadzora kot dokaznega orodja v preiskovalnih postopkih in nadzoru.

Z digitalno obdelavo slike so kamere sposobne izvajati izboljšave slike (npr. zmanjšanje šuma, korekcija osvetlitve), digitalni zoom brez mehanskih komponent, pa tudi lokalno obdelavo videa že na sami kameri. Večina sodobnih IP kamer vključuje tudi funkcije zaznavanja gibanja, prilagajanja kontrasta in digitalne stabilizacije slike, kar povečuje uporabnost posnetkov tudi v težjih okoljskih pogojih (Cehner, 2017).

Povečana ločljivost pa pomeni tudi večjo količino obdelanih podatkov, kar zahteva ustrezno infrastrukturo za shranjevanje, učinkovito kompresijo (npr. kodek H.264, H.265) ter višjo pasovno širino za prenos. Hkrati se s tem povečuje tudi tveganje za varstvo osebnih podatkov, saj kakovostnejši posnetki lažje omogočajo identifikacijo posameznika, kar pomeni, da mora biti upravljalca posebej pozoren na zakonitost obdelave, roke hrambe ter nadzor nad dostopom (čl. 5 in 25, GDPR).

3.3.2 Uporaba umetne inteligence (UI) in videoanalitike

Sodobni sistemi vse pogosteje vključujejo algoritme umetne inteligence, ki omogočajo funkcije, kot so:

- avtomatsko prepoznavanje obrazov;

- štetje oseb;
- zaznavanje nenavadnega vedenja;
- optično prepoznavanje znakov (ANPR).

Sistemi z umetno inteligenco omogočajo boljši odziv na varnostne dogodke, optimizacijo človeških virov in boljše spremljanje tveganj (Mihaescu, 2024). Vendar pa UI sistemom pogosto primanjkuje vgrajenih mehanizmov za zaščito zasebnosti (privacy by design), kar pomeni večje tveganje za pravice posameznikov (Board, 2020).

3.3.3 Povezljivost in dostopnost prek oblakov

Z razvojem oblačnih rešitev (Cloud VMS) so upravljalci pridobili možnost shranjevanja in dostopanja do video posnetkov s katere koli lokacije. Oblačne storitve omogočajo:

- avtomatsko varnostno kopiranje;
- razširljivost (npr. dodajanje kamer brez nove strojne opreme);
- centralizirano upravljanje več lokacij (ENISA, 2022).

Obenem pa takšne rešitve povečujejo izpostavljenost kibernetiskim tveganjem, prenos podatkov v tretje države in izgubo nadzora nad lokacijo obdelave. Zato GDPR v členih 44-50 zahteva natančno pogodbeno ureditev, zlasti pri uporabi zunanjih obdelovalcev in oblačnih ponudnikov.

3.3.4 Mobilnost in oddaljen nadzor

Razvoj mobilnih naprav in širokopasovnih povezav je pomembno spremenil delovanje videonadzornih sistemov. Upravljalci lahko danes prek pametnih telefonov, tablic ali računalnikov dostopajo do videoposnetkov v živo, pregledujejo arhiv, prejemajo opozorila ter upravljajo z nastavitvami kamer, vse to na daljavo. Ta mobilnost omogoča večjo odzivnost in fleksibilnost, hkrati pa prinaša nova tveganja za varnost in zasebnost.

Funkcionalnosti oddaljenega dostopa vključujejo:

- ogled slike v realnem času z večih kamer hkrati;
- vklop ali izklop snemanja glede na zaznane dogodke;
- obvestila o dogodkih;
- tskanje po arhivu glede na časovni žig, dogodek ali zaznano spremembo.

A prav oddaljen dostop pomeni potencialno točko ranljivosti sistema. Slabo zavarovane povezave, uporaba privzetih gesel ali pomanjkanje nadzora nad dostopnimi pravicami lahko vodijo v zlorabe ali krajo podatkov. Zato je ključno, da se za zaščito mobilnega dostopa uvedejo:

- dvostopenjska avtentikacija;
- VPN povezave z IP omejitvami;
- nadzor uporabniških pravic;
- revizijsko sledenje dostopov (ENISA, 2022).

Mobilnost je nedvomno prednost sodobnih sistemov, vendar mora biti podprta z ustreznimi tehničnimi in organizacijskimi varnostnimi ukrepi, da se zagotovi skladnost z zakonodajo in zaščita zasebnosti posameznikov.

3.4 Tehnični ukrepi za varovanje osebnih podatkov

Za zagotavljanje zakonite, varne in transparentne obdelave osebnih podatkov prek videonadzora morajo upravljalci izvajati ustrezne tehnične ukrepe. Ti ukrepi izhajajo iz določb Splošne uredbe o varstvu podatkov (GDPR) in Zakona o varstvu osebnih podatkov (ZVOP-2) ki jih dopolnjujejo priporočila nadzornih organov, kot so Informacijski pooblaščenec RS in ENISA. V nadaljevanju so predstavljeni ključni tehnični mehanizmi za zaščito posnetkov in nadzor nad njihovim obdelovanjem.

3.4.1 Šifriranje posnetkov

Šifriranje je ključni tehnični ukrep za zagotavljanje varnosti videoposnetkov, saj preprečuje, da bi do njih dostopale nepooblaščen osebe. Posnetki morajo biti šifrirani že med prenosom (npr. HTTPS ali VPN) in tudi pri shranjevanju na snemalnikih, strežnikih ali v oblčnih storitvah, z uporabo preverjenih algoritmov, kot je AES-256 (ENISA, 2022). Namen takšnega pristopa je zaščita podatkov tudi v primeru kraje ali vdora.

V praksi mora biti sistem zasnovan tako, da do posnetkov lahko dostopajo le pooblaščen osebe z ustreznimi pravicami in orodji. Snemalne enote uporabljajo šifriran prenos med kamerami in DVR, hkrati pa so vključeni tudi mehanizmi za upravljanje z dekripcijskimi ključi. Ključi morajo biti zaščiteni in ločeno shranjeni, dostop pa mora biti tehnično in organizacijsko nadzorovan (Aerodrom Portorož, interna dokumentacija o videonadzoru, 2023).

Z vidika zakonodaje sta šifriranje in varovanje ključev opredeljena kot obvezna ukrepa skladno z 32. členom GDPR ter 74. členom ZVOP-2. Informacijski pooblaščenec v svojih smernicah poudarja, da šifriranje ne sme biti le priporočilo, temveč obvezen element pri vsakemu sistemu, kjer videonadzor vključuje obdelavo osebnih podatkov.

3.4.2 Nadzor dostopa

Nadzor dostopa do videonadzornih sistemov predstavlja ključen element za zagotavljanje varnosti osebnih podatkov. V skladu z načelom najmanjših privilegijev mora biti dostop do posnetkov omogočen le pooblaščenim osebam, in sicer v obsegu, ki je potreben za opravljanje njihovih delovnih nalog (čl. 5(1)(f), GDPR; čl. 74, ZVOP-2). Posamezniki morajo imeti dodeljene edinstvene uporabniške račune, zaščitene z močnimi gesli, pripomočki za dvofaktorsko avtentikacijo ali pristopnimi karticami.

