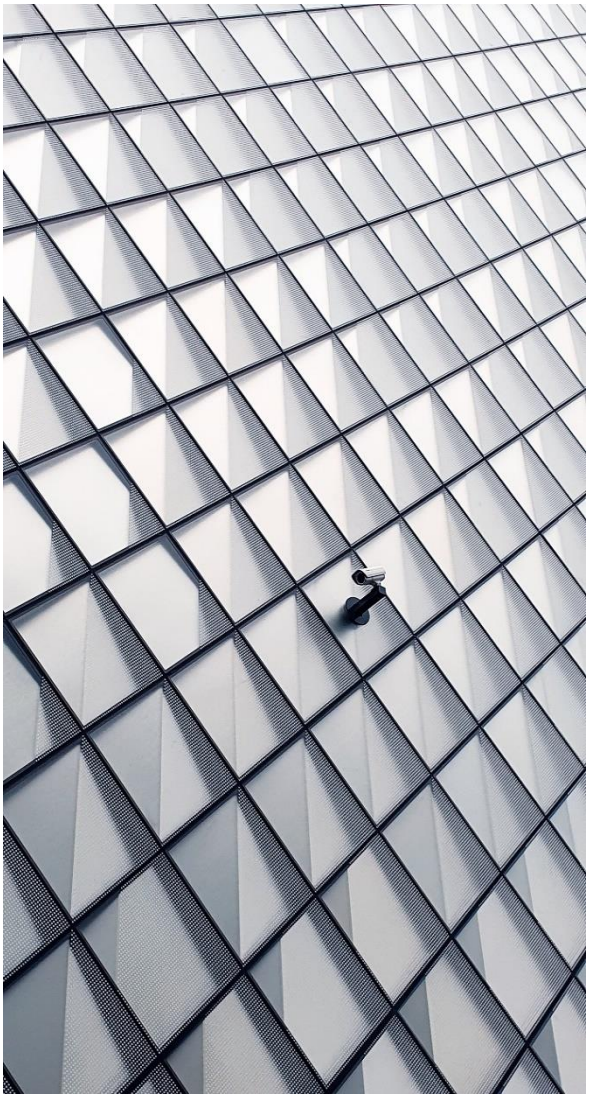


Smernice glede izvajanja videonadzora

Smernice Informacijskega pooblaščenca

INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo odgovore na najpogosteje zastavljena vprašanja glede videonadzora z vidika zahtev Zakona o varstvu osebnih podatkov (ZVOP-2), kot so: splošna zakonska ureditev videonadzora, posebnosti na posameznih področjih (uradni službeni oziroma poslovni prostori, delovni prostori, prevozna sredstva, namenjena javnemu potniškemu prometu, javne površine), ustreznost zavarovanja videonadzornega sistema ter nekatera novejša vprašanja, kot je uporaba kamer v avtomobilih, na osebi uradnih oseb, dostop do videonadzora preko spleta in podobno.
Ciljne javnosti	Izvajalci in uporabniki videonadzora, splošna javnost
Status	javno
Verzija	2.0
Datum izdaje	14. 4. 2023
Avtorji	Informacijski pooblaščenec, vir slik: Unsplash, Flaticon.
Ključne besede	Smernice, videonadzor, kamere, snemanje, nadzor, obdelava osebnih podatkov uporabnikov, sorazmernost, namen obdelave, privolitev uporabnikov, posredovanje podatkov tretjim osebam.

KAZALO

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA

Namen smernic Informacijskega pooblaščenca (v nadaljevanju: IP) je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk osebnih podatkov. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22; v nadaljevanju ZVOP-2) in Splošne uredbe o varstvu podatkov (Splošna uredba; GDPR).

Pravno podlago za izdajo smernic IP daje 56. člen ZVOP-2, ki med drugim določa, da IP daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletnih straneh ali na drug primeren način ter pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- Mnenja IP: https://www.ip-rs.si/mnenja-zvop-2/
- Priročniki in smernice IP: https://www.ip-rs.si/publikacije/priročniki-in-smernice/.

1. UVOD

ZVOP-2 daje, upoštevajoč glede na področja tudi druga dva sistemska predpisa s področja varstva podatkov (to sta Splošna uredba in Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj) zgolj splošen okvir in usmeritve za izvajanje videonadzora, njihovo dokončno zapolnjevanje pa prepušča področni zakonodaji in praksi.

V praksi se tako pogosto pojavljajo vprašanja, ki se nanašajo na konkretno izvajanje videonadzora, zakon pa morda ne predpiše vedno povsem jasno, v kakšnem obsegu in v katerih primerih izvajalci lahko izvajajo videonadzor. To potrjuje tudi praksa IP, saj je področje videonadzora eno od tistih, kjer kot nadzorni organ najpogosteje naleti na kršitve zakonodaje.

S ciljem poenotenja prakse, povečanja jasnosti in pravne varnosti na tem področju IP objavlja pričujoče smernice glede izvajanja videonadzora[1]. Smernice so pri tem zasnovane praktično – v obliki odgovorov na pogosta vprašanja iz prakse, ki jih navajamo po pregledu pravne ureditve vsakega pomembnejšega vprašanja v zvezi z videonadzorom. Upamo, da vam bodo v pomoč - tako tistim, ki se šele odločate za uvedbo videonadzora, kakor tudi tistim, ki ste videonadzor že uvedli, pa morda tega še nimate vzpostavljenega v skladu z določili ZVOP-2.

2. SPLOŠNO O ZAKONSKI UREDITVI VIDEONADZORA

Kaj štejemo za videonadzor?

ZVOP-2, iz zgoraj navedenih razlogov, v svojih določbah o pomenu izrazov (5. člen) oziroma področnih določbah o videonadzoru (76.-80. člen) ne opredeljuje pojma videonadzora[2]. IP zatorej podaja definicijo videonadzora, kot jo je izoblikovala praksa.

Za videonadzor, v najširšem smislu, se šteje **uporabo video kamer za sistematično snemanje, prenos in shranjevanje žive slike z ene lokacije na drugo**, praviloma z namenom zagotavljanja varnosti. Prav tako se za videonadzor štejejo tudi rešitve, ki zajemajo zgolj **prenos žive slike brez snemanja** (t.i. podaljšano oko).

Videonadzor ima več različnih namenov, od katerih je glavni varovanje ljudi ali premoženja. V uradnih službenih oziroma poslovnih okoljih se mu pridružuje tudi namen zagotavljanja nadzora vstopa v te prostore ali izstopa iz njih, preprečevanja ali odkrivanja kršitev na področju iger na srečo, varovanja tajnih podatkov oziroma poslovnih skrivnosti. Videonadzor pri tem olajšuje razreševanje preteklih incidentov, omogoča zavarovanje s temi povezanih dokazov za rabo v morebitnih kasnejših postopkih ter ima nezanemarljiv preventivni učinek, saj naj bi

[1] Smernice se nanašajo na videonadzor, kot ga ureja ZVOP-2 in se ne nanašajo na ureditev po Zakonu o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD).

[2] Več tehničnih informacij o videonadzornih sistemih na splošno je na voljo v Smernicah Evropskega odbora za varstvo podatkov št. 3/2019 o obdelavi osebnih podatkov z video napravami (zlasti poglavje 9.1.).

že njegova prisotnost odvračala potencialne kršitelje. Stranski nameni videonadzora so različni, od izvedbe mejne kontrole, priprave video dokumentacije o določenih dogodkih, nadzora izvajanja izpitov na lokaciji ali na daljavo in tako dalje. Namen uporabe videonadzora je zelo pomemben, saj je prav od njega velikokrat odvisna njegova dopustnost.

Pri tem velja upoštevati, da je tehnologija videonadzora v zadnjih desetletjih izjemno napredovala. Prvotni video nadzorni sistemi so bili sistemi z »neumno kamero« (angl. dumb camera), ki so za analizo posnetka potrebovali stalno prisotnost človeka. Novejše rešitve so prinesle rabo snemalnikov in boljše optične značilnosti kamer, danes pa so na voljo že moderne IP kamere s pripadajočimi računalniškimi vmesniki. Na tržišču so tako na voljo številne kakovostne in cenovno ugodne rešitve za videonadzor, pogosto s kamerami višje ločljivosti, dobrim delovanjem tudi v temnih razmerah ter že vključenimi kontrolnimi centri za shranjevanje, inteligentno video analitiko in obveščanje upravljavca. Videonadzor tako ni več na voljo zgolj večjim javnim in korporativnim uporabnikom, čeprav je prav na tem področju rabe najbolj napredoval. Vseprisotnost cenenih potrošniških naprav z vgrajeno video kamero (in omrežno povezavo) je namreč v zadnjih letih povzročila izjemen porast zasebnega videonadzora. Niso več drage in težko dosegljive rešitve, ki vsakomur omogočajo spremljanje žive slike tudi iz oddaljene lokacije preko računalnika ali mobilnega telefona. Kamere je mogoče namestiti na stanovanjsko hišo, v avtomobil, jih nositi na sebi oziroma v žepu, saj je že vsak pametni mobilni telefon lahko sredstvo videonadzora.

Posledično postajamo vse bolj izpostavljeni videonadzoru tekom vsakodnevnega življenja, naj bo to na cesti na poti v šolo ali službo, v poslovnih in nakupovalnih centrih, na parkirišču pred blokom, na javnih prireditvah,... Videonadzor se pojavlja povsod in vedno več posameznikov oziroma organizacij ima dostop do posnetkov. Posameznikom je vse težje ohranjati njihovo zasebnost in videonadzorni sistemi v veliki meri vplivajo na njihovo vedenje in medsebojno interakcijo.

Na tako povečan občutek posameznika o podvrženosti nadzoru morata zakonodaja in nadzorni organi odgovoriti z ustrezno prilagoditvijo pravil za delovanje in omejevanje videonadzora.

Pregled pravne ureditve videonadzora v ZVOP-2 in drugih zakonih

Prvotni Zakon o varstvu osebnih podatkov iz l. 1990 še ni vseboval določb o urejanju videonadzora. Delno ureditev je prinesel šele Zakon o zasebnem varovanju iz l. 2003[3], vendar zgolj na področju pogojev za izvajanje videonadzora v okviru dejavnosti zasebnega varovanja. To po oceni[4] takratnega Inšpektorata za varstvo osebnih podatkov pri Ministrstvu za pravosodje (predhodnika današnjega IP) ni zadostovalo za pokritje vseh odprtih vprašanj na tem področju, še posebej ne za to, ker je v zvezi z videonadzorom začel prejemati večje število prijav. Posledično je bilo leta 2004 v prenovljeni ZVOP-1 vneseno posebno poglavje o videonadzoru, po vzoru ureditev v Nemčiji in Franciji. Od takrat je videonadzor v slovenskem pravnem redu obravnavan kot ena od posebnih oblik (področij) obdelave osebnih podatkov (v ZVOP-2 v 3. poglavju II. dela – Področne ureditve obdelave osebnih podatkov).

Tako je treba najprej šteti, da za izvajanje videonadzora prvenstveno veljajo iste določbe Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter razveljavitvi Direktive 95/46/ES (v nadaljevanju: **Splošna uredba**) kot za obdelavo osebnih podatkov na splošno, še zlasti tiste o načelih v zvezi z obdelavo osebnih podatkov (5. člen), zakonitosti obdelave oziroma pravni podlagi (6. člen), pravicah posameznika glede posnetkov, na katerih se nahaja (12. – 22. člen) – npr. pravici pridobitve izseka iz nastalega posnetka videonadzora, ki se nanaša nanj (15. člen), zavarovanju nastalih posnetkov pred nepooblaščenimi dostopi (24. in 32. člen), pogodbeni obdelavi - v primeru zaupanja izvajanja videonadzora tretjemu izvajalcu, npr. varnostni službi (28. člen), in evidenci dejavnosti obdelave (30. člen). Tovrstna vprašanja je IP že obširno obravnaval v svojih mnenjih. Enako velja glede določb Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD)[5], kadar izvajajo videonadzor pristojni organi za obravnavanje kaznivih dejanj ali izvrševanje kazenskih sankcij za namene po ZVOPOKD.

Ob splošnih določbah Splošne uredbe (oziroma ZVOPOKD) pa je posebno pozornost treba nameniti določbam 76. do 80. člena ZVOP-2, ki urejajo posebnosti videonadzora v Republiki Sloveniji.