V praksi to pomeni, da se dostop do sistemov beleži in nadzira. V dokumentu *Pravilnik o videonadzoru in pristopni kontroli* (Aerodrom Portorož, interna dokumentacija o videonadzoru, 2023) je jasno določeno, kdo ima pravico do ogleda slike v živo, pregleda arhiva ali upravljanja s posnetki. Poleg tega je v *Tehničnem poročilu o sistemu videonadzora* opisan sistem upravljanja z vlogami, ki omogoča ločevanje pravic med operaterji in skrbniki sistema. Vsi dostopi se evidentirajo, kar omogoča kasnejšo revizijo in sledenje dostopom.

Za dodatno varnost se priporočajo:

- redna preverjanja aktivnih uporabniških računov;
- uvedba časovno omejenih pooblastil;
- uporaba revizijskih dnevnikov.

ENISA (2022) poudarja pomen omejevanja dostopa na osnovi principa “need to know”, saj je neustrezno upravljanje z dostopnimi pravicami eden najpogostejših razlogov za zlorabe videonadzornih podatkov.

3.4.3 Samodejno brisanje po izteku roka hrambe

Načelo omejitve shranjevanja je eno temeljnih načel varstva osebnih podatkov kot ga določa člen 5(1)(e) Splošne uredbe o varstvu podatkov (GDPR). To pomeni, da se osebni podatki, vključno z videoposnetki, ne smejo hraniti dlje, kot je nujno potrebno za dosego namena obdelave. V kontekstu videonadzora je to še posebej pomembno, saj so posnetki pogosto občutljivi in lahko razkrijejo gibanje, navade ali identiteto posameznika.

Slovenska zakonodaja (ZVOP-2, čl. 76) natančneje določa, da je privzeti rok hrambe videoposnetkov največ 30 dni, razen če so ti potrebni za obravnavo konkretnega incidenta, sodnega postopka ali uveljavljanje pravice. Po preteku tega roka mora sistem omogočati samodejno in neodvisno brisanje, brez možnosti vpliva uporabnikov na ta proces. Namen tega je preprečiti naknadno zlorabo ali nenamerno razkritje podatkov. Ta ukrep je vključen v večino

priporočil Informacijskega pooblaščenca RS, ki opozarja na pomen neprekinjenega in preverljivega mehanizma samodejnega brisanja (Informacijski pooblaščenec (IP RS), 2023).

Tehnično mora sistem vsebovati funkcijo samodejne rotacije ali prepisovanja vsebine, vezano na časovno omejen interval. V sodobnih sistemih se to izvaja na ravni snemalnikov, kjer lahko administrator vnaprej določi čas hranjenja in omogoči samodejno brisanje datotek po izteku tega obdobja. Pomembno je tudi, da se ta funkcionalnost redno preverja in da sistem evidentira, kdaj je bil posamezni posnetek izbrisan, kar dodatno prispeva k uresničevanju načela odgovornosti (čl. 5(2), GDPR).

3.4.4 Zapisovanje dnevnikov dostopov (logi)

Zapisovanje dnevnikov dostopov (logov) predstavlja pomemben tehnični ukrep za zagotavljanje sledljivosti pri obdelavi osebnih podatkov v videonadzornih sistemih. Namen logiranja je beleženje vseh aktivnosti v sistemu, predvsem dostopov do videoposnetkov, z namenom preprečevanja zlorab, zagotavljanje nadzora in omogočanje dokazovanja skladnosti z zakonodajo. Po priporočilih Informacijskega pooblaščenca mora sistem beležiti kdo, kdaj in zakaj je nekdo dostopal do posameznega posnetka, ter zagotoviti zaščito teh zapisov pred naknadnimi spremembami ali izbrisi.

Tehnično mora biti sistem zasnovan tako, da omogoča trajno, samodejno beleženje vseh pomembnih dogodkov, pri čemer se priporoča uporaba ločenega dnevniškega modula ali centraliziranega sistema SIEM (Security Information and Event Management). Dnevniki se naj hranijo vsak toliko časa, kolikor traja hramba videoposnetkov, oziroma dlje, če je to potrebno za dokazovanje skladnosti. Ključno je, da sistem podpira preglednost in revizijsko sledljivost, kar tudi nadzornim organom zagotavlja možnost učinkovitega nadzora ob morebitni prijavi kršitve.

3.4.5 Ločevanje pravic uporabnikov

Ločevanje pravic uporabnikov je ključen ukrep za varno upravljanje videonadzornih sistemov, saj zagotavlja, da ima vsak uporabnik dostop samo do tistih funkcij, ki jih dejansko potrebuje. Uredba GDPR v 32. členu in ZVOP-2 v 74. členu predvidevata tehnične ukrepe za preprečevanje nepooblaščenega dostopa, kar vključuje tudi razdelitev uporabniških pravic glede na vloge in odgovornosti.

Uporabniki so v sistemu običajno razvrščeni kot operaterji, skrbniki ali nadzorniki, pri čemer imajo različne ravni dostopa, kot na primer ogled v živo, izvoz ali izbris posnetkov. Informacijski pooblaščenec RS priporoča, da so te vloge natančno dokumentirane, spremembe

pravic pa zabeležene v revizijskih dnevnikih. ENISA dodatno svetuje redno preverjanje uporabniških računov in takojšnjo ukinitve dostopa neaktivnim uporabnikom.

3.4.6 Redno testiranje in posodabljanje programske opreme

Redno posodabljanje in testiranje videonadzornih sistemov je bistveno za zagotavljanje varnosti, stabilnosti in skladnosti s predpisi. Zastarela programska oprema predstavlja resno tveganje za varnost podatkov, saj lahko vsebuje znane ranljivosti, ki jih napadalci izkoristijo za pridobitev nepooblaščenega dostopa do posnetkov ali sistema. Uredba GDPR izrecno zahteva izvajanje ustreznih tehničnih ukrepov, vključno z rednim preverjanjem, ocenjevanjem in posodabljanjem sistemov (Splošna uredba o varstvu osebnih podatkov (GDPR), 2016).

ENISA (2022) priporoča, da organizacije vzpostavijo načrt upravljanja z ranljivostmi, ki vključuje redne varnostne popravke, testiranja funkcionalnosti po nadgradnjah in preverjanje nastavitvev sistemov. Prav tako naj spremljajo objave proizvajalcev opreme o varnostnih pomanjkljivostih (t. i. security advisories), da lahko ukrepajo pravočasno.

4 ORGANIZACIJSKI IN VARNOSTNI UKREPI

Organizacijski in varnostni ukrepi so bistven del varstva osebnih podatkov pri izvajanju videonadzora. Z njimi upravljalec zagotavlja, da so obdelava posnetkov, dostopi do sistema ter ravnanje zaposlenih skladni z zakonodajo in načeli varovanja zasebnosti. Zakonodaje in uredbe predvidevajo sprejetje ustreznih notranjih pravil, določitev odgovornih oseb, vodenje evidenc ter zagotavljanje usposobljenosti vseh, ki sodelujejo v postopkih obdelave.

Smernice (Board, 2020) poudarjajo, da tehnični ukrepi brez organizacijske podpore niso zadostni. Upravljalci morajo zato s pravilniki, postopkovniki, nadzorom in rednim preverjanjem uvesti kulturo skladnosti in odgovornosti. V nadaljevanju bodo obravnavani trije ključni sklopi ukrepov, in sicer nadzor dostopov in evidenc, politike in usposabljanje ter upravljanje s tveganji.

4.1 Nadzor dostopov in vodenje evidenc

Učinkovit nadzor nad dostopom do videonadzornih sistemov je eden ključnih organizacijskih ukrepov za zaščito osebnih podatkov. Namen nadzora dostopov je preprečiti nepooblaščen obdelavo posnetkov ter zagotoviti sledljivost dejavnosti znotraj sistema. Skladno z načelom integritete in zaupnosti (člen 5(1)(f), GDPR ter člen 32 GDPR) morajo upravljalci zagotoviti, da imajo do podatkov dostop le pooblaščen osebe, in to le takrat, ko je to nujno za opravljanje njihovih nalog (Board, 2020).

Za uresničitev teh ciljev je priporočljivo uvesti naslednje ukrepe:

- evidentiranje vseh dostopov, vključno z datumom, uro, uporabnikom, dostopanim posnetkom ter razlogom za dostop;
- določitev stopenj dostopa na podlagi funkcije (npr. varnostnik, vodja varovanja, administrator), kar je v praksi urejeno z notranjim aktom podjetja (Aerodrom Portorož, interna dokumentacija o videonadzoru, 2023);
- uporaba identifikacijskih mehanizmov, kot so osebna gesla, pametne kartice ali biometrična avtentikacija (Informacijski pooblaščenec (IP RS), 2023);
- ločevanje vlog in pristojnosti, tako da se npr. osebi, zadolženi za spremljanje v živo, ne omogoča izvoza ali brisanja posnetkov.

Tudi ZVOP-2 (čl. 71 in 78) določa obveznost vodenja evidence dejavnosti obdelave, kot to zahteva tudi člen 30 GDPR. Ta mora vsebovati podatke o vrstah zbranih osebnih podatkov,

namenu obdelave, kategorijah posameznikov, obdobju hrambe, vrstah dostopa in varnostnih ukrepih.

Redno revidiranje evidenc dostopa in občasno testiranje nadzora sistema (npr. z internim nadzorom ali presojo) omogočata pravočasno odkrivanje morebitnih zlorab ter izpolnjevanje obveznosti načela odgovornosti iz člena 5(2) GDPR. Informacijski pooblaščenec priporoča, da se te evidence hranijo skladno z roki hrambe posnetkov in da so zaščitene pred manipulacijo ali nenamernim izbrisom (Informacijski pooblaščenec (IP RS), 2023).

Za boljšo preglednost obdelave videoposnetkov je dobro, da imajo podjetja vzpostavljene vsaj tri evidence, in sicer Uporabo medijev (snemanje), Uporabo posnetkov (pregledovanje posnetkov, izdelava kopij) in Brisanje ter uničenje medija. Kot dober primer iz prakse so vse tri evidence predstavljene v 8. poglavju Priloge.

4.2 Politike in usposabljanje zaposlenih

Za zakonito in varno izvajanje videonadzora je poleg tehničnih in pravnih zahtev ključnega pomena tudi vzpostavitev jasnih notranjih politik ter dosledno usposabljanje vseh zaposlenih, ki sodelujejo v postopkih obdelave osebnih podatkov. Takšni organizacijski ukrepi so temelj načela odgovornosti (ang. accountability) iz 5. člena GDPR, ki od upravljalca zahteva, da dokaže skladnost z zakonodajo (čl. 5(2), GDPR).

Notranje politike običajno urejajo vse vidike videonadzora: od postavitve kamer in tehničnih zahtev, do postopkov za pridobitev in pregled posnetkov, določitev odgovornih oseb, evidenc dostopov in postopanja v primeru incidentov. Priporočljivo je, da so te politike opredeljene v formalnem aktu, kot je pravilnik o videonadzoru ali pravilnik o varstvu osebnih podatkov, ki mora biti dostopen vsem zaposlenim (Informacijski pooblaščenec (IP RS), 2023).

Zelo pomembno je tudi, da so v pravilniku jasno razdelane vloge in odgovornosti zaposlenih. To vključuje ločevanje pristojnosti med na primer operaterjem sistema, skrbnikom, upravljalcem in obdelovalcem. Prav tako je priporočljivo, da se za vsako od teh vlog izda poseben sklep o imenovanju in da je seznam pooblaščenih oseb voden ažurno.

V skladu z ZVOP-2 (čl. 24 in 71) je nujno tudi, da upravljalec zagotovi usposabljanje zaposlenih, ki imajo dostop do videonadzornih sistemov ali osebnih podatkov. Usposabljanje mora obsegati razumevanje osnov varstva osebnih podatkov, zakonodajnih zahtev, pravil uporabe sistemov ter postopkov ob zaznavi incidenta. Informacijski pooblaščenec priporoča,

da se usposabljanja izvajajo redno, ob vstopu novega zaposlenega ter ob vsaki pomembnejši spremembi sistema (Informacijski pooblaščenec (IP RS), 2023).

V praksi so učinkovita naslednja orodja:

- seznanitveni obrazci in podpisnice, ki potrjujejo, da je bil zaposleni seznanjen s politiko;
- pisna navodila o uporabi sistema in ravnanju s posnetki;
- dokumentirane vaje in preverjanje razumevanja predpisov;
- vklučitev temeljnih načel zasebnosti v splošna varnostna in tehnična izobraževanja (Board, 2020).

Z ustreznimi politikami in usposabljanji se zmanjšuje tveganje za nenamerno kršitev zakonodaje, hkrati pa se v organizaciji gradi kultura varstva osebnih podatkov.

4.3 Ozaveščenost in upravljanje s tveganji

Za videonadzorne sisteme upravljalci izvajajo sistematično oceno tveganj in dvigujejo ozaveščenost vseh vpletenih, saj lahko le tako zagotavljajo skladnost z zakonodajo in odgovorno interpretacijo posnetkov. GDPR (čl. 35) določa, da je treba za obdelavo, ki verjetno predstavlja visoko tveganje (npr. javni nadzor, uporaba obrazne prepoznavne), izvesti oceno vpliva na varstvo podatkov (Data Protection Impact Assessment, DPIA). Med praksami, ki jih priporoča (Video Surveillance Guidance, 2023), je uporaba standardiziranih predlog za DPIA in redna revizija vseh tveganj prek življenjskega cikla sistema.

Ocena tveganja vključuje prepoznavanje težav, kot so preširok dostop, obdelava občutljivih osebnih podatkov, uporaba UI, visok volumen snemanja ali integracija z drugimi sistemi. V literaturi se poudarja, da je pred uvedbo videonadzora potrebno razmisliti o manj invazivnih ukrepih (npr. izboljšana razsvetljava okolice, prostorov ali fizični nadzor) in videonadzor uporabiti le, če ni druge poti.

Uspešna implementacija sistema tveganja vključuje:

- vzdrževanje registra tveganj (npr. vrste tveganj, ocena, ukrepi za ublažitev);
- periodični pregledi in prilagoditve ob vpeljavi novih tehnologij (npr. videoanalitika);
- kombiniranje minimizacije (minimalno zbiranje podatkov) z uporabo principa *privacy by design* in *privacy by default* (Vgrajeno in privzeto varstvo podatkov) (čl. 25, GDPR).

Kompletno upravljanje videonadzornih sistemov zahteva uravnotežen pristop med tehničnimi rešitvami in organizacijskimi ukrepi. Nadzor dostopov, jasno opredeljene politike, redna usposabljanja zaposlenih in sistematično upravljanje tveganj so ključni dejavniki, ki omogočajo

skladnost z zakonodajo ter učinkovito zaščito zasebnosti posameznikov. Le z ustrezno notranjo organizacijo in doslednim izvajanjem pravil lahko upravljalec izpolni obveznosti, ki jih določajo zakoni in uredbe.