Prvo navedeni 76. člen ZVOP-2 vsebuje **splošne določbe o videonadzoru in varstvu osebnih podatkov**. Uvodoma v prvem odstavku določa, da se določbe navedenih členov uporabljajo za izvajanje videonadzora, če drug zakon ne določa drugače. Določbe ZVOP-2 o videonadzoru so torej subsidiarne, se pravi, veljajo na splošno za vsak videonadzor, lahko pa jih drug zakon za svoje specifično področje še dodatno precizira oziroma spremeni. Takšne posebne določbe vsebuje več zakonov, npr.:

- Že omenjeni Zakon o zasebnem varovanju (Uradni list RS, št. 17/11, glej http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5760), ki predpisuje normative za projektante in izvajalce sistemov tehničnega varovanja s pomočjo videonadzora ter pooblastila zasebnih varnostnikov v zvezi z uporabo tovrstnih sistemov;
- Zakon o detektivski dejavnosti (Uradni list RS, št. 17/11, glej http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5759), ki določa pogoje za uporabo tehničnih sredstev za video snemanje s strani detektivov;
- Zakon o nalogah in pooblastilih policije (Uradni list RS, št. 15/13, 23/15 – popr., 10/17, 46/19 – odl. US, 47/19, 153/21 – odl. US, glej http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314), ki določa pogoje za uporabo tehničnih sredstev za avdio in video snemanje v policiji;

[3] Uradni list RS, št. 126/03, 16/07 - odl. US, 102/07, 96/08 - odl. US, 41/09.
[4] Poročilo o delu Inšpektorata za varstvo osebnih podatkov v letu 2004, oddelek 4.6, glej http://www2.gov.si/zak/Pre_akt.nsf/0/a71531dd2e720b50c12570140035500d?OpenDocument
[5] Uradni list RS, št. 177/20; ZVOPOKD.

- Zakon o izvrševanju kazenskih sankcij (Uradni list RS, št. 110/06 – UPB, 76/08, 40/09, 9/11 – ZP-1G, 96/12 – ZPIZ-2, 109/12, 54/15, 11/18, 200/20 – ZOOMTVI, 141/22, glej http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1223), ki določa namestitev in uporabo videonadzornih sistemov za varovanje varovanih objektov in varovanih območij ter preprečevanje pobegov obsojencev;
- Zakon o sodiščih (Uradni list RS, št. 94/07 - UPB, 45/08, 96/09, 86/10 - ZJNepS, 33/11, 75/12 - ZSPDSLS-A,63/13, 17/15, 23/17 – ZSSve, 22/18 – ZSICT, 16/19 – ZNP-1, 104/20, 203/20 - ZIUPOPDVE, glej http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO332) oziroma na njegovi podlagi sprejet Pravilnik o določitvi varnostnih standardov poslovanja sodišč (Uradni list RS, št. 41/07, glej http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV8321), ki določa okvir za odločanje o varovanju sodnih stavb s pomočjo videonadzora;
- Zakon o igrah na srečo (Uradni list RS, št. 14/11 - UPB, 108/12, 11/14 - popr., 40/14 - ZIN-B, glej http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO409) in Pravilnik o prirejanju posebnih iger na srečo v igralnih salonih (Uradni list RS, št. 31/07, 50/09, 71/09 – popr., 112/09, 105/22, glej http://pisrs.si/Pis.web/pregledPredpisa?id=PRAV5414), ki predpisuje obvezni video nadzor vhodov in igralnih prostorov igralnih salonov;
- Zakon o orožju (Uradni list RS, št. 23/05 – UPB, 85/09, 125/21, 105/22 - ZZNŠPP, glej http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO1440) oziroma na njegovi podlagi sprejet Pravilnik o tehničnih pogojih varovanja prostorov, kjer se nahaja orožje, redu na strelišču in pogojih za izvajanje streljanja (Uradni list RS, št. 66/01, 45/22, glej http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV3934), ki predpisuje obvezni videonadzor za zavarovanje orožja v trgovinah in muzejih..

Naslednji štirje členi ZVOP-2 (77. - 80.) precizirajo pogoje za uporabo videonadzora:

- za nadzor dostopa v uradne službene oziroma poslovne prostore (77. člen),
- znotraj samih delovnih prostorov (78. člen),
- v prevoznih sredstvih, namenjenih javnemu potniškemu prometu (79. člen),
- na javnih površinah (80. člen).

Navedene obveznosti po ZVOP-2 so podrobneje razčlenjene v nadaljevanju.

V 100. do 105. členu ZVOP-2 so določeni **prekrški v zvezi s kršitvami določb o videonadzoru in sankcije zanje**. Tipična globa za kršitev določb 76. do 80. člena ZVOP-2 je v višini od 4.000 do 10.000 eurov za pravne osebe oziroma 8.000 do 20.000 eurov za pravne osebe, ki se po zakonu, ki ureja gospodarske družbe[6], štejejo za srednjo ali veliko gospodarsko družbo, 1.000 do 2.000 eurov za samostojne podjetnike posameznike ali posameznike, ki samostojno opravljajo dejavnost ter 500 do 2.000 eurov za njihove odgovorne osebe in odgovorne osebe državnih organov ali organov samoupravne lokalne skupnosti. Za fizično osebo oziroma posameznika, ki ne opravlja dejavnosti, je predpisana globa v višini 100 do 1.000 eurov.

[6] Zakon o gospodarskih družbah (ZGD-1; Uradni list RS, št. 65/09 – UPB, 33/11, 91/11, 32/12, 57/12, 44/13 – odl. US, 82/13, 55/15, 15/17, 22/19 – ZPosS, 158/20 – ZIntPK-C, 18/21; http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4291)

3. SPLOŠNI POGOJI V ZVEZI Z IZVAJANJEM VIDEONADZORA (76. ČLEN ZVOP-2)

IP ponovno opozarja, da mora biti (tako kot za vsako drugo obdelavo osebnih podatkov) tudi **pravna podlaga za vzpostavitev in izvajanje videonadzora zagotovljena v skladu s prvim odstavkom 6. člena Splošne uredbe oziroma 6. členom ZVOPOKD, ZVOP-2 pa le podrobneje ureja posamezna vprašanja v zvezi z vzpostavitvijo in izvajanjem videonadzora.**

IP šteje, da **v javnem sektorju** (njegova opredelitev je podana v 3. točki drugega odstavka 5. člena ZVOP-2) kot pravni podlagi za zakonito izvajanje videonadzora lahko prideta v poštev **točki (c) in (e) prvega odstavka 6. člena Splošne uredbe**. Pri točki (c) gre za izpolnitev zakonske obveznosti upravljavca (torej je pravna podlaga zagotovljena s posebnim zakonom; glej zgoraj), pri točki (e) pa gre za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu. V primeru izvajanja nadzora s strani zavezancev in za namene po ZVOPOKD morajo biti izpolnjeni pogoji iz 6. člena ZVOPOKD, torej mora biti obdelava določena z zakonom. Ob tem je treba upoštevati tudi določbe 77., 78. ali 80. člena ZVOP-2 oziroma drugega posebnega zakona. Izjemoma je lahko pravna podlaga v javnem sektorju (razen po ZVOPOKD) zagotovljena tudi na podlagi četrtega odstavka 6. člena ZVOP-2, ki določa, da se za izvrševanje točke (e) prvega odstavka 6. člena Splošne uredbe lahko v javnemu sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujno potrebni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo. Pri presoji utemeljenosti obdelave osebnih podatkov na tej pravni podlagi je ključno tehtanje interesov javnega sektorja na eni in interesov posameznikov, na katere se nanašajo podatki, na drugi strani. Obdelava osebnih podatkov ob izvajanju videonadzora tako ne sme biti nesorazmerna in ne sme prekomerno posegati v zasebnost posameznikov.

IP šteje, da **v zasebnem sektorju** (njegova opredelitev je podana v 4. točki drugega odstavka 5. člena ZVOP-2) kot pravni podlagi za zakonito izvajanje videonadzora lahko prideta v poštev točki (**c) in (f) prvega odstavka 6. člena Splošne uredbe**. Pri točki (c) gre za izpolnitev zakonske obveznosti upravljavca (torej je pravna podlaga zagotovljena s posebnim zakonom; glej zgoraj), pri točki (f) pa gre za zakonite interese, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok. Pogoj za uporabo te pravne podlage je izvedba dokumentirane utemeljitve prevladujočega interesa (test tehtanja, v katerem upravljavci izkažejo, da njihov zakoniti interes prevlada nad upravičenim pričakovanjem zasebnosti posameznikov na posnetkih). Tak test tehtanja bi morali upravljavci izvesti pred začetkom izvajanja videonadzora na tej pravni podlagi. Ob tem IP opozarja, da mora biti v primeru uvedbe videonadzora na podlagi točke (f) prvega odstavka 6. člena Splošne uredbe utemeljitev prevladujočega zakonitega interesa (povzetek testa tehtanja) podana tudi v obvestilu posamezniku po točki (d) prvega odstavka 13. člena Splošne uredbe.

ZVOP-2 v 76. členu izvajalcu videonadzora nadalje določa nekatere **splošne obveznosti**, ki jih mora izpolniti za zakonito vzpostavitev in izvajanje videonadzora.

Drugi odstavek 76. člena ZVOP-2 tako določa, da odločitev o uvedbi videonadzora sprejme predstojnik, direktor ali drug pooblaščen posameznik osebe javnega sektorja ali osebe zasebnega sektorja kot upravljavca. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora. Razlogi za uvedbo videonadzora torej ne smejo

biti zgolj našteti, temveč tudi obrazloženi (npr. podkrepljeno s primeri in argumenti, zakaj je dejansko na predvidenih mestih potrebno izvajati videonadzor, kako se bo z njim pripevalo k doseganju zastavljeni ciljev in zakaj milejši oziroma drugi ukrepi niso primerni).

Nadalje 76. člen ZVOP-2 v 3., 4., 5. in 6. odstavku predpisuje način **obveščanja posameznikov o izvajanju videonadzora z objavo ustreznega obvestila**. Obvestilo mora biti **vidno** in **razločno** objavljeno na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove. Takšno obvestilo mora poleg informacij iz prvega (**in drugega**) odstavka 13. člena Splošne uredbe obvezno vsebovati naslednje informacije:

1. pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;
2. namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov;
3. informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave;
4. kontaktne podatke pooblaščene osebe (telefonska številka ali naslov e-pošte);
5. neobičajne nadaljnje obdelave, kot so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.

Namesto objave v obvestilu se lahko obveščanje posameznika izvede tudi na način, da upravljavec informacije iz prvega (in drugega odstavka) 13. člena Splošne uredbe in informacije iz 3. do 5. točke obvestila **objavi na spletnih straneh.** V tem primeru mora na obvestilu iz prejšnjega odstavka objaviti spletni naslov, kjer so te informacije dostopne (URL naslov spletne strani, poleg tega pa lahko tudi QR kodo).

Šteje se, da je s takšnim obvestilom posameznik obveščen o obdelavi osebnih podatkov.

IP posebej opozarja, da mora upravljavec zagotoviti informacije tako iz prvega:

- identiteta in kontaktni podatki upravljavca in njegovega predstavnika, kadar ta obstaja;
- kontaktni podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja;
- nameni, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo;
- zakoniti interesi, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba, kadar obdelava temelji na točki (f) člena 6(1) Splošne uredbe; uporabniki ali kategorije uporabnikov osebnih podatkov, če obstajajo;
- kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo, ter obstoj ali neobstoj sklepa Komisije o ustreznosti ali v primeru prenosov iz člena 46 ali 47 ali drugega pododstavka člena 49(1) sklic na ustrezne ali primerne zaščitne ukrepe in sredstva za pridobitev njihove kopije ali kje so na voljo);

…kot tudi drugega odstavka 13. člena Splošne uredbe:

- obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitev obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;
- kadar obdelava temelji na točki (a) člena 6(1) ali točki (a) člena 9(2), obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica;
- pravica do vložitve pritožbe pri nadzornem organu;
- ali je zagotovitev osebnih podatkov statutarna ali pogodbena obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo;

- obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz člena 22(1) in (4), ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

ZVOP-2 sicer predpisuje, da obvestilo o videonadzoru vsebuje informacije iz prvega odstavka 13. člena Splošne uredbe, vendar **obveznost zagotovitve informacij iz drugega odstavka 13. člena izhaja neposredno iz Splošne uredbe**, zato je navedene informacije treba zagotoviti, četudi ZVOP-2 tega posebej ne predpisuje. V primeru izvajanja videonadzora s strani zavezancev in za namene po ZVOPOKD veljajo zgolj določbe 76. člena ZVOP-2 v povezavi z 23. členom ZVOPOKD, če drug zakon ne določa drugače.

Nekatere informacije iz navedenih odstavkov 13. člena Splošne uredbe in informacije, ki jih mora vsebovati obvestilo o videonadzoru iz četrtega odstavka 76. člena ZVOP-2, se smiselno lahko podvajajo, zato jih v takšnih primerih seveda upravljavec ni zavezan dvakrat objaviti na obvestilu.

IP priporoča, da se navedene informacije iz 13. člena Splošne uredbe in informacije iz 3. do 5. točke obvestila iz 76. člena ZVOP-2 o videonadzoru objavijo na spletnih straneh in ne na samem obvestilu. Slednje pa mora vsebovati najmanj pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor, ter spletni naslov, kjer so dostopne vse ostale informacije (URL naslov spletne strani, poleg tega pa lahko tudi QR kodo). IP priporoča, da obvestilo poleg tega vsebuje tudi namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov. IP pojasnjuje še, da ZVOP-2 sedaj (za razliko od ZVOP-2) zahteva izrecno navedbo **upravljavca** in ne več obdelovalca (npr. zunanje varnostne službe, ki izvaja videonadzor za naročnika-upravljavca).

Sedmi odstavek 76. člena ZVOP-2 določa vsebino zbirke posnetkov videonadzornega sistema. Ta vsebuje posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma, če je to posebej nujno potrebno, pa tudi zvok. Pri tem IP opozarja, da gre glede dopustnosti snemanja zvoka za resnično zelo izjemne situacije in nikakor ne za splošno dovoljeno snemanje zvoka z videonadzornim sistemom – upravljavec mora znati izkazati »nujno potrebnost«, kar pomeni, da na drug način dejansko ni mogoče.

Osmi odstavek 76. člena ZVOP-2 določa način zavarovanja videonadzornega sistema, in sicer mora biti videonadzorni sistem, s katerim se izvaja videonadzor, zavarovan, kot to določata 24. in 32. člen Splošne uredbe. Upravljavec, ki izvaja videonadzor, mora tako skladno z določbami 24. člena Splošne uredbe ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, izvesti ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da obdelava poteka v skladu s Splošno uredbo. Ti ukrepi se pregledajo in dopolnijo, kjer in kadar je to potrebno. Kadar je to sorazmerno glede na dejavnosti obdelave, ti ukrepi vključujejo tudi izvajanje ustreznih politik za varstvo podatkov s strani upravljavca.

Skladno z določbami 32. člena Splošne uredbe mora upravljavec ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se pri različnem obsegu, načinu in okoliščinah izvajanja videonadzora razlikujejo po verjetnosti in resnosti, z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotoviti ustrezno raven varnosti glede na tveganja. Ti ukrepi so odvisno od okoliščin na primer: psevdonimizacija in šifriranje osebnih podatkov, zmožnost zagotoviti stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo, zmožnost pravočasno povrniti razpoložljivost in dostop do osebnih podatkov v primeru fizičnega ali tehničnega incidenta, postopek rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave. Pri določanju ustrezne ravni varnosti se upoštevajo

zlasti tveganja, ki jih pomeni obdelava, zlasti zaradi nenamernega ali nezakonitega uničenja, izgube, spremembe, nepooblaščenega razkritja ali dostopa do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

Deveti odstavek 76. člena ZVOP-2 določa splošni rok hrambe posnetkov videonadzornega sistema, ki se lahko ob upoštevanju načel iz 5. člena Splošne uredbe hranijo **največ eno leto od trenutka nastanka posnetka**. Navedeno velja za vse vrste videonadzora, razen za videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu (rok hrambe takšnih posnetkov je v skladu z drugim odstavkom 79. člena ZVOP-2 največ sedem dni od njihovega nastanka), ter za videonadzor javnih površin (rok hrambe takšnih posnetkov je v skladu s šestim odstavkov 80. člena ZVOP-2 največ šest mesecev od trenutka nastanka posnetka).

Deseti odstavek 76. člena ZVOP-2 določa, v katerih prostorih videonadzora ni dovoljeno izvajati - v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih posameznik utemeljeno pričakuje višjo stopnjo zasebnosti. Zakonodajalec ni mogel taksativno naštetih vseh podobnih prostorov, po naravi stvari pa bi sem sodili npr. tudi prostori za masaže, savne, različne terapije in drugi podobni prostori, kjer enostavno ne pričakujemo kamer.

Enajsti odstavek 76. člena ZVOP-2 določa namene, za katere so dopustni vpogled, uporaba ali posredovanje posnetkov videonadzornega sistema. To je dopustno samo za namene, ki so zakonito obstajali ali bili navedeni na obvestilu v času zajema posnetka. Nedopustno bi bilo npr. posnetke naknadno javno objaviti ali jih uporabiti za prodajo v komercialne namene (brez posebne pravne podlage za to).

Dvanajsti odstavek 76. člena ZVOP-2 določa obveznost zagotovitve možnosti naknadnega ugotavljanja določenih vrst obdelave osebnih podatkov ter rok hrambe podatkov o teh vrstah obdelav. Upravljavec videonadzornega sistema mora za vsak vpogled ali uporabo posnetkov zagotoviti možnost naknadnega ugotavljanja, kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi. Te podatke hrani v dnevniku obdelave iz 22. člena ZVOP-2 dve leti po koncu leta, ko so nastali. Kolikor sistem samodejno ne zagotavlja ozirom podpira takšnega evidentiranja uporabe videoposnetkov, je treba zagotoviti drugačen način beleženja dostopa in uporabe videoposnetkov. Ob tem mora upravljavec v primeru, da videonadzorni sistem spada v sklop iz prvega odstavka 23. člena ZVOP-2, upoštevati tudi zahteve, ki mu jih nalaga ta člen.

Vzorčni (neobvezni) primer dnevnika obdelave oz. manipulacije z videoposnetki je na voljo na povezavi: https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/EVIDENCA_UPORABE_VIDEONADZORNEGA_SISTEMA.doc

Ob tem je treba opozoriti, da morajo upravljavci videonadzornega sistema obdelave v okviru videonadzora tudi ustrezno evidentirati v skladu z zahtevami iz 30. člena Splošne uredbe (evidenca dejavnosti obdelave).

Prav tako je izvajalec videonadzora obvezan, da svoj videonadzorni sistem zavaruje pred dostopom nepooblaščenih oseb. Več o tej obveznosti IP pojasnjuje v 9. poglavju teh smernic.

3.1 Odgovori na pogosta vprašanja

Vprašanje: Ali morajo na obvestilu nujno biti vse sestavine iz četrtega odstavka 76. člena ZVOP-2?

Odgovor: Ne.

Upravljavec, ki izvaja videonadzor, mora na obvestilu navesti vsaj dejstvo (pisno ali grafično), da se izvaja videonadzor ter objaviti spletni naslov (URL naslov spletne strani, poleg tega pa lahko dodatno tudi QR kodo) spletne strani, kjer so dostopne vse informacije iz 13. člena Splošne uredbe ter točke 3. do 5. četrtega odstavka 76. člena ZVOP-2. IP pa vsekakor priporoča, da ob tem navede tudi namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov.

ZVOP-2 vsebino obvestila natančno določa in tudi izrecno kaznuje upravljavce osebnih podatkov, če obvestila ne objavijo ali če (četudi iz malomarnosti) ne vsebuje vseh potrebnih podatkov – glej točki 2. in 3. prvega odstavka 100. člena ZVOP-2, zato upravljavcem svetujemo posebno pozornost pri pripravi obvestil o videonadzoru.

Vprašanje: Ali se lahko obvestilo o izvajanju videonadzora objavi v medijih?

Odgovor: Lahko se objavi, vendar to ne zadosti zakonski zahtevi.

Tretji odstavek 76. člena ZVOP-2 jasno določa, da mora biti obvestilo vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove. To pomeni, da mora biti z izvajanjem videonadzora seznanjen vsak posameznik, ki vstopa v območje videonadzora. Obvestila v medijih ni moč šteti kot zagotovilo, da bodo z videonadzorom seznanjeni vsi posamezniki, ki bodo vstopali v območje videonadzora.

Vprašanje: Ali gre v primeru t.i. podaljšanega očesa (prikaza žive slike na zaslonu brez shranjevanja) tudi za videonadzor?

Odgovor: Da.

T.i. podaljšano oko pomeni uporabo kamer za ogled slike v živo, brez priklopljenega snemalnika. Tipično se uporablja v pogojih, kjer se slika iz kamer prenaša na enega ali več monitorjev na delovnem mestu varnostne službe in kjer je slika na monitorjih spremljana v živo.

Določbe ZVOP-2 veljajo za obdelave osebnih podatkov na področjih, ki jih ureja Splošna uredba ali jih posebej ureja ZVOP-2 in se izvajajo v celoti ali delno z avtomatiziranimi sredstvi, in za drugačno obdelavo kakor z avtomatiziranimi sredstvi za osebne podatke, ki so del zbirke ali so namenjeni oblikovanju dela zbirke. Ob t.i. podaljšanem očesu ni shranjevanja posnetkov in torej zbirka ne nastane, gre pa za avtomatizirano obdelavo osebnih podatkov, zato se za takšno obdelavo uporabljajo določbe Splošne uredbe in ZVOP-2.

Stališče IP je, da se za videonadzor v najširšem smislu šteje uporaba video kamer za sistematično snemanje, prenos in shranjevanje žive slike z ene lokacije na drugo, prav tako pa tudi vse rešitve, ki zajemajo zgolj prenos žive slike brez snemanja (t.i. podaljšano oko). Uporaba video kamer zgolj za tekoči nadzor dogajanja na določenem področju, brez priklopljenega snemalnika, se zato šteje za avtomatizirano obdelavo osebnih podatkov, za katero pa ni potrebno, da zadeva osebne podatke, ki so del zbirke ali so vsaj namenjeni umestitvi v zbirko. Zato se **t.i. podaljšana očesa štejejo za obliko videonadzora in zanje veljajo enake obveznosti kot sicer za kamere s priključenimi snemalniki**. Enaka obravnava je na mestu tudi zavoljo podobnega vpliva na zasebnost, ki ga občutijo posamezniki, ki so izpostavljeni takšnemu nadzoru. IP meni tudi, da je kakršen koli prenos žive slike ali dostop do posnetkov preko mobilnih telefonov, prenosnih računalnikov in drugih tehničnih sredstev osebam, ki niso pooblaščene za izvajanje videonadzora ter izven zakonitih namenov izvajanja videonadzora, nedopusten.

Vprašanje: Ali mora biti obvestilo objavljeno, četudi imamo nameščene »slepe«, torej nedelujoče kamere?

Odgovor: Ne, saj se na podlagi nedelujočih kamer ne obdeluje osebnih podatkov, zato IP uporabo takšnih obvestil odsvetuje, ker predstavljajo nepošten, zavajajoč, nesorazmeren in neprimeren ukrep.

ZVOP-2 varuje osebne podatke, ki so del neke zbirke ali so namenjeni oblikovanju dela zbirke oziroma so avtomatizirano obdelani. Ob uporabi t.i. slepih kamer do snemanja ne pride, zatorej zbirka osebnih podatkov ne more nastati, prav tako se ne izvaja avtomatizirana obdelava osebnih podatkov. Takšne postavitve tako ni mogoče šteti za videonadzor v smislu ZVOP-2.

Ob tem pa IP opozarja, da tudi pri rabi slepih kamer vendarle lahko pride do vpliva na obnašanje posameznika, saj tudi takšne kamere povzročajo občutek nadzorovanosti. Uporabnik takšnih kamer mora zato vseeno računati na možnost pritožb prizadetih posameznikov, posledično pa tudi na možnost inšpekcijskega nadzora s strani IP, kjer bo treba vsakič znova ugotavljati, ali gre zares in izključno za slepe kamere. V nobenem primeru pa naj se niti slepih kamer ne namešča v prostore, kjer v skladu s 76. členom ZVOP-2 izvajanje videonadzora nasploh ni dovoljeno (npr. v dvigalih ali sanitarijah).

Prav tako IP opozarja, da resničnih, a izklopljenih (ali okvarjenih) kamer ni mogoče šteti za slepe kamere, zato je pri teh treba spoštovati vse siceršnje pogoje za zakonito izvajanje videonadzora, podobno pa velja tudi za sistem, kjer je poleg nekaj delujočih tudi nekaj lažnih kamer.

Ali imajo posamezniki res pravico zahtevati posnetke videonadzornega sistema, češ da gre za njihove osebne podatke in ali moramo prekriti obraze drugih oseb? Ali jim to lahko zaračunamo, saj pridobivanje posnetkov pomeni za nas precejšnje stroške?

Odgovor: Da, vendar le do dela videoposnetka, ki se nanaša na njih.

Vsak posameznik ima na podlagi pravice do seznanitve iz 15. člena Splošne uredbe pravico, da od upravljavca videonadzora zahteva seznanitev z lastnimi osebnimi podatki, se pravi s tistim delom videonadzornega posnetka, na katerem je on. To v skladu s tretjim odstavkom navedenega člena vključuje tudi pravico zahtevati pridobitev kopije tega dela posnetka.