Praksa kaže, da organizacije, ki vlagajo v ozaveščanje zaposlenih ter redno preverjajo učinkovitost svojih ukrepov, pomembno zmanjšajo možnosti zlorab in povečajo zaupanje javnosti. Kombinacija pravnega razumevanja, tehnične podpore in organizacijske odgovornosti tvori trdno podlago za zakonito izvajanje videonadzora v sodobnem digitalnem okolju.

5 PRAKTIČNE SMERNICE IN PRIPOROČILA

Zakonodajni in tehnični okvir videonadzora zagotavljata stabilno osnovo za varno in zakonito uporabo tovrstnih sistemov, vendar se pri dejanski implementaciji v praksi pogosto pojavijo izzivi. Zato je zelo pomembno, da se poleg pravil in načel ponudijo tudi konkretne smernice in priporočila, ki organizacijam pomagajo pri vsakodnevnem odločanju in delovanju. Ti napotki morajo biti dovolj jasni, prilagodljivi in izvedljivi, da jih je mogoče učinkovito vključiti v notranje procese.

V tem poglavju bodo predstavljeni izbrani primeri dobrih praks iz Slovenije in tujine, najpogostejše napake pri izvajanju videonadzora ter ključne smernice za zagotavljanje skladnosti z GDPR in ZVOP-2. Namen poglavja je povezati teoretične temelje in pravne obveznosti s praktičnim delovanjem ter tako ponuditi uporabno vsebino tako za strokovnjake na področju varnosti kot za vodstva organizacij, ki upravljajo z osebnimi podatki preko videonadzornih sistemov.

5.1 Primeri dobrih praks v Sloveniji in tujini

Dobre prakse izvajanja videonadzora ponazarjajo, kako je mogoče uskladiti varnostne cilje organizacij z zakonodajnimi zahtevami glede varstva osebnih podatkov. Učinkovitost videonadzornih sistemov ne izhaja zgolj iz tehnične sofisticiranosti, temveč tudi iz odgovornega, premišljenega in zakonitega ravnanja pri njihovi uporabi. Pomembna skupna načela vseh uspešnih praks so sorazmernost, transparentnost, minimalna obdelava podatkov in zagotavljanje pravic posameznikov.

5.1.1 Slovenija

V Sloveniji je uporaba videonadzora razširjena tako v javnem kot zasebnem sektorju, vendar je nadzorovana s precej strogimi pravnimi določili, predvsem z ZVOP-2 in GDPR ter nadzorom Informacijskega pooblaščenca RS. Številne slovenske ustanove so v zadnjih letih izboljšale svojo skladnost z zakonodajo z uvedbo strukturiranih politik videonadzora, internih aktov ter omejitvijo obsega obdelave.

5.1.1.1 Javni sektor

Javni sektor, kot so občine, zdravstvene ustanove, šole in upravne enote, največkrat uporabljajo videonadzor za nadzor nad vhodi v objekte, parkirišči in skupnimi prostori. Glavno je, da je vsako nadzorovano območje vidno označeno z ustreznimi piktogrami in informacijami o upravljalcu, kar določa 76. člen ZVOP-2. Dobre prakse vključujejo tudi omejitev dostopa do

videoposnetkov zgolj na pooblaščen osebe, običajno z uporabniškim imenom in geslom, ter opredeljen rok hrambe, ki le redko presega 30 dni (Informacijski pooblaščenec (IP RS), 2023).

5.1.1.2 Zdravstveni zavodi

Zdravstveni zavodi, kjer je zasebnost še posebej občutljiva, pogosto uporabljajo t. i. segmentiran videonadzor, kjer se snemajo le vhodi, recepcije in kritične točke, kot na primer lekarna, nikakor pa ne čakalnice ali ambulate, saj bi to pomenilo pretiran poseg v pravico do zasebnosti pacientov. Nekateri zavodi so uvedli tudi evidenco upravičenih razlogov za vpogled, kar omogoča sledenje namenu vsakega dostopa do posnetkov.

5.1.1.3 Kritična infrastruktura

V podjetjih, ki delujejo kot kritična infrastruktura (npr. letališča, jedrske elektrarne, elektrodistribucijska podjetja idr.), se uveljavljajo visoki standardi zaščite videoposnetkov. Med dobrimi praksami izstopajo:

- šifriranje posnetkov v tranzitu in mirovanju;
- različne ravni dostopa glede na vlogo zaposlenega (npr. varnostnik, skrbnik sistema ...);
- obvezna avtentikacija;
- redno letno testiranje sistema;
- revizije dostopov.

V določenih primerih podjetja izvajajo tudi DPIA, če sistem vključuje videoanalitiko ali druge nadstandardne funkcije.

5.1.1.4 Zasebna podjetja

Zasebna podjetja, predvsem trgovine, gostinski obrati in poslovni prostori, se pogosto srečujejo z izzivom usklajevanja poslovnih interesov in varovanja zasebnosti. Med pozitivne prakse sodi snemanje zgolj blagajniških linij, brez nepotrebnega snemanja zaposlenih v zalednih prostorih ali strank v čakalnicah in podobnih situacijah. Pogosto je čas hrambe posnetkov skrajšan na 7 do 14 dni, razen v primeru incidentov. Nekatera podjetja zagotavljajo tudi usposabljanje zaposlenih za ravnanje s posnetki, kjer je sam postopek vpogleda tudi dokumentiran z internimi obrazci.

Z razvojem tehnologije in strožjimi pravnimi okvirji se v slovenskih organizacijah krepi zavedanje, da je videonadzor dopusten le, če je nujen, sorazmeren in zakonit. Dobre prakse se zato ne nanašajo le na uporabo opreme, temveč tudi na način odločanja, dokumentiranja in presoje upravičenosti ter na redno preverjanje skladnosti z zakonodajo.

5.1.2 *Tujina*

Izkušnje držav članic Evropske unije in nekaterih drugih razvitih pravnih ureditev na področju varstva osebnih podatkov so dragocen vir dobrih praks, ki lahko služijo kot vzor tudi slovenskim upravljalcem videonadzornih sistemov. Čeprav temeljne zahteve izhajajo iz skupne zakonodaje (GDPR), se nacionalni nadzorni organi pri oblikovanju smernic pogosto osredotočajo na specifične kulturne, pravne in tehnološke okoliščine. Posledično se razvijajo različni pristopi k izvedbi načel, kot so sorazmernost, minimizacija obdelave, transparentnost in pravica posameznika do zasebnosti.

Francija, Nemčija in Združeno kraljestvo veljajo za jurisdikcije z izrazito razvitimi regulatornimi okvirji na področju videonadzora. Njihovi nadzorni organi – CNIL (Francija), DSK (Nemčija) in ICO (Združeno kraljestvo), redno objavljajo podrobne smernice, ki obravnavajo tako tehnične kot organizacijske vidike nadzora, vključno s pravili snemanja na delovnem mestu, upravljanjem podatkov, oceno učinka na zasebnost (DPIA) ter uporabo naprednih tehnologij, kot so biometrija ali videoanalitika.