Posameznik mora v svojem zahtevku ustrezno navesti podatke, na podlagi katerih je možno identificirati tisti del posnetka, ki se nanaša nanj. To bo praviloma pomenilo, da mora vsaj okvirno navesti, katerim kameram je bil izpostavljen in kdaj, ter podati okvirni opis svoje podobe, oblačil, vozila, številke registrske tablice oziroma ustrezno referenčno fotografijo in ne zgolj pavšalno navesti, da želi vse posnetke, na katerih se nahaja.

Glede stroškov IP pojasnjuje, da mora upravljavec informacije posameznikom po III. poglavju Splošne uredbe (pravica odstopa do lastnih osebnih podatkov, pravica do izbrisa ipd.) zagotoviti brezplačno, lahko pa upravljavec za dodatne kopije, ki jih zahteva posameznik, na katerega se nanašajo osebni podatki, zaračuna razumno pristojbino ob upoštevanju upravnih stroškov posredovanja zahtevanih informacij.

V primeru očitno neutemeljenih ali pretiranih zahtev posameznika, zlasti ker se ponavljajo, lahko upravljavec kljub temu zahtevi ugodi, če je po vsebini utemeljena, in posamezniku zaračuna razumne stroške. Razumni stroški vključujejo samo materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja. Višino glede dodatnih kopij osebnih podatkov, pravila o zaračunavanju, način vnaprejšnjega obveščanja posameznika o nastalih stroških iz prejšnjega odstavka, višino stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov predpiše minister, pristojen za pravosodje, v soglasju z ministrom, pristojnim za zdravje, po predhodnem mnenju nadzornega organa (glej 17. člen ZVOP-2).

4. VIDEONADZOR DOSTOPA V URADNE SLUŽBENE OZIROMA POSLOVNE PROSTORE (77. ČLEN ZVOP-2)

Pravna ureditev videonadzora prostorov v ZVOP-2 ločuje dve različni situaciji. 77. člen ZVOP-2 ureja pogoje za uvedbo videonadzora **dostopa v uradne službene oziroma poslovne prostore**, 78. člen pa **videonadzor znotraj samih delovnih prostorov**. Pri tem so zavoljo večjega posega v zasebnost zaposlenih v drugem primeru pogoji za uvedbo takšnega videonadzora bistveno strožji.

Videonadzor dostopa v uradne službene oziroma poslovne prostore se skladno z določbami 77. člena ZVOP-2 lahko izvaja, **če je to potrebno**:

- za varnost ljudi ali premoženja,
- zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov, ali
- če zaradi narave dela obstaja možnost ogrožanja zaposlenih.

Odločitev o uvedbi videonadzora sprejme predstojnik, direktor ali drug pooblaščen posameznik osebe javnega ali zasebnega sektorja. V svoji odločitvi, ki mora biti sklenjena v pisni obliki, mora ustrezno obrazložiti razloge za uvedbo videonadzora za vsako nameščeno video kamero posebej. Kamere, ki zaradi svojega položaja že očitno

niso namenjene kontroli dostopa, tako ne morejo biti postavljene na tej podlagi, če pa so, jih je treba odstraniti. Potreba po varovanju ljudi in premoženja mora biti izkazana, zlasti tako, da se kamere namesti pred dele poslopja, kjer se nahaja premoženje večje vrednosti (npr. skladišče) ali ki jih je sicer treba varovati (npr. zaradi nahajanja tajnih podatkov).

Z drugimi besedami, predstojnik, direktor ali drug pooblaščen posameznik osebe javnega ali zasebnega sektorja mora vsakič, ko namerava uvesti ali dopolniti videonadzor, oceniti z vidika načela sorazmernosti, ali ga je res potrebno uvesti, in to obrazložiti v pisni odločitvi. Če bo izvajanje videonadzora zaupano zunanji organizaciji (npr. varnostni službi ali upravniku najetih prostorov), mora s to organizacijo skleniti še ustrezno pogodbo o pogodbeni obdelavi (28. člen Splošne uredbe[7]) ter v njej opredeliti vsa vprašanja v zvezi z videonadzorom. O izvajanju videonadzora in o vseh informacijah, ki jih mora v skladu s četrtim odstavkom 76. člena ZVOP-2 vsebovati obvestilo o izvajanju videonadzora, pa mora tudi pisno obvestiti vse zaposlene, ki opravljajo delo v nadzorovanem prostoru.

Alternativno se uvedba videonadzora dostopa lahko določi že z zakonom ali s predpisom, sprejetim na njegovi podlagi. Takšno ureditev določata npr. Zakon o igrah na srečo (ZIS) za kontrolo dostopa v igralnice (78. člen) ali Zakon o tajnih podatkih (ZTP), preko pripadajočega podzakonskega predpisa[8] za videonadzor vhodov in izhodov v varnostna in upravna območja.

Pri sprejemu odločitve o uvedbi videonadzora je potem treba upoštevati še določene omejitve, ki preprečujejo razširitev rabe sistema še na druge namene (t.i. function creep).

Ker so v praksi poslovni prostori velikokrat v isti stavbi s stanovanjskimi enotami, mora izvajalec videonadzora paziti, da se videonadzor izvaja brez snemanja delov stanovanjskih stavb, ki niso uradni službeni oziroma poslovni prostori in brez snemanja vhodov v stanovanja. Navedena določba je bila v ZVOP-2 prenesena iz francoske prakse in jo je treba pri uvedbi nadzora v večnamenskih objektih, ki vsebujejo tako poslovne kot stanovanjske prostore, dosledno spoštovati.

Videonadzor dostopa v uradne službene oziroma poslovne prostore je dovoljen, če s tem soglašajo lastniki teh prostorov, ki imajo v lasti več kot 70-odstotni delež skupnih delov. Stvarnopravni zakonik (SPZ)[9] v tretjem odstavku 105. člena določa, da so skupni deli zgradbe drugi deli, namenjeni skupni rabi etažnih lastnikov, in zemljišče, na katerem stoji zgradba. Med skupne dele lahko spadajo tudi druge nepremičnine.

Zbirka osebnih podatkov v zvezi z nadzorom dostopa v uradne službene oziroma poslovne prostore lahko vsebuje posnetek posameznika (slika oziroma zvok), podatek o lokaciji, datum in čas vstopa in izstopa iz prostora, lahko pa (ob integraciji s sistemi za kontrolo dostopa) tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo skupaj s posnetkom videonadzornega sistema. Osebni podatki oziroma posnetki iz te zbirke se lahko hranijo največ eno leto od trenutka njihovega nastanka.

---

[7] Vse informacije o pogodbeni obdelavi osebnih podatkov so na voljo na: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/pogodbena-obdelava

[8] Uredba o varovanju tajnih podatkov (Uradni list RS, št. 50/22).

[9] Uradni list RS, št. 87/02, 91/13, 23/20.

4.1 Odgovori na pogosta vprašanja

Vprašanje: Ali je lahko obvestilo o izvajanju videonadzora dostopa v uradne službene oziroma poslovne prostore objavljeno v pravilniku o zavarovanju osebnih podatkov?

Odgovor: Da, vendar takšno obvestilo ne zadosti zakonski zahtevi.

Takšno obvestilo se bo namreč štelo le kot del pravilnika, ne pa tudi kot obvestilo v smislu 76. člena ZVOP-2. Posebno obvestilo je še vedno treba objaviti.

Vprašanje: Ali je videonadzor dostopov v službene oziroma poslovne prostore dopustno namestiti oziroma ga uporabiti izključno zaradi kontrole evidentiranja delovnega časa? Ali lahko te posnetke uporabimo za dokazovanje goljufanja pri evidentiranju delovnega časa?

Odgovor: Da, vendar je v vsakem primeru treba oceniti, ali je uvedba videonadzora v skladu z načelom sorazmernosti – ali ne bi mogli želenega namena (v konkretnem primeru kontrolo evidentiranja oziroma preprečitev kršitev pri registraciji delovnega časa) doseči tudi na milejši način, ki bi manj posegal v zasebnost posameznikov (zaposlenih). Za dosego tega namena namreč splošno obstajajo nekatere bistveno manj invazivne metode, zato mora delodajalec izkazati, da s takimi metodami ne more doseči želenega namena, ampak je za to potrebno izvajanje videonadzora. Delodajalec ima pravico do nadzora nad registracijo delovnega časa svojih zaposlenih, pri tem pa mora seveda upoštevati tudi načelo zakonitosti in sorazmernosti.

Upravljavci torej lahko pod pogoji iz 77. člena ZVOP-2 izvajajo videonadzor dostopa v uradne službene oziroma poslovne prostore tudi tako, da kamere zajamejo registracijski terminal za evidentiranje delovnega časa. Posnetki videonadzornega sistema se lahko uporabijo tudi za dokazovanje morebitnih kršitev pravil glede evidentiranja delovnega časa, saj gre za uporabo v okviru dopustnih namenov izvajanja videonadzora dostopa v uradne službene oziroma poslovne prostore.

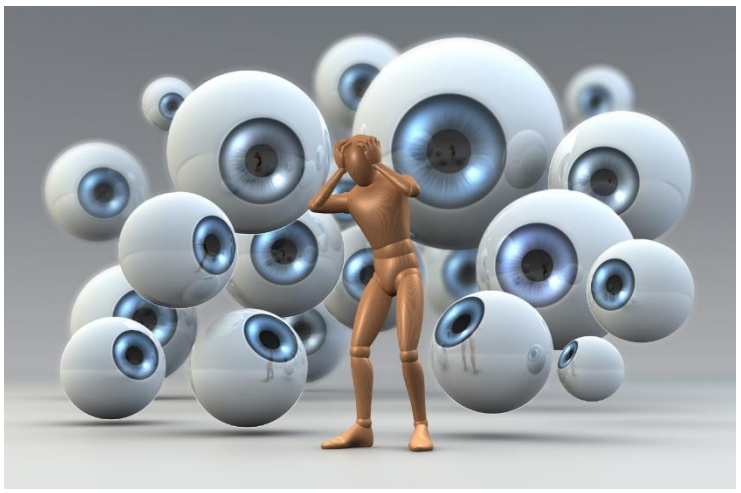
Ob tem je treba opozoriti, da se zgornja pojasnila nanašajo na izvajanje videonadzora, ob katerem ne pride do obdelave biometričnih podatkov zaposlenega.

Vprašanje: Podjetje ima prostore v pritličju stanovanjskega kompleksa, pri čemer je vhod skupen s tistim za prebivalce kompleksa. Kakšni so pogoji za uvedbo kontrole dostopa pri tem glavnem vhodu?

Odgovor: V tem primeru gre hkrati za dostop v poslovne in stanovanjske prostore. Videonadzor se lahko vzpostavi, če s tem soglašajo lastniki, ki imajo v lasti več kot 70-odstotni delež skupnih delov.

V takih primerih IP priporoča, da izvedbo videonadzora organizira upravnik stavbe.

5. VIDEONADZOR ZNOTRAJ DELOVNIH PROSTOROV (78. ČLEN ZVOP-2)



Kot že poudarjeno v prejšnjem razdelku, gre v danem primeru za snemanje delavcev v samih delovnih prostorih, kar predstavlja večji poseg v zasebnost posameznikov. Pri tem IP izpostavlja tudi mednarodno sodno prakso, ki določa, da »morajo biti pravice zaposlenega, ki je v prvi vrsti človek in ne zgolj delavec, spoštovane. Tudi na delovnem mestu ima vsakdo pravico do določene stopnje avtonomije. Podjetja ali druge ustanove ne smejo biti mesta, kjer bi delodajalci arbitrarno in brez omejitev izvajali svoje diskrecijske pravice; ne smejo postati okolja totalnega nadzora, kjer temeljne človekove pravice nimajo veljave«[10].

Posledično je zakonodajalec določil **bistveno strožje pogoje za uvedbo videonadzora znotraj delovnih prostorov**. Namen tega člena je prav »varovanje zasebnosti posameznikov, ki obstaja tudi v delovnih prostorih in se v njo ne sme nesorazmerno posegati« .

Po določbi prvega odstavka 78. člena ZVOP-2 je možno izvajanje videonadzora znotraj delovnih prostorov le v **izjemnih** primerih, kadar je to **nujno potrebno** za varnost ljudi ali premoženja ali preprečevanja ali odkrivanja kršitev na področju iger na srečo ali za varovanje tajnih podatkov ali za varovanje poslovnih skrivnosti, teh namenov pa ni mogoče doseči z milejšimi sredstvi. Navedeni standard "nujno potrebno" se torej razlikuje od standarda "potrebno" v prvem odstavku 77. člena ZVOP-2.

Posledično mora izvajalec videonadzora v vsakem primeru izrecno ugotoviti, ali obstaja milejši ukrep, ki bi omogočal, da zaposleni ne bi bili podvrženi snemanju, torej, ali je uvedba videonadzora zares sorazmerna v ožjem smislu. Izvajalec pa se mora še pred uvedbo posvetovati z reprezentativnim sindikatom pri delodajalcu in svetom delavcem oziroma delavskim zaupnikom o nujnosti uvedbe takšnega videonadzora. Posvetovanje se izvede v roku 30 dni ali v drugem daljšem roku, ki ga določi delodajalec. Kadar gre za uvedbo videonadzora, s katerim se snema delovna mesta, kjer delavec po navadi dela, se posvetovanje izvede v roku 60 dni ali v drugem daljšem roku, ki ga določi delodajalec.

V vsakem primeru morajo biti zaposleni še pred začetkom izvajanja videonadzora **pisno obveščeni** o tem, da se bo začel izvajati videonadzor.

IP dodaja, da je vprašanje varstva zasebnosti v razmerju delodajalec – delojemalec treba reševati vsakokrat od primera do primera, saj se v tem vprašanju sooča več nasprotujočih si interesov – na eni strani interes delodajalca, ki ima pravico do oblasti nad svojimi sredstvi (torej tudi pravico, da jih nadzira), na drugi strani pa je zakoniti interes zaposlenega, ki utemeljeno pričakuje določeno stopnjo zasebnosti in delno samostojnost ter zaupnost tudi na delovnem mestu. Pri varovanju premoženja delodajalca je treba upoštevati tudi pravico do

[10] Glej sodbi Kasacijskega (Vrhovno) sodišča Republike Francije iz oktobra 2001 v primeru S.A. Nikon France v. Frédérick Onof in Evropskega sodišča za človekove pravice iz junija 1997 v zadevi Halford proti Združenemu kraljestvu.

zasebnosti, zato se varovanja premoženja delodajalca ne more izvajati na način, ki bi posamezniku na delovnem mestu povsem odvzel pravico do zasebnosti. Po drugi strani pa pretirano opravičevanje pravice do zasebnosti ne more privesti do položaja, ko bi se s tem povsem izključila tudi pravica do varovanja premoženja delodajalca. Navsezadnje gre za dve ustavni pravici (35. člen (in dalje) Ustave RS – pravica do zasebnosti; 67. člen Ustave RS – lastnina).

Primer napačne presoje tega ravnotežja je IP opredelil v enem od svojih inšpekcijskih primerov: »*V skladu z navedenim Pooblaščenec ugotavlja, da je zavezanec, s tem ko je videonadzorne kamere postavil na način, da je neposredno in neprestano snemal posameznike, nedvomno posegel v njihovo zasebnost. S takšno namestitvijo omenjenih kamer je zavezanec kršil načelo sorazmernosti, saj je osebne podatke (kar fizična podoba posameznika nedvomno je) obdeloval na način, ki po obsegu ni bil primeren za namen, ki ga je navedel za uvedbo videonadzora – varovanje premoženja.* ***Ta namen bi namreč lahko dosegel z milejšimi sredstvi****. Glede na to, da je namen, za katerega se izvaja videonadzor na delovnih mestih, mogoče doseči z milejšimi sredstvi, je zavezanec z izvajanjem videonadzora z v izreku te odločbe navedenimi kamerami kršil tisti del 1. odst. 77. člena ZVOP-1*[11]*, ki določa, da se videonadzor uvede, če katerega od navedenih namenov ni mogoče doseči z milejšimi sredstvi. Nadzornik poudarja, da v konkretnem primeru vidi milejši ukrep v tem, da se zaščiti integriteta posameznikov (zaposlenih)* ***na način, da se videonadzorne kamere izklopijo med delovnim procesom, katerega časovni okvir določi delodajalec****. V času delovnega procesa se namreč v nadzorovanih prostorih nahaja več oseb (zaposlenih), tako je s tega vidika manjša možnosti za morebitne odtujitve opreme, kot bi bila v primeru, ko v prostoru ni nikogar. Prav tako se med delovnim procesom ne bo izvajal psihični pritisk na zaposlene, ki delajo v nadzorovanih delovnih*

[11] Uradni list RS, št. 94/07 – UPB, 177/20, 163/22 – ZVOP-2). Gre za predpis, ki je veljal v času obravnave inšpekcijskega primera in ki je videonadzor delovnih prostorov urejal zelo podobno kot ZVOP-2 (slednji le dodaja namen preprečevanja ali odkrivanja kršitev na področju iger na srečo).

prostorih, na kar opozarja sindikat. Takšna rešitev pa po drugi strani omogoča zavezancu, da kljub temu varuje svojo tehnično opremo v času, ko so odtujitve najbolj možne; torej v času, ko se v prostorih ne izvaja delovni proces«.

IP dodaja, da se videonadzor na delovnem mestu lahko izvaja le glede tistih delov prostorov in v obsegu, kjer je treba varovati interese, navedene v prvem odstavku 78. člena ZVOP-2. Praviloma gre za prostore, kjer se ravna s premoženjem ali informacijami večje vrednosti. Izrecno pa je prepovedano z videonadzorom snemati delovna mesta, kjer delavec po navadi dela, razen če je to nujno v skladu s prvim odstavkom 78. člena ZVOP-2. Seveda tudi znotraj delovnih prostorov velja splošna prepoved izvajanja videonadzora v prostorih izven delovnega mesta, zlasti v prostorih za preoblačenje (garderobah), dvigalih in sanitarnih prostorih.

Neposredno spremljanje dogajanja pred kamerami je pod pogoji iz prvega in drugega odstavka 78. člena ZVOP-2 dopustno le, če ga izvaja izrecno pooblaščeno osebje upravljavca. Ob upoštevanju zgoraj pojasnjenih strogih pogojev za izvajanje videonadzora znotraj delovnih prostorov je videonadzor praviloma dopustno izvajati npr. v trgovinah, v skladiščih, na mestih v proizvodnji, kjer obstaja velika verjetnost odtujitve predmetov ali povzročitve večje škode, na bančnih okencih, nad blagajnami v gostinskih obratih, na delovnih mestih, kjer se posluje z gotovino, na vhodih v sistemske (IT) sobe in upravna notranja območja, na mestih, kjer se hranijo tajni ali drugi zaupni podatki, pri čemer morajo biti kamere usmerjene na nosilce takšnih podatkov in ne na zaposlene. Ni pa videonadzora dopustno izvajati npr. v jedilnicah, na hodnikih, v sejnih in konferenčnih sobah, v čajnih kuhinjah ali v običajnih pisarnah, kjer delajo zaposleni. Pri tem IP opozarja, da se vsak primer presoja posebej, pri čemer se upošteva vse relevantne okoliščine, zato naštetih primerov ni dopustno vzeti kot usmeritev, ki držijo v vsaki situaciji.

Na področju varnosti države in varovanja tajnih podatkov, razen za varovanje tajnih podatkov najnižje stopnje tajnosti, in za koncesionarje po zakonu, ki ureja igre na srečo (ZIS), v delih prostorov, kjer se izvajajo igre na srečo, veljajo določene izjeme. V teh primerih se delodajalec ni dolžan vnaprej posvetovati z reprezentativnimi sindikati pri delodajalcu in svetom delavcev oziroma delavskim zaupnikom.

5.1 Odgovori na pogosta vprašanja

Vprašanje: Ali je dovoljeno, da delodajalec – ob sicer postavljenih obvestilih o izvajanju videonadzora – izvaja snemanje zaposlenih na način, da zaposleni ne vedo, kje so nameščene kamere?

Odgovor: ZVOP-2 delodajalcu sicer ne nalaga dolžnosti predstavitve natančnih lokacijah vseh kamer, mora pa upoštevati vse pogoje iz 76., 77. oziroma 78. člena ZVOP-2. Ključno je torej, da zaposleni ve, da se nahaja v videonadzorovanem območju.

Namen obvestila iz 76. člena ZVOP-2 je torej predvsem v tem, da je posameznik seznanjen, da se izvaja videonadzor ter kje (v katerih prostorih oziroma na katerih mestih) se izvaja videonadzor. Zato sama po sebi taka videokamera ne bi bila sporna, če bi bila postavljena na takšen način, ki je posamezniku pričakovan. Vendar bi moral delodajalec tudi v tem primeru – ko gre za delovne prostore – o takšni postavitvi obvestiti zaposlene. Če tega ni storil, kamere pa so postavljene na način, da snemajo delovne prostore ali dostop v uradne službene oziroma poslovne prostore, krši določila 78. oziroma 77. člena ZVOP-2 v delu, ko bi moral zaposlene pisno obvestiti o uvedbi videonadzora. Delodajalec bi storil prekršek tudi v primeru, če kamere namesti na način, da te

snemajo delovni prostor, pa se pred tem (poleg pisnega obvestila zaposlenim) ni posvetoval tudi z reprezentativnim sindikatom in svetom delavcev oziroma delavskim zaupnikom.

Če delodajalec ne krši ničesar od zgoraj navedenega, lahko torej postavi kamere tudi tako, da se jih sicer ne vidi, vendar pod pogojem, da je predhodno določil območje obsega videonadzora in zaposlene obvestil o videonadzoru oziroma se v primeru videonadzora znotraj delovnih prostorov tudi posvetoval z reprezentativnim sindikatom in svetom delavcev oziroma delavskim zaupnikom. IP pa posebej poudarja, da delodajalec ne sme postaviti kamer v prostorih, kjer je videonadzor izrecno prepovedan. ZVOP-2 kot takšne prostore določa zlasti dvigala, sanitarne prostore in prostore za preoblačenje.

Vprašanje: Ali lahko delodajalec v primeru suma kraje s strani zaposlenih namesti prikriti videonadzor, v smislu, da zaposlene z njim sploh ne seznani?

Odgovor: Zgolj izjemoma, v zelo omejenem obsegu (časovno in prostorsko) in ob upoštevanju strogo določenih pogojev.

ZVOP-2 ureja videonadzor na način, da za njegovo izvajanje sicer ni potrebna izrecna privolitev snemanih, morajo pa biti o njem obveščeni, da lahko prilagodijo svoje vedenje in ravnanje oziroma se lahko v posameznih primerih tudi ognejo prostorom, kjer se takšen videonadzor izvaja (t.i. opt-out). Pravočasna in ustrezna seznanjenost z videonadzorom je zato ključni element njegove zakonitosti in sorazmernosti.

Za odstop od tega pogoja morajo biti zato podani tehtni in prepričljivi razlogi, predvsem pa je to dovoljeno le izjemoma. Kot je izpostavilo Evropsko sodišče za človekove pravice v zadevi KÖPKE proti Nemčiji, glej http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-101536#{"itemid":["001-101536"]}, je takšen nadzor lahko zakonit, če (kumulativni pogoji) obstaja **utemeljen sum storitve kaznivega** dejanja s strani zaposlenega, če tega suma **ni mogoče preveriti drugače** ali vsaj ne brez velikih stroškov, naporov ali porabe časa, **če se nadzor časovno, prostorsko in glede izpostavljenih oseb ustrezno omeji** ter če se nastali posnetki uporabijo **izključno za obravnavo navedenega kaznivega dejanja** (v disciplinskem postopku, morebitnem sledečem sodnem postopku). Skratka, namen prikritega nadzora sme biti le v preiskavi konkretnega in resnejšega incidenta, npr. dlje časa trajajoče evidentne kraje zaposlenih. Delodajalec mora pred odločitvijo za takšen korak preveriti druge možnosti preiskave primera. Priporočljivo je tudi, da izvedbo takšnega videonadzora zaupa zasebnemu detektivu oziroma zunanji varnostni službi.

Vprašanje: Ali lahko kot delodajalec najamem družbo, ki se ukvarja s t.i. skrivnostnimi nakupi, ter ta snema delo zaposlenih?

Odgovor: Ne.

V odnosu delodajalec – delavec je pogosto (če ne celo vedno) delodajalec močnejša stranka. Prav zato je treba striktno upoštevati določila Zakona o delovnih razmerjih (ZDR-1)[12], tudi v delu, ko ta omejuje obdelavo osebnih podatkov zaposlenih. Prvi odstavek 48. člena tako določa, da se osebni podatki delavcev lahko zbirajo, obdelujejo, uporabljajo in dostavljajo tretjim osebam samo, če je to določeno s tem ali drugim zakonom, ali če je to treba

[12] Uradni list RS, št. 21/13, 78/13 – popr., 47/15 – ZZSDT, 33/16 – PZ-F, 52/16, 15/17 – odl. US, 22/19 – ZPosS, 81/19, 203/20 – ZIUPOPDVE, 119/21 – ZČmIS-A, 202/21 – odl. US, 15/22, 54/22 – ZUPŠ-1.

zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem. Določilo prvega odstavka 48. člena ZDR-1 je treba brati skupaj z načelom najmanjšega obsega podatkov (sorazmernosti), ki v točki c) 5. člena Splošne uredbe določa, da morajo biti osebni podatki ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo.

V konkretnem primeru je namen jasen – preverjanje pravilnosti poslovanja zaposlenih ter njihov odnos do kupcev.