5.1.2.1 Francija

Francija velja za eno najbolj reguliranih držav na področju videonadzora na delovnem mestu, kjer nadzor izvaja njihov nacionalni varuh varstva podatkov (CNIL). Njegove smernice in odločbe pogosto služijo kot referenca za sorazmernost uporabe videonadzornih tehnologij, transparentnosti obdelave in spoštovanje zasebnosti zaposlenih. CNIL izrecno zahteva izvedbo DPIA pred uvedbo videonadzora zaposlenih, še posebej pri stalnem nadzoru ali sistematičnem snemanju delovnih mest (CNIL, Guidelines on DPIA, 2017). Poleg tega prepoveduje snemanje prostorov, kot so sanitarije, prostori za odmor ali zasebne pisarne, razen v izjemnih, vnaprej obrazloženih primerih (CNIL, Guidelines on DPIA, 2017).

CNIL je večkrat izrazil zaskrbljenost nad prekomernim in nepreglednim nadzorom zaposlenih, zlasti kadar je snemanje stalno in neustrezno utemeljeno. V primeru podjetja Unionrad je na primer CNIL zaključil, da stalna videonadzorna dejavnost ni bila sorazmerna z varnostnimi cilji in predstavlja prevelik poseg v zasebnost (CNIL, Security of personal data, 2018). Prav tako je bilo kaznovano francosko nepremičninsko podjetje zaradi podobnega principa, kjer so brez izvedene DPIA spremljali zvok in sliko zaposlenih brez ustrezne transparentnosti in brez varnih načinov dostopa do podatkov (Employee Monitoring at Work, 2025).

Francoski CNIL prav tako zahteva spoštovanje načel minimalne obdelave, kjer se sme snemati samo toliko, kot je nujno za zaščito ljudi ali premoženja in omejevanje hrambe podatkov,

skladno z najustreznejšim ciljem varstva. Pomembno je tudi jasno obveščanje zaposlenih o uporabi videonadzora, imenovanje odgovornih oseb ter uporaba notranjega zakona in internega pravilnika, katera definirata postopek zasebnosti (CNIL, Security of personal data, 2018).

5.1.2.2 Nemčija

V Nemčiji veljajo za področje videonadzora izjemno strogi standardi, ki izhajajo iz razlage določb GDPR, pa tudi iz sodne prakse in posebnih smernic nemških nadzornih organov (t. i. "Datenschutzkonferenz"). Leta 2021 so organi izdali posodobljene smernice za izvajanje videonadzora s strani zasebnih subjektov (Datenschutzkonferenz, 2021), ki natančno določajo pogoje za zakonito izvajanje obdelave z video napravami.

Ključna zahteva je, da se vsako izvajanje videonadzora utemelji po zakonitem interesu upravljalca (čl. 6(1)(f), GDPR), ki mora biti natančno opredeljen glede na pravice in svoboščine posameznika. To pomeni, da mora upravitelj izvesti t. i. test sorazmernosti, kjer primerja korist nadzora (npr. preprečevanje tatvin, zaščita osebja) z morebitnim posegom v zasebnost. Smernice posebej poudarjajo, da videonadzor ni dovoljen iz preventivnih razlogov, če ni konkretne grožnje ali zgodovine incidentov.

V Nemčiji je dodatno priporočeno, da organizacije pripravijo vizualno oceno pokritosti (npr. tloris z območji snemanja), kar omogoča natančno presojo, ali je obseg snemanja res nujen. Prav tako se spodbuja anonimizacija ali zameglitev nepomembnih področij (npr. cest ali sosednjih objektov), kar je možno z uporabo sodobnih sistemov za dinamično zakrivanje slike (Datenschutzkonferenz, 2021).

Samodejno brisanje posnetkov po največ 72 urah (razen v primeru incidenta), dnevniški sistem dostopa in ustrezna obveščenost posameznikov prek jasnih obvestil na vhodih v nadzorovana območja so sestavni del nemškega modela skladnosti. Priporočene so tudi notranje smernice, ki zaposlenim natančno določajo pravice, omejitve in postopke pri uporabi videoposnetkov. V primerih snemanja na delovnem mestu je skoraj obvezna ocena učinka za zasebnost (DPIA) in vključitev predstavnikov zaposlenih (npr. sindikata) v presojo.

5.1.2.3 Združeno kraljestvo

Združeno kraljestvo ima vzpostavljen enega najcelovitejših regulatornih okvirjev za izvajanje videonadzora, ki temelji na britanskem Zakonu o varstvu podatkov iz leta 2018 (Data Protection Act 2018) in na priporočilih Information Commissioner's Office (ICO). Ta je leta 2023 objavil posodobljene smernice o uporabi videonadzora, ki organizacijam vseh velikosti ponujajo jasna navodila za zakonito in sorazmerno obdelavo osebnih podatkov z video napravami (ICO, 2023).

Eden bolj pomembnih poudarkov ICO je, da mora biti vsaka odločitev o uvedbi videonadzora vodena z načelom *“privacy by design and by default”*, kar pomeni, da se mora varstvo zasebnosti vgrajevati že v zasnovu sistemov. Pred uvedbo nadzora se priporoča izvedba ocene učinka na varstvo podatkov (DPIA), zlasti kadar gre za snemanje javnih mest, delovnega okolja ali uporabo naprednih tehnologij, kot so videoanalitika in biometrična prepoznavna.

Smernice ICO določajo tudi, da mora biti vsak sistem videonadzora podprt z jasno opredeljenim namenom, npr. varnost oseb, preprečevanje kriminala ali zaščita premoženja. Območje snemanja mora biti minimalno potrebno in ne sme posegati v območja, kjer posamezniki pričakujejo več zasebnosti, kot so sanitarije, dvigala, prostori za počitek ipd. Pomembna dobra praksa je tudi uporaba tehničnih rešitev za zamegljevanje področij, ki niso relevantna za varnostne namene.

Poleg tehničnih vidikov ICO priporoča tudi organizacijske ukrepe, kot so vzpostavitev notranjih politik, usposabljanje osebja, določitev oseb za upravljanje sistemov in redno revizijo delovanja. Videonadzorni sistem mora omogočati revizijsko sledljivost (logiranje dostopov), posnetki pa morajo biti zaščiteni pred nepooblaščenim dostopom. Pomembno je tudi, da se posameznikom omogoči uveljavljanje pravic, kot na primer pravica do dostopa do posnetkov, v primeru da so na njih prepoznani.

ICO izpostavlja, da mora biti celotna obdelava podatkov dokumentirana in pregledna, kar vključuje tudi redno preverjanje skladnosti ter odzivnost v primeru prijav kršitev. Dobro prakso predstavlja tudi objava t. i. Transparency Notices v bližini nadzorovanih območij, ki posameznikom jasno pojasnjujejo, kdo je upravljalec, za kakšen namen se izvaja snemanje ter kako lahko uveljavljajo svoje pravice.

5.2 Sinteza dobrih praks izvajanja videonadzora v Sloveniji, Franciji, Nemčiji in Združenem kraljestvu

Ob pregledu regulativnih okvirov in dejanskih izvedbenih praks v štirih evropskih državah, Sloveniji, Franciji, Nemčiji in Združenem kraljestvu, se izrišejo jasne skupne smernice za skladno, zakonito in sorazmerno izvajanje videonadzora. Čeprav se zakonodaje nekoliko razlikujejo v podrobnostih, vse štiri države temeljijo na načelih GDPR in dopolnilnih nacionalnih aktih.