Najprej je treba ugotoviti, da gre v konkretnem primeru za videonadzor oseb in ne delovnih prostorov, kot to določa 78. člen ZVOP-2, ki v prvem odstavku 78. člena ZVOP-2 natančno določa, kdaj in pod katerimi pogoji se videonadzor znotraj delovnih prostorov lahko uvede. Predvsem mora obstajati nujnost:

- za varnost ljudi ali premoženja;
- za preprečevanje ali odkrivanje kršitev na področju iger na srečo;
- za varovanje tajnih podatkov;
- za varovanje poslovnih skrivnosti.

Brez večjega napora se da ugotoviti, da nadzor zaposlenih in njihovega dela v okviru prikritih nakupov ni vsebovan v zgoraj naštetih namenih. Zato IP opozarja, da bi kakršnokoli prikrito snemanje pomenilo prekršek po ZVOP-2, lahko pa tudi kaznivo dejanje neupravičenega slikovnega snemanja po 138. členu Kazenskega zakonika (KZ-1)[13].

IP posebej opozarja še na morebitni položaj, ko bi gospodarska družba izvajala takšen videonadzor v obliki pogodbene obdelave. Delodajalec namreč nima pravice izvajati t. i. prikritih nakupov s pomočjo skrivnega snemanja zaposlenih. V skladu z načelom, da nihče ne more na drugega prenesti več pravic, kot jih ima sam, tako tudi delodajalec takšne pravice nima. To torej pomeni, da delodajalec ne more najeti pogodbenega obdelovalca z namenom, da bi ta zanj izvajal prikrite nakupe s pomočjo skrivnega snemanja, saj bi s tem bistveno presegel pravice, ki jih ima sam. S tem pa bi tvegal tudi prekrškovni in sodne postopke.

Vprašanje: Ali je dopustno uporabiti videonadzor na delovnem mestu izključno zaradi kontrole izrabe delovnega časa (za preverjanje, kdaj je delavec prisoten na delovnem mestu)?

Odgovor: Ne.

Takšen videonadzor po mnenju IP ni dopusten, saj pretirano oziroma nesorazmerno posega v zasebnost zaposlenih. Izvajanje videonadzora znotraj delovnih prostorov je namreč z vidika določb 78. člena ZVOP-2 dopustno le v izjemnih primerih, to je takrat, kadar je to nujno treba za varnost ljudi ali premoženja ali preprečevanja ali odkrivanja kršitev na področju iger na srečo ali za varovanje tajnih podatkov ali poslovne skrivnosti, pa teh namenov ni mogoče doseči z milejšimi sredstvi. Navedeno pomeni, da bo moral delodajalec, ki se bo odločil za videonadzor delovnih prostorov, za vsako nameščeno kamero obrazložiti, zakaj je namestitev kamere oziroma izvajanje videonadzora v določenem prostoru nujno potrebna za navedene namene.

[13] Uradni list RS, št. 50/12 – UPB, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20, 95/21, 186/21, 105/22 – ZZNŠPP.

Vprašanje: Ali je zaposlene dovoljeno snemati v raziskovalne namene brez njihovega dovoljenja?

Odgovor: Ne.

Glede na pogoje, ki morajo biti izpolnjeni za zakonito izvajanje videonadzora, sme delodajalec izvajati videonadzor nad zaposlenimi samo v primerih in pod pogoji, ki jih določa ZVOP-2. ''Raziskovalni namen'' je preohlapen in ni določen v zakonu, zato IP ocenjuje, da v primeru, da ob tem nastaja zbirka osebnih podatkov (predvsem da so zaposleni določeni oziroma določljivi), za tovrstno izvajanje video snemanja ni zakonske podlage.

Vprašanje: V šolski avli pred garderobnimi omaricami želimo uvesti videonadzor. Glede na to, da je videonadzor v garderobah prepovedan, v tem primeru pa ne gre za tipično zaprto garderobo, nas zanima, ali lahko pred garderobe, kjer se odlagajo le vrhnja oblačila in obutev, namestimo videonadzor?

Odgovor: Da.

Deseti odstavek 76. člena ZVOP-2 določa, da videonadzora ni dovoljeno izvajati v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih posameznik utemeljeno pričakuje višjo stopnjo zasebnosti.

Ne glede na navedeno, v opisanem primeru ne gre za pojmovanje garderobe v smislu desetega odstavka 76. člena ZVOP-2, kot prostora, ki je namenjen preoblačenju in je ločen od ostalih prostorov, temveč se garderobne omarice nahajajo v šolski avli, vanje pa se odlaga le vrhnja oblačila in obutev. Zaradi tega se ta vrsta garderobe ne opredeljuje kot garderoba, v kateri je po določbah ZVOP-2 prepovedano izvajati videonadzor, kot je to npr. garderoba v sklopu šolske telovadnice, kjer je videonadzor strogo prepovedan. Videonadzor v takšnem primeru se torej lahko izvaja, vendar je treba njegovo izvajanje v celoti uskladiti s pogoji za njegovo zakonito izvajanje.

Posebej je treba upoštevati, da šolska avla lahko predstavlja tudi delovni prostor zaposlenih na šoli. Videonadzor delovnih prostorov se lahko izvaja le skladno z 78. členom ZVOP-2, torej je tako snemanje dovoljeno le, če je to nujno potrebno, kar pomeni, da mora šola vnaprej pretehtati, ali je verjetno, da se bodo tam dogajale tatvine, in šele na podlagi tega uvesti videonadzor.

Vprašanje: ZVOP-2 med drugim zahteva, da se mora delodajalec pred uvedbo videonadzora znotraj delovnih prostorov posvetovati z reprezentativnim sindikatom. To sem kot delodajalec storil, vendar mi je sindikat podal negativno mnenje. Ali lahko videonadzor vseeno vzpostavim?

Odgovor: Da, če so izpolnjeni ostali pogoji iz 78. člena ZVOP-2.

ZVOP-2 v šestem odstavku 78. člena določa, da se mora delodajalec zgolj posvetovati z reprezentativnim sindikatom in svetom delavcem oziroma delavskim zaupnikom, ne zahteva pa njihove privolitve. IP vseeno priporoča, da delodajalci upoštevajo mnenja in razloge sindikata in sveta delavcev oziroma delavskega zaupnika in da se poizkuša najti skupno stališče glede nameravane uvedbe videonadzora.

Vprašanje: Želim uvesti videonadzor delovnih prostorov, vendar v naši družbi ni reprezentativnega sindikata. Kako je z obvezo glede posvetovanja z njim?

Odgovor: Če reprezentativnega sindikata nimate, se vam seveda ni treba posvetovati z njim. V tem primeru obstaja le obveznost posvetovanja s svetom delavcev oziroma delavskim zaupnikom.

Vprašanje: Ali je dovoljeno izvajanje videonadzora v učilnicah pri opravljanju izpitov in pri študiju?

Odgovor: Ne.

Videonadzor učilnic med izvajanjem pouka, študija oziroma izpitov je, zavoljo intenzivnosti in trajnosti posega v zasebnost učencev in zaposlenih, po mnenju IP treba šteti kot obliko videonadzora delovnih prostorov. Posledično je v skladu z določbo prvega odstavka 78. člena ZVOP-2 mogoče videonadzor v učilnicah izvajati le v izjemnih primerih, kadar je to **nujno potrebno** zaradi varnosti ljudi ali premoženja, in teh namenov **ni možno doseči z milejšimi sredstvi**. Navedene pogoje pa bo v učnem okolju, kjer je zagotovljena stalna prisotnost pedagoških delavcev, težko izkazati.

Vprašanje: Ali je dovoljeno izvajanje videonadzora študenta pri opravljanju izpita na daljavo (preko spleta)?

Odgovor: Da, za namen preverjanja identitete.

Ker ne gre za rabo kamer za sistematični nadzor, snemanje opravljanja izpita v tem primeru ne pomeni videonadzora v smislu ZVOP-2, vendar pa vseeno pomeni obdelavo osebnih podatkov v smislu Splošne uredbe in ZVOP-2.

Glede na določbe četrtega odstavka 6. člena ZVOP-2 je v konkretnem primeru dopustno obdelovati videoposnetke študentov za namen preverjanja njihove identitete pri opravljanju izpita. Študent ima obveznosti, ki jih mora opraviti v okviru študija, in nedopustno je, da te obveznosti namesto posameznega študenta opravi kdo drug. Dolžnost oziroma obveznost fakultete pri tem je, da vedno preveri identiteto študenta in zagotovi, da bo izpit dejansko opravljal on in ne nekdo drug namesto njega.

Glede snemanja prostora IP pojasnjuje, da to vprašanje presega pravico do varstva osebnih podatkov in bolj sodi v domet širšega varstva pravic zasebnosti. Vsekakor pa ob primerjavi s tradicionalnimi načini opravljanja izpitov (v prostorih fakultete ob prepovedi pogovarjanja med študenti) lahko zaključimo, da fakulteta v zasebnost študentov ne posega prekomerno, če v času opravljanja izpita zahteva snemanje »prostora, kjer študent opravlja izpit« (torej, če študentu prepusti izbiro prostora, kjer bo opravljal izpit in ki ga bo, posledično, moral posneti).

Da pa bi fakulteti zakonito posredovali osebne podatke oseb, ki vstopijo v prostor med opravljanjem spletnega izpita, je treba pridobiti osebno privolitev vsakega posameznika.

Vprašanje: Ali je dovoljeno postaviti spletno stran, ki bi s pomočjo spletne kamere prikazovala dogajanje v lokalu?

Odgovor: Ne, razen če so bili obiskovalci in zaposleni v lokalu o tem izrecno in nedvoumno obveščeni (npr. z ustreznim napisom na vhodu) in s svojim vstopom v lokal tudi nedvoumno podali privolitev za takšno rabo posnetkov.

V takih primerih je potrebno ločiti videonadzor, ki ga ureja ZVOP-2 in je namenjen varnosti ljudi in premoženja, od snemanja dogajanja v lokalu za druge namene (npr. zaradi zagotavljanja zanimivih vsebin za gledalce, kot je to pri TV ali resničnostnih šovih). V slednjem primeru je že samo bistvo izkušnje v lokalu povezano s tem, da se vse dogajanje tam snema in javno objavlja oziroma izpostavlja. Zaposleni in obiskovalci so s prisotnostjo kamer dobro seznanjeni in ji (očitno) ne nasprotujejo, zatorej ni mogoče govoriti o nesorazmernem posegu v njihovo zasebnost.

V vseh ostalih primerih pa je treba izhajati predvsem iz prvega odstavka 78. člena ZVOP-2, ki strogo zamejuje namen videonadzora na primere, ko je to **nujno potrebno** zaradi varnosti ljudi ali premoženja, in teh namenov **ni možno doseči z milejšimi sredstvi**. Oddajanje posnetkov na internet samo še veča intenzivnost posega, pri čemer pa bo težko utemeljiti, kako se z objavo žive slike prispeva k navedenim namenom. Zato IP opozarja, da bo upravljavec videonadzora v takšnih in temu podobnih primerih izredno težko prestal morebitni inšpekcijski test razlogov za uvedbo videonadzora po ZVOP-2.

Takšna objava posnetkov bo dopustna le, če bodo podani dodatni nameni (kot zgoraj pri televizijskem šovu) in bo hkrati tudi izkazano, da so zaposleni in obiskovalci z njimi nedvoumno seznanjeni oziroma so v obdelavo njihovih osebnih podatkov v te namene tudi privolili.

Vprašanje: Ali lahko videonadzorna kamera na blagajni snema tudi PIN kode?

Odgovor: Ne.

Trgovske družbe nimajo pravice do obdelave PIN kode in je torej ne bi smele imeti v svojih zbirkah osebnih podatkov (konkretno videonadzornih posnetkov), saj je možnost zlorabe velika. Kamere, ki so namenjene varovanju premoženja in verjetno nadzoru dela blagajnikov in blagajničark v rokovanju z gotovino, bi morale torej v skladu z načelom sorazmernosti biti postavljene tako, da ne snemajo terminalov oziroma ozkega področja tipkovnice, v katere kupci vtipkajo svoje PIN kode, ali pa bi bilo treba na te terminale namestiti oviro, ki bi preprečila snemanje kamer na področje vpisa PIN kode.

6. VIDEONADZOR V PREVOZNIH SREDSTVIH, NAMENJENIH JAVNEMU POTNIŠKEMU PROMETU (79. ČLEN ZVOP-2)

Videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, se sme izvajati **le v delih prevoznega sredstva, namenjenih potnikom**, za namen **varnosti potnikov in premoženja**, če tega ni mogoče doseči z drugimi ukrepi, ki manj posegajo v pravice, katerih uresničevanje ureja ZVOP-2. Videonadzor se sme torej izvajati le v omejenem obsegu (le v delih prevoznega sredstva, namenjenih potnikom) in ga ni možno izvajati npr. nad prostorom oziroma sedežem voznika (v takšnem primeru bi šlo za videonadzor njegovega delovnega prostora).

Rok hrambe posnetkov je prav tako omejen, saj mora upravljavec uničiti posnetke najpozneje **v sedmih dneh po njihovem nastanku**. Posnetki se smejo uporabljati za točno določene namene - uveljavljanje ali obrambo pravnih zahtevkov ali za izvrševanje nalog policije (npr. v primerih poškodovanja prevoznega sredstva, vandalizma, kršitev javnega reda in miru ipd.).

7. VIDEONADZOR NA JAVNIH POVRŠINAH (80. ČLEN ZVOP-2)

ZVOP-2 posebej ureja videonadzor na javnih površinah. To področje do njegove uveljavitve ni bilo posebej urejeno.

Videonadzor na javnih površinah, kot jih določa zakon, ki ureja urejanje prostora, je dovoljen le, kadar je to potrebno zaradi obstoja **resne in utemeljene nevarnosti** za življenje, osebno svobodo, telo ali zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca v prenosu in teh namenov ni mogoče doseči z drugimi sredstvi, ki manj posegajo v pravice, katerih uresničevanje ureja ZVOP-2.

Videonadzor na javnih površinah je dovoljen tudi za **namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov**, ki jih varuje policija, Slovenska vojska, pristojni organi za področje varnosti države, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona, in sicer samo v obsegu in trajanju, potrebnem za doseganje namena. Vpogled, uporaba ali posredovanje posnetkov so dopustni le za te namene.

Videonadzor se lahko izvaja le glede tistih bližnjih ali povezanih delov javne površine in v obsegu, kjer je treba varovati zgoraj navedene interese.

Zakon o urejanju prostora (ZUreP-3)[14] v 17. točki prvega dostavka 3. člena določa, da je **javna površina** praviloma odprta prostorska ureditev, namenjena splošni rabi, naravna ali ustvarjena z gradbenimi ali drugimi posegi v prostor, kot so cesta, ulica, pasaža, trg, tržnica, atrij, parkirišče, pokopališče, park, zelenica, otroško igrišče, športno igrišče ter druga površina za rekreacijo in prosti čas; javna površina je grajena ali zelena; javna površina je lahko v lasti države, občine ali v zasebni lasti.

Videonadzor na javnih površinah **lahko izvaja oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost.** Videonadzor smejo za javni sektor izvajati le uradne osebe ali pooblaščeno varnostno osebje, za zasebni sektor pa pooblaščeno varnostno osebje. Osebe ali osebje iz prejšnjega stavka mora biti izrecno pooblaščeno za izvajanje videonadzora.

Videonadzor se lahko izvaja tudi na način, da se ob snemanju izvaja spremljanje dogajanja v živo.

Videonadzor na javnih površinah se za namen varovanja oseb, tajnih podatkov v prenosu, poslovnih skrivnosti ali premoženja večje vrednosti lahko opravlja tudi z uporabo **telesne kamere**, če jo uporablja za to posebej usposobljena oseba. Takšna oseba je lahko npr. ustrezno usposobljen policist, ki varuje varovano osebo.

[14] Uradni list RS, št. 199/21.

Posnetki videonadzora na javnih površinah se lahko hranijo največ **šest mesecev od trenutka nastanka posnetka**. Tudi v primerih videonadzora na javnih površinah je torej določen krajši rok hrambe v primerjavi s splošnim, enoletnim maksimalnim rokom hrambe iz devetega odstavka 76. člena ZVOP-2.

Upravljavec videonadzornega sistema, ki izvaja videonadzor javnih površin, mora v primeru, ko videonadzorni sistem posname dogodek, ki ogroža zdravje ali življenje posameznika, o tem nemudoma obvestiti policijo ali drug pristojni subjekt.

Na področju **videonadzora cestnega prometa** sme upravljavec izvajati videonadzor le na vnaprej določenih odsekih cest v svojem upravljanju, tako da se ne izvaja sistemsko nadzorovanje gibanja posameznikov ali poseganje v zasebnost posameznikov. Upravljavec mora v skladu z zakonom določiti tiste odseke ceste v svojem upravljanju, kjer z drugimi sredstvi ni mogoče doseči nujnega in učinkovitega varovanja cestnega prometa ali njegovega upravljanja.

Upravljavec videonadzornega sistema iz prejšnjega odstavka mora pred dokončno določitvijo lokacij iz prejšnjega odstavka izdelati **oceno učinka, ki vsebuje lokacijo odsekov cest, in jo posredovati v predhodno mnenje IP** (glej 35. in 36. člen Splošne uredbe in 24. člen ZVOP-2).

Na javnih površinah je prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic (ANPR) in sistemov, s katerimi se obdelujejo biometrični osebni podatki. Glede na določbo prvega odstavka 76. člena ZVOP-2 pa takšno obdelavo lahko določi drug zakon (npr. Zakon o cestninjenju[15], ki določa uporabo tehničnih sredstev za samodejno optično prepoznavo registrskih tablic pri opravljanju nadzora nad plačevanjem cestnine).

IP je temo uporabe biometrije in ANPR na javnih površinah, npr. z vidika dopustnosti uporabe bralnikov registrskih tablic pred trgovskimi centri, podrobneje in celovito obdelal v mnenju, ki je dostopno na: https://www.ip-rs.si/mnenja-zvop-2/videonadzor-javnih-površin-1677224569.

Iz tega mnenja izhaja, da se prepoved obdelave osebnih podatkov iz desetega odstavka 80. člena ZVOP-2 lahko nanaša na sisteme za avtomatsko prepoznavo registrskih tablic, ki bi jih upravljavci na javnih površinah uporabljali ob izpolnjevanju pogoja iz c) ali e) prvega odstavka 6. člena Splošne uredbe, ne pa tudi na primere, ko bi uporaba teh sistemov na javnih površinah temeljila na kateri drugi od pravnih podlag iz prvega odstavka 6. člena Splošne uredbe. To pomeni, da so na javnih površinah prepovedani sistemi za avtomatsko prepoznavo registrskih tablic, katerih uporaba bi bila potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca ali za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti upravljavca. Take sisteme pa je na javnih površinah dovoljeno uporabljati, če upravljavec izkaže, da za to obstaja katere od drugih pravnih podlag iz prvega odstavka 6. člena Splošne uredbe. Po mnenju IP bi glede na dejstvo, da gre za uporabo sistemov na javnih površinah in glede na naravo takih površin ter tudi naravo samega sistema avtomatske prepoznave registrskih tablic v praksi kot pravna podlaga, na kateri bi lahko temeljila uporaba takih sistemov, lahko prišla v poštev (zgolj) pravna podlaga iz točke f) prvega odstavka 6. člena Splošne uredbe in bi bila njihova uporaba lahko zakonita pod pogojem, da bi bil upravljavec zmožen dokazati, da je obdelava osebnih podatkov na tak način potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika.

[15] Uradni list RS, št. 24/15, 41/17, 158/20, 159/21.

8. DRUGE OBLIKE VIDEONADZORA

Napredek tehnike na področju video kamer in snemalnikov je povzročil izjemen porast videonadzora. To pomeni, da obstajajo tudi take oblike videonadzora, ki jih ni mogoče izrecno uvrstiti h kateremu od členov 77-80 ZVOP-2 in jih je zato treba obravnavati po splošnih določbah ZVOP-2 o videonadzoru (76. člen) oziroma nasploh po določbah Splošne uredbe in ZVOP-2. Prav tako obstajajo številne uporabe video kamer, ki jih, predvsem zavoljo občasne in namenske rabe, sploh ni mogoče šteti za videonadzor, imajo pa še vedno pomemben vpliv na zasebnost posameznikov, ki so jim izpostavljeni.

Prav tako je, zlasti zavoljo cenovne dostopnosti tovrstnih naprav, prišlo do porasta zasebnega videonadzora na stanovanjskih objektih, v avtomobilih in drugih prevoznih sredstvih, ter na osebi posameznika. V teh primerih je snemanje izvzeto iz ureditve po ZVOP-2 pod pogoji iz drugega odstavka 3. člena ZVOP-2, torej, če jih posamezniki izvajajo med potekom popolnoma **osebne ali domače dejavnosti**. Ta izjema ne velja, če gre za snemanje javno dostopnih površin ali javno objavo oziroma drugo posredovanje teh posnetkov izven zasebnega kroga posameznikov.

8.1 Odgovori na pogosta vprašanja

Vprašanje: Videonadzor izvajam doma in snemam zgolj svojo posest. Moram objaviti obvestilo?

Odgovor: Ne, če res snemate zgolj svojo posest.

Drugi odstavek 3. člena ZVOP-2 določa, da določbe tega zakona (torej ZVOP-2) ne veljajo za obdelave osebnih podatkov, ki jih izvajajo posamezniki med potekom popolnoma osebne ali domače dejavnosti.

V primeru, ko gre samo za nadzor nad posestjo posameznika (npr. stanovanjsko hišo, gospodarskim poslopjem in zasebno parcelo), IP ne vidi razlogov, da bi takšnemu izvajalcu videonadzor preprečevali oziroma prepovedovali uvedbo videonadzora. Kamere pa nikakor ne smejo biti usmerjene na del dvorišča, kjer se gibljejo tudi drugi oziroma po katerem ima služnost za prevoz tudi sosed, ali na javne površine.

IP ob tem poudarja, da kljub dejstvu, da takšnih primerov ZVOP-2 ne ureja, ne pomeni, da posameznik nima možnosti pravnega varstva, če meni, da mu je bila zaradi izvajanja videonadzora kršena njegova pravica do zasebnosti. Če izvajalec videonadzora v takem primeru brez dovoljenja in vednosti snema tudi druge ljudi na zemljišču izven meja svojih nepremičnin, je za svoja dejanja lahko civilno in kazensko odgovoren. Posameznik, katerega pravica do zasebnosti je kratena, pa lahko v skladu s 134. členom Obligacijskega zakonika (OZ)[16] vloži tožbo na sodišče, s katero sodišču predlaga, da odredi prenehanje dejanja (videonadzora), s katerim se krši nedotakljivost človekove osebnosti, osebnega in družinskega življenja ali kakšna druga osebnostna pravica. Poleg tega lahko posameznik, če ocenjuje, da mu je bila s posegom v zasebnost povzročena premoženjska ali nepremoženjska škoda, na podlagi 179. člena OZ zahteva tudi denarno odškodnino.

[16] Uradni list RS, št. 97/07 - UPB1, 64/16 – odl. US, 20/18 – OROZ631.

Vprašanje: Kaj pa, če s kamero, nameščeno na hiši, snemam tudi sosednja zemljišča ali javne površine?

Odgovor: Takšen videonadzor praviloma ne bo dovoljen.

Tujega zasebnega zemljišča ni dovoljeno snemati brez privolitve lastnika tega zemljišča.

Pri snemanju javnega zemljišča je treba upoštevati ureditev glede snemanja javnih površin ter prakso Sodišča EU, po kateri uporabe kamere, ki jo je fizična oseba namestila na družinsko hišo zaradi varovanja premoženja, zdravja in življenja lastnikov hiše, pri tem pa nesorazmerno nadzira tudi javni prostor, ni več mogoče šteti za izključno osebno uporabo[17].

Če torej upravljavec brez dovoljenja in njihove vednosti snema tudi druge ljudi na zemljišču izven meja svojih nepremičnin, je lahko za svoja dejanja odgovoren odškodninsko in kazensko. Prizadeti posamezniki lahko namreč po 134. členu OZ vložijo tožbo na sodišče, ki lahko odredi prenehanje dejanja (videonadzora), s katerim se krši nedotakljivost človekove osebnosti, osebnega in družinskega življenja ali kakšna druga osebnostna pravica. Prav tako lahko po splošnih pravilih o odškodninski odgovornosti od izvajalca videonadzora zahtevajo odškodnino. V hujših primerih lahko takšno samovoljno snemanje predstavlja tudi kaznivo dejanje po 138. členu KZ-1, ki določa, da se, kdor neupravičeno slikovno snema ali naredi slikovni posnetek drugega ali njegovih prostorov brez njegove privolitve in s tem občutno poseže v njegovo zasebnost, kaznuje z denarno kaznijo ali z zaporom do enega leta.

Vprašanje: Kakšni so pogoji za videonadzor javnih površin? Kako je npr. z videonadzorom semaforiziranih križišč, ekoloških otokov ipd.?

Odgovor: Videonadzor na javnih površinah ZVOP-2 posebej ureja v 80. členu, kjer so v prvem odstavku določeni izjemni primeri, v katerih se ga lahko izvaja. Dovoljen je le, kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca v prenosu in teh namenov ni mogoče doseči z drugimi sredstvi, ki manj posegajo v pravice, katerih uresničevanje ureja ZVOP-2.