5.2.1 Skupne točke

- Sorazmernost in zakoniti interesi: v vseh državah mora biti videonadzor utemeljen z zakonitim interesom in nujnostjo za določen namen (npr. varnost, zaščita premoženja). Prekomerno snemanje brez konkretnega razloga je nedopustno.
- Transparentnost: obvezno je jasno označevanje nadzorovanih območij ter informiranje posameznikov o upravljalcu, namenu in njihovih pravicah.
- DPIA (ocena učinka na varstvo podatkov): priporočena ali obvezna je pri snemanju zaposlenih, uporabi videoanalitike ali večjih sistemih (zlasti Francija, Nemčija in Združeno kraljestvo).
- Omejitev hrambe: vse države priporočajo najkrajši možni čas hrambe posnetkov, običajno največ 30 dni, razen ob utemeljenih incidentih.
- Dostop samo pooblaščenim osebam: strogo omejen dostop do videoposnetkov, vključno z beleženjem vpogledov in pravic uporabnikov.
- Organizacijski in tehnični ukrepi: vključujejo šifriranje, vodenje dnevnikov (logov), ločevanje dostopnih pravic in redno testiranje sistemov.
- Zamejitev snemanja občutljivih območij: prepoved snemanja sanitarij, prostorov za počitek, dvigal in zasebnih delovnih mest je v vseh državah standard.

5.2.2 Posebnosti po državah

Država	Posebnosti
Slovenija	Močno sledenje smernicam Informacijskega pooblaščenca RS, dobra praksa v javnem sektorju (označevanje, omejena hramba, omejen dostop ...). Še vedno razmeroma pomanjkljivo izvajanje DPIA v zasebnem sektorju.
Francija	Strogo nadzorovana uporaba videonadzora na delovnem mestu, obvezna DPIA, prepoved snemanja pisarn brez utemeljitve, visoka transparentnost.
Nemčija	Zelo podrobne smernice (Orientierungshilfe), zahteva po tehtanju zakonitega interesa, priporočila za zamegljevanje in vizualno presojo pokritosti.

Združeno kraljestvo	Vodenje po načelih “ <i>privacy by design</i> ”, natančna navodila za uporabo videoanalitike in biometrije, redne notranje presoje in obveznost revizijske sledljivosti.
---------------------	--

Tabela 1: Povzetek Posebnosti po državah

Vir: Lasten vir

5.2.3 Sklepna ugotovitev

Dobre prakse v omenjenih državah kažejo, da zakonit in učinkovit videonadzor zahteva kombinacijo tehničnih rešitev, organizacijskih ukrepov in pravne presoje. Skladnost z GDPR ni le formalna, temveč vključuje celovit pristop k upravljanju tveganj, zagotavljanju transparentnosti in spoštovanju temeljnih pravic posameznikov. Učinkovite rešitve se kažejo v celostni regulaciji, od predhodne presoje do spremljanja izvajanja in preverjanja učinkov sistema.

5.3 Najpogostejše napake izvajalcev videonadzora

Kljub jasnim zakonskim zahtevam in številnim smernicam nacionalnih ter evropskih nadzornih organov se pri izvajanju videonadzora v praksi še vedno pojavljajo številne ponavljajoče se napake, ki lahko vodijo do nezakonite obdelave osebnih podatkov ter kršitve pravic posameznikov.

1. Pomanjkanje jasnega namena snemanja

Ena najpogostejših napak je izvajanje videonadzora brez jasno določenega, zakonitega in sorazmernega namena. Pogosto se kamere postavljajo “za vsak primer”, kar ni dopustno. Namen snemanja mora biti opredeljen že pred namestitvijo sistema in dokumentiran v internih aktih.

2. Nepopolno ali neustrezno obveščanje posameznikov

Upravljalci pogosto ne poskrbijo za ustrezno označitev območij, kjer se izvaja videonadzor ali pa opozorila ne vsebujejo vseh zakonsko predpisanih informacij (npr. kontaktnih podatkov upravljalca, namena snemanja, pravic posameznikov). To pomeni kršitev načela transparentnosti iz člena 5(1)(a) GDPR.

3. Snemanje prostorov, kjer posamezniki pričakujejo večjo stopnjo zasebnosti

Pogosta praksa, ki jo Informacijski pooblaščenec dosledno sankcionira, je snemanje garderob, sanitarij, prostorov za počitek in zasebnih pisarn. Takšno snemanje praviloma pomeni nesorazmeren poseg v zasebnost in je dovoljeno le izjemoma, ob izjemno tehtnih razlogih.

4. Predolga hramba posnetkov

GDPR ne določa natančnega roka hrambe, vendar pa določa, da se osebni podatki ne smejo hraniti dlje, kot je to potrebno za namen obdelave (čl. 5(1)(e), GDPR). V praksi se pogosto srečujemo s hranjenjem posnetkov več mesecev brez pravne podlage. Smernice IP RS in EDPB priporočajo običajen rok največ 30 dni.

5. Nepopoln nadzor dostopov in pomanjkanje logov

Veliko organizacij ne beleži dostopov do posnetkov (npr. kdo, kdaj, zakaj), kar pomeni, da ni mogoče zagotoviti revizijske sledi v primeru zlorabe. Pogosto tudi ni jasno, kdo ima kakšna pooblastila glede dostopa do videonadzornega sistema.

6. Neizvedba ocene učinka na varstvo podatkov (DPIA)

Čeprav je DPIA zakonsko zahtevana za večje ali občutljive videonadzorne sisteme (npr. v delovnem okolju, na javnih mestih, pri uporabi videoanalitike), se pogosto sploh ne izvede, ali pa ni ustrezno dokumentirana (Board, 2020).

7. Neustrezna zaščita sistema in posnetkov

Uporaba zastarelih sistemov brez šifriranja ali rednega posodabljanja lahko predstavlja veliko tveganje za uhajanje podatkov. Prav tako pogosto ni ustrezno omejeno kopiranje, prenos ali brisanje posnetkov.

5.4 Smernice za skladnost z GDPR in ZVOP-2

Za zakonito izvajanje videonadzora ni dovolj zgolj tehnična namestitvev sistema, temveč celovit pristop, ki vključuje pravne, organizacijske in tehnične ukrepe. Spodaj so predstavljene pomembne smernice, ki temeljijo na določilih GDPR in ZVOP-2, smernicah IP RS in priporočilih EDPB.

- **Predhodna ocena tveganj (DPIA);**
- **oblikovanje jasnih politik in postopkov;**
- **transparentnost in označevanje;**
- **načelo minimizacije;**
- **tehnična zaščita posnetkov;**
- **nadzor dostopov in revizijska sledljivost;**
- **usposabljanje zaposlenih in redni pregledi.**

5.4.1 *Predhodna ocena tveganj (DPIA)*

Ocena učinka na varstvo podatkov je obvezna, kadar videonadzor predstavlja visoko tveganje za pravice in svoboščine posameznikov (čl. 35, GDPR). To velja zlasti pri sistematičnem snemanju javnih mest, delovnega okolja ali uporabi naprednih funkcionalnosti (npr. videoanalitika ali prepoznavanje obrazov). DPIA mora vsebovati analizo namena, obsega obdelave, tveganj in ukrepov za njihovo ublažitev (Board, 2020).

5.4.2 *Oblikovanje jasnih politik in postopkov*

Vsaka organizacija mora imeti jasno napisan pravilnik o videonadzoru, ki določa namen snemanja, lokacije kamer, roke hrambe posnetkov, dostopne pravice, odgovorne osebe in postopke ob incidentih. Politike morajo biti dostopne zaposlenim in redno posodobljene.

5.4.3 *Transparentnost in označevanje*

Obvezna je vidna in razumljiva označitev vseh nadzorovanih območij, ki mora vsebovati:

- ikono (piktogram) za videonadzor;
- podatke o upravljalcu (naziv, kontakt);
- namen snemanja;
- osnovne informacije o rokih hrambe in pravicah posameznikov. ZVOP-2 (čl. 76) določa, da mora biti obvestilo nameščeno pred vstopom na nadzorovano območje (Informacijski pooblaščenec (IP RS), 2023).

5.4.4 *Načelo minimizacije in sorazmernosti*

Sistem mora biti zasnovan tako, da zajema samo nujno potrebne prostore, z omejitvijo časa hrambe (največ 30 dni, razen ob preiskave incidentov) ter izključitvijo območij, kjer posamezniki pričakujejo večjo stopnjo zasebnosti (npr. sanitarije, dvigala ...) (čl. 5(1)(c), GDPR) (Board, 2020).

5.4.5 *Tehnična zaščita posnetkov*

Posnetki morajo biti zaščiteni z ustreznimi tehničnimi ukrepi:

- šifriranje prenosa in shranjenih podatkov;
- uporaba avtentikacije (močna gesla, pametne kartice);
- redno posodabljanje sistemov in testiranje varnosti;
- zaščita pred nepooblaščenim kopiranjem ali spreminjanjem.

5.4.6 Nadzor dostopov in revizijska sledljivost

Dostop do posnetkov mora biti strogo omejen na pooblaščne osebe. Vsak vpogled, kopiranje ali brisanje posnetkov mora biti evidentirano v dnevnikih (logih), ki vsebujejo podatke o uporabniku, datumu, času in namenu dostopa (čl. 30, ZVOP-2) (Informacijski pooblaščenec (IP RS), 2023).

5.4.7 Usposabljanje zaposlenih in redni pregledi

Zaposleni, ki imajo dostop do videonadzornega sistema, morajo biti seznanjeni s pravili varstva osebnih podatkov in internih politik. Organizacije naj izvajajo periodične preglede skladnosti ter posodablajo ukrepe v skladu z razvojem tehnologije ali spremembami zakonodaje (Board, 2020).

6 SKLEP

Diplomsko delo je temeljito preučilo področje varovanja osebnih podatkov, ki jih organizacije zbirajo s pomočjo videonadzornih sistemov, pri čemer je bila osrednja pozornost usmerjena v razumevanje in razlago pravnega, tehničnega in organizacijskega okvira, ki ureja to področje. V hitro razvijajočem se tehnološkem okolju, kjer videonadzor postaja vseprisoten v javnih in zasebnih prostorih, se pojavljajo številna vprašanja o zakonitosti, sorazmernosti in etičnosti obdelave osebnih podatkov. Skladnost z zakonodajo, kot sta Splošna uredba o varstvu podatkov (GDPR) in Zakon o varstvu osebnih podatkov (ZVOP-2), zahteva celovit in interdisciplinaren pristop, ki vključuje jasno opredeljene postopke, ustrezno tehnično opremo ter ozaveščeno in usposobljeno osebje. Diplomaska naloga je skozi teoretični pregled literature, analizo zakonodaje, strokovnih priporočil in primerov iz prakse ponudila celostno obravnavo te problematike.

Namen naloge je bil identificirati ključna področja, kjer prihaja do neskladnosti v praksi, prepoznati tehnična in organizacijska tveganja ter na podlagi preučene zakonodaje in primerov oblikovati priporočila za izboljšave. V ta namen je bilo delo strukturirano tako, da zajema temeljne zakonske zahteve (GDPR, ZVOP-2), tehnične vidike videonadzora (sistemske arhitekture, varnostne funkcionalnosti, videoanalitika) ter organizacijske pristope (evidence, notranji pravilniki, dostopi, izobraževanje). V okviru raziskave so bile oblikovane tri raziskovalne hipoteze, ki so bile kritično analizirane in ovrednotene na podlagi ugotovitev posameznih poglavij. Delo je tako doseglo zastavljene cilje, saj ponuja strukturiran pregled ključnih izzivov in konkretne rešitve za izboljšanje zakonitosti in učinkovitosti pri izvajanju videonadzora.

H1: Organizacije pogosto izvajajo videonadzor brez popolne skladnosti z zakonodajo zaradi pomanjkanja znanja in notranjih politik.

Obravnava prve hipoteze temelji na ugotovitvah, da številne organizacije še vedno izvajajo videonadzor na način, ki ni popolnoma skladen z veljavno zakonodajo, predvsem zaradi pomanjkanja strokovnega znanja, sistematičnega pristopa in formaliziranih notranjih politik. Pogosto je videonadzor vzpostavljen ad hoc – brez predhodne ocene učinka na varstvo osebnih podatkov (DPIA), brez jasnega pravnega temelja ali vnaprej določenega namena obdelave. Poleg tega manjkajo ključni dokumenti, kot so pravilniki o videonadzoru, evidence dejavnosti obdelave ali določena interna pooblastila za dostop do posnetkov.

Zaznana je tudi pomanjkljiva ozaveščenost upravljalcev in zaposlenih o svojih obveznostih in odgovornostih v postopkih obdelave. V številnih primerih so nadzorne kamere nameščene brez ustreznega obvestila posameznikom, brez transparentne komunikacije o njihovih pravicah ali brez jasne opredelitve obdobja hrambe posnetkov. To kaže na sistemske pomanjkljivosti, ki jih ne moremo pripisati zgolj nevednosti, temveč tudi pomanjkanju organizacijskih virov in načrtnega pristopa k obvladovanju tveganj, povezanih z zasebnostjo. Hipoteza H1 je s tem **potrjena**: neusklajenost z zakonodajo je pogosto rezultat kombinacije neznanja, odsotnosti jasnih notranjih pravil ter neustrezne vloge vodstva pri uveljavljanju kulture varstva podatkov.

H2: Tehnična zasnova sistema pomembno vpliva na tveganja za zasebnost posameznikov.

Druga hipoteza se osredotoča na neposredno povezavo med tehnično zasnovo videonadzornega sistema in tveganji za zasebnost posameznikov, kar se je skozi celotno raziskavo potrdilo kot ključni dejavnik. Tehnični elementi sistema, kot so vrsta uporabljenih kamer, lokacija postavitve, zmogljivost snemanja, način shranjevanja posnetkov, možnosti oddaljenega dostopa in uporaba vidoanalitike, niso nevtralni, temveč oblikujejo temeljne pogoje obdelave osebnih podatkov.

Slabo zasnovani sistemi, ki na primer omogočajo neomejen dostop brez preverjanja identitete uporabnikov, ne uporabljajo šifriranja ali ne omogočajo revizijske sledi, ustvarjajo izjemno visoka varnostna tveganja in povečujejo verjetnost za zlorabe ali nepooblaščne vpogleda. Na drugi strani pa kakovostna tehnična zasnova, ki vključuje šifriranje podatkov, avtomatsko brisanje posnetkov po preteku roka hrambe, ločene ravni dostopa glede na vloge in beleženje vseh aktivnosti, deluje kot pomembno varovalo pred kršitvami zakonodaje.

Posebej izstopa tudi vloga novih tehnologij, kot je umetna inteligenca, ki lahko ob nepravilni uporabi (npr. samodejno prepoznavanje obrazov brez ustrezne pravne podlage) pomeni resen poseg v zasebnost posameznikov. Zato mora biti tehnična zasnova v vsakem primeru prilagojena zakonitim ciljem, sorazmerna glede na tveganja in skladna z načelom "*zasebnost po zasnovi in zasebnost kot privzeta nastavitve*". Na tej podlagi lahko hipotezo H2 zanesljivo **potrdimo**: tehnična struktura sistema pomembno oblikuje tveganja in s tem tudi stopnjo skladnosti z zakonodajo.

H3: Učinkovita organizacijska ureditev (evidence, dostopi, usposabljanje) bistveno zmanjša možnost kršitev in poveča zaupanje uporabnikov.

Tretja hipoteza izpostavlja pomen organizacijskega vidika pri varovanju osebnih podatkov, zlasti v kontekstu uporabe videonadzora. Iz ugotovitev je razvidno, da zgolj pravna skladnost

in tehnična ustreznost ne zadostujeta za zakonito in učinkovito obdelavo osebnih podatkov. Ključno vlogo ima celostna organizacijska ureditev, ki vključuje jasno določene politike, vnaprej opredeljene postopke in redno izobraževanje zaposlenih. Hipoteza H3 je s tem **potrjena**, saj so organizacije z vzpostavljenimi notranjimi akti, evidencami dostopov, nadzorom nad dodeljenimi pravicami ter strukturiranim sistemom usposabljanj občutno manj izpostavljene tveganjem za zlorabe in kršitve.

Ena ključnih organizacijskih praks je dosledno vodenje evidenc dejavnosti obdelave in dnevnikov dostopov do videoposnetkov. Takšna evidenca omogoča sledljivost, odgovornost in nadzor nad vsakim posameznim vpogledom ali obdelavo posnetkov, kar je pomembno tako z vidika zakonodaje kot zaupanja uporabnikov sistema. Prav tako se je izkazalo, da redna usposabljanja in osveščanje zaposlenih o njihovih obveznostih pomembno vplivajo na zmanjšanje tveganja za nenamerne napake ali neustrezno ravnanje z videoposnetki.

Zelo pomembno je tudi, da se notranje politike redno posodabljaajo, usklajujejo z aktualno zakonodajo ter se dejansko izvajajo v praksi, ne le kot formalnost, temveč kot dejansko orodje upravljanja. Takšen celostni pristop krepi tudi zaupanje posameznikov, ki so podvrženi videonadzoru, saj jim organizacija z jasno komunikacijo in odgovornim ravnanjem sporoča, da varstvo njihovih osebnih podatkov jemlje resno. Vse to potrjuje, da so organizacijski ukrepi ključni element učinkovitega varovanja zasebnosti.

Na podlagi analiziranih pravnih določil, tehničnih rešitev in organizacijskih pristopov lahko sklenemo, da uspešno varovanje osebnih podatkov v okviru videonadzora zahteva celovit in usklajen pristop na vseh ravneh, tako na zakonodajni, tehnološki, kot tudi upravljavski. Samo tehnična dovršenost brez jasnih pravil in usposobljenih izvajalcev ne zagotavlja skladnosti, prav tako tudi pravna podlaga brez primerne izvedbe ne preprečuje tveganj za varovanje zasebnosti posameznikov. Ključno spoznanje diplomske naloge je, da mora biti varstvo osebnih podatkov načrtno, premišljeno in vključujoče v smislu notranje odgovornosti organizacije in spoštovanja pravic posameznikov.

V prihodnje bo pomen varovanja osebnih podatkov v okviru videonadzora le še naraščal, zlasti ob razvoju tehnologij, kot so umetna inteligenca, avtomatizirano prepoznavanje obrazov in centralizirani sistemi za spremljanje. To bo zahtevalo še večjo odgovornost upravljalcev in še bolj natančno presojo zakonitosti obdelave. Diplomsko delo s svojimi ugotovitvami, hipotezami in priporočili predstavlja uporabno izhodišče za oblikovanje boljših praks, boljše

zakonodajne skladnosti ter večjega zaupanja v nadzorne tehnologije kot orodje za varnost, ne pa za nepotrebno “invazijo” v zasebnost.

7 VIRI IN LITERATURA

Aerodrom Portorož, interna dokumentacija o videonadzoru. (2023).

Arthur Cox. (2025). Pridobljeno iz https://www.arthurcox.com/knowledge/employee-monitoring-at-work-regulatory-enforcement-actions-against-excessive-employee-monitoring-practices-continue/?utm_source=chatgpt.com

Board, E. D. (29. januar 2020). *Smernice 3/2019 o obdelavi osebnih podatkov z video napravami*. Pridobljeno iz https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_sl

Cehner, A. (2017). Osnove sistemov video nadzora. *Študijsko gradivo*.

CNIL. (2017). *Guidelines on DPIA*. Pridobljeno iz <https://www.cnil.fr/en/guidelines-dpia>
cnil.fr

CNIL. (2018). *Security of personal data*. Pridobljeno iz
https://www.cnil.fr/sites/cnil/files/atoms/files/guide_security-personal-data_en.pdf

Datenschutzkonferenz. (2021). Pridobljeno iz <https://www.datenschutzkonferenz-online.de/>

ENISA. (2022). *Guidelines on Security Measures for Cloud-based Video Surveillance*.
Pridobljeno iz <https://www.enisa.europa.eu/publications/guidelines-on-security-measures-for-cloud-based-video-surveillance>

ICO. (2023). Pridobljeno iz <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/video-surveillance>

Intact Public Entities Inc.. (2012). *Risk management Considerations for Video Surveillance*.
Pridobljeno iz intactpublicentities.ca+1worshipfacility.com+1

Informacijski pooblaščenec (IP RS). (2023). Pridobljeno iz spletno mesto Informacijskega
pooblaščenca RS: https://www.ip-rs.si/varstvo-osebnih-podatkov/obveznosti-upravljavcev/vzpostavitev-videonadzora?utm_source=chatgpt.com

Information Commissioner's Office (ICO). (2023). Pridobljeno iz <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/video-surveillance/>

Lesjak, B., & Savić, M. (2023). *Mednarodno inovativno poslovanje*. Pridobljeno iz
<https://journal.doba.si/OJS/index.php/jimb/article/view/JIBM.2023.15.2.3>

Mihaescu, D. K. (2024). GDPR Compliance in Video Surveillance Systems and Applications.
Journal of Privacy and Security, 45-66.

Splošna uredba o varstvu osebnih podatkov (GDPR). (2016). Pridobljeno iz <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32016R0679>

Zadeva Rigas Satiksme, C-13/16 (4. maj 2017).

Zakon o varstvu osebnih podatkov (ZVOP-2). (15. december 2022). Pridobljeno iz <https://pisrs.si/pregledPredpisa?id=ZAKO7959>

Zhou, Y. L. (2021). Security and privacy in smart surveillance systems. *ACM Computing Surveys*, 1-36.

8 PRILOGE

Priloga 1: UPORABA MEDIJEV (SNEMANJE)

UPORABA MEDIJEV (SNEMANJE)

[illegible]

Legenda :

IOM: Identifikacijska oznaka medijev (CD, DVD, USB ključ... ..)

Priloga 2: UPORABA POSNETKOV

UPORABA POSNETKOV

[illegible]

Legenda :

IOM: Identifikacijska oznaka medijev (CD, DVD, USB ključ ..)

Priloga 3: BRISANJE, UNIČENJE MEDIJA

BRISANJE , UNIČENJE MEDIJA

[illegible]

Legenda :

IOM: Identifikacijska oznaka medijev (CD, DVD, USB ključ ...)