Pred izvajanjem videonadzora javnih površin je torej treba pretehtati, ali je njegova uvedba res potrebna za dosego navedenih namenov in ali teh namenov ni mogoče doseči s sredstvi, ki manj posegajo v pravice, katerih uresničevanje ureja ZVOP-2.

Opraviti je treba test sorazmernosti. To pomeni, da je treba pred uvedbo videonadzora oceniti stopnjo nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, za premoženje ali za tajne podatke v prenosu, ki jih je treba varovati z videonadzorom, ter verjetnost (glede na pretekle izkušnje), da bo prišlo do poškodovanja ali odtujitve tega premoženja. Informacijski pooblaščenec dodaja, da bi bil, glede na navedeno, zakonit namen, zaradi katerega bi se lahko pregledovali posnetki (npr. v primeru ekoloških otokov), ki bi nastali z izvajanjem videonadzora javnih površin, zagotavljanje varnosti ljudi in varovanje premoženja. Izvajalec videonadzora bi lahko torej posnetke pregledoval v primeru, ko bi prišlo do poškodovanja ali odtujitve njegovega premoženja

[17] Glej sodbo Sodišče EU v zadevi C-212/13, František Ryneš proti Úřad pro ochranu osobních údajů, http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=SL&mode=lst&dir=&occ=first&part=1&cid=281763

oziroma zgolj ob nekem deviantnem dogodku, ko bi bil videoposnetek le dodaten dokaz v prekrškovnem ali kazenskem postopku. Videonadzor ekoloških otokov pa ni dopusten z namenom odkrivanja in dokazovanja prekrškov v zvezi z napačnim odlaganjem odpadkov. Podobno ni dopustno npr. s strani občinskega redarstva postavljati ali izrabljati videonadzor za namen ugotavljanja kršitev in sankcioniranja oseb, ki napačno parkirajo.

Vprašanje: Kakšni so pogoji za vzpostavitev videonadzora v večstanovanjski stavbi?

ZVOP-2 ne vsebuje posebnih določb glede videonadzora večstanovanjskih stavb, zato je pri izvajanju videonadzora treba zadostiti zahtevam iz 6. in 13. člena Splošne uredbe ter 76. člena ZVOP-2, glede zavarovanja videonadzornega sistema pa zahtevam iz 24. in 32. člena Splošne uredbe ter 22. člena ZVOP-2.

Ustrezna pravna podlaga za izvajanje videonadzora bi lahko izhajala iz točke (f) prvega odstavka 6. člena Splošne uredbe, če in v obsegu, v katerem so za to izpolnjeni pogoji. Izvajanje videonadzora bi torej lahko bilo dopustno, če je takšna obdelava osebnih podatkov potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba in če nad takimi interesi ne prevladajo interesi ali temeljne pravice in svoboščine posameznika, ki bi lahko bil na posnetkih. Upravljavec mora pred uvedbo videonadzora na tej pravni podlagi izvesti zgoraj omenjeni test tehtanja (glej zgoraj). Upravljavec videonadzora je dolžan ne glede na pravno podlago, na temelju katere obdeluje osebne podatke, v skladu s 13. členom Splošne uredbe o varstvu podatkov posameznikom na jasen in pregleden način zagotoviti osnovne informacije v zvezi z obdelavo osebnih podatkov ter informacije navedene v četrtem odstavku 76. člena ZVOP-2.

V skladu s 25. členom SZ-1 je za posle rednega upravljanja (mednje po mnenju IP sodi tudi izvajanje videonadzora) večstanovanjske stavbe potrebno soglasje solastnikov, ki imajo več kot polovico solastniških deležev glede na večstanovanjsko stavbo.

Vprašanje: Kakšni so pogoji za postavitev panoramske kamere?

Odgovor: Če je kamera postavljena tako, da posamezniki na posnetku niso določljivi (npr. so posneti tako od daleč, da se obraza ne vidi, kot so npr. panoramske, turistične in vremenske kamere), ne gre za videonadzor v smislu ZVOP-2 in torej tudi obvestilo o izvajanju snemanja ni potrebno.

Vprašanje: Ali uporaba ročne oziroma naglavne kamere šteje za videonadzor?

Odgovor: Ne, ker ne gre za sistematični nadzor, vendar pa to ne pomeni, da je nadzor upravičen.

Še vedno gre lahko pri takem snemanju za poseg v osebnostne pravice tretjih ali celo za kaznivo dejanje, zato IP priporoča, da se takšno snemanje omeji na pogoje zasebne uporabe, posameznike, ki bi se lahko znašli na posnetku, pa je koristno vedno vnaprej prositi za dovoljenje.

Vprašanje: Ali se uporaba video kamere, ki je vgrajena v avtomobil za zagotavljanje pomoči pri parkiranju, šteje za videonadzor?

Odgovor: Ne, ker načeloma ne gre za sistematični nadzor. Pri tem pa je treba paziti, da je kamera izdelana ali prilagojena tako, da ne zbira informacij v zvezi s fizično osebo (kot so registrske tablice ali informacije, ki bi se lahko uporabile za identifikacijo mimoidočih). V nasprotnem primeru gre lahko za poseg v osebnostne pravice tretjih ali celo za kaznivo dejanje.

Vprašanje: Zanimajo nas napredne oblike video sistemov, ki omogočajo zaznavanje čakalnih vrst, prepoznavo spola in starosti obiskovalcev in podobno. Ali tudi to sodi v videonadzor?

Odgovor: V primeru aplikacij t.i. inteligentne video analitike, ki se lahko namesti na obstoječe videonadzorne sisteme, uporablja samostojno ali v povsem novih namestitvah video nadzornih sistemov, vam predlagamo, da si podrobno preberete Smernice glede inteligentne video analitike, ki jih najdete na tej povezavi:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_inteligentna_video_analitika.pdf

9. ZAVAROVANJE VIDEONADZORNEGA SISTEMA

Oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, mora skladno z določbami 24. in 32. člena Splošne uredbe zagotoviti, da je videonadzorni sistem ustrezno zavarovan.

Upravljavec, ki izvaja videonadzor, mora skladno z določbami 24. člena Splošne uredbe ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, izvesti ustrezne tehnične in organizacijske ukrepe, da zagotovi in je zmožen dokazati, da obdelava poteka v skladu s Splošno uredbo.

Skladno z določbami 32. člena Splošne uredbe mora ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotoviti ustrezno raven varnosti glede na tveganja. Vpogled, uporaba ali posredovanje posnetkov videonadzornega sistema so dopustni samo za namene, ki so zakonito obstajali ali bili navedeni na obvestilu v času zajema posnetka.

Po določbah 76. člena ZVOP-2 mora upravljavec videonadzornega sistema zagotoviti t.i. sledljivost obdelave – možnost naknadnega ugotavljanja, kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi. Te podatke hrani v dnevniku obdelave iz 22. člena ZVOP-2 dve leti po koncu leta, v katerem so nastali (če so npr. nastali tekom leta 2023, jih hrani do konca leta 2025).

9.1 Odgovori na pogosta vprašanja

Vprašanje: Kako mora biti videonadzorni sistem zavarovan, da bo v skladu s Splošno uredbo?

Odgovor: IP poudarja, da za zavarovanje sistema videonadzora, kakor tudi za zavarovanje posnetkov, veljajo enaka pravila kot za zavarovanje osebnih podatkov na splošno. Zavarovanje urejata 24. in 32. člen Splošne uredbe, ob pogodbeni obdelavi tudi 28. člen Splošne uredbe.

Pri tem IP priporoča predvsem sledeče ukrepe:

- dostop do prostorov, kjer se hranijo posnetki oziroma kjer je mogoče pregledovati posnetke, naj bo ustrezno fizično in logično zavarovan ter dostopen zgolj pooblaščenim osebam upravljavca oziroma pogodbenega izvajalca videonadzora (npr. varnostne službe);
- zasloni naj bodo nameščeni tako, da jih lahko vidijo samo pooblaščene osebe;
- če je mogoče, naj se dostop do posnetkov vrši čez programski vmesnik in ne neposredno; pri tem naj se vsakemu uporabniku dodeli ločen uporabniški račun na podlagi ustrezne politike gesel; uporabniki se morajo po zaključku dela;
- vsak dostop do posnetkov naj se evidentira (kateri posnetki, kdo, kdaj, za kakšen namen);
- opredelijo in izvajajo naj se postopki za odobritev, spremembo in preklic fizičnega in logičnega dostopa;
- pri nadgradnji obstoječega vmesnika naj se stremi k odpravi morebitnih pomanjkljivosti z navedenega seznama;
- vsi ukrepi naj se redno in sistematično pregledujejo in evidentirajo.

IP pa posebej odsvetuje:

- možnost neposrednega dostopa do surovih posnetkov oziroma do neomejenega kopiranja posnetkov;
- uporabo istega gesla za vse pooblaščene osebe;
- uporabo skupinskih uporabniških men (npr. »popoldanska izmena«).

Vprašanje: Ali moramo voditi evidenco uporabe videoposnetkov in ali obstajajo kakšna priporočila glede tega?

Odgovor: Da.

Kot pri drugih zbirkah osebnih podatkov velja, da mora biti zagotovljena sledljivost obdelave osebnih podatkov, torej mora obstajati **evidenca dostopov do osebnih podatkov (posnetkov)**. Zagotovljena mora biti možnost naknadnega ugotavljanja, kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi (12. odstavek 76. člena ZVOP-2). Priporočljivo je, da tovrstna evidenca vsebuje naslednje podatke glede posameznega dostopa (vpogleda, posredovanja ipd.): zaporedno številko vpogleda ali iznosa, ime in priimek osebe, ki je dostopala do posnetkov, datum dostopa, namen dostopa, podatki o časovnem obdobju pridobljenih posnetkov (od-do), podatki o tem, komu, kdaj in s kakšnim namenom ali na kateri pravni podlagi so se posredovali, medij, na katerem so bili posnetki posredovani (CD, USB ključ ipd.), morebitne opombe in podpis pooblaščene osebe. Podatke o dostopu mora upravljavec videonadzornega sistema hraniti dve leti po koncu leta, ko so nastali.

Neprimerna je praksa, ko varnostniki, ki s pomočjo videonadzora nadzirajo dogajanje, v tovrstno evidenco navedejo zgolj čas prihoda na delovno mesto in čas odhoda z delovnega mesta. Ne gre namreč za evidenco njihovega delovnega časa, temveč je evidenca namenjena temu, da se da naknadno ugotoviti, kateri posnetki so bili obdelani, s kakšnim namenom ter kdo in kdaj je posnetke pregledoval ali drugače uporabljal.

Vzorčni (neobvezni) primer dnevnika obdelave oz. manipulacije z videoposnetki je na voljo na povezavi: https://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/ZVOP/EVIDENCA_UPORABE_VIDEONADZORNEGA_SISTEMA.doc.

Vprašanje: Kdaj lahko nastale posnetke ali njihove izseke posredujem tretjim osebam?

Odgovor: Nastale posnetke je tretjim osebam (zlasti pravosodnim organom, novinarjem, raziskovalcem) dopustno posredovati le, če izkažejo ustrezno pravno podlago v skladu s 6. členom ZVOP-2. Pri tem je treba skladno z zahtevami šestega odstavka 41. člena ZVOP-2 zagotoviti možnost poznejše ugotovitve, kateri osebni podatki (posnetki) so bili posredovani, komu, kdaj in na kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če drug zakon za posredovanje posameznih vrst podatkov določa drugače oziroma je to razvidno iz dnevnika obdelave po 22. členu ZVOP-2.

V dvomu IP predlaga, da se posnetek ustrezno anonimizira, če je to le mogoče. To pomeni, da se npr. pri posredovanju posnetkov prometnih nesreč prekrije registrske tablice, obraze in podobno.

10. ZAKLJUČEK

Videonadzor je v moderni družbi ena od ključnih tehnologij za zagotavljanje varnosti tako v javnem kot tudi zasebnem sektorju. Zavoljo vse večje cenovne dostopnosti in učinkovitosti je kljub svojemu že več desetletnemu staležu še vedno v porastu. Posledično smo kot družba videonadzornih kamer že dodobra navajeni, pravzaprav tako zelo, da se pogosto sploh več ne zavedamo njihovega obstoja. A vendar je, kot pri vsaki drugi tehnologiji, ki temelji na obdelavi osebnih podatkov, zelo pomembno, da je njena uporaba izvedena na način, ki upošteva tudi koncepte zasebnosti.

Zakonitih in legitimnih ciljev namreč ni mogoče doseči zgolj »na račun zasebnosti«, temveč tako, da jo s pravočasnim premislekom in ukrepi ohranimo; pri tem morajo biti večja tveganja povezana z večjimi varovalkami.

ZVOP-2 in drugi področni zakoni zato določajo pogoje, pod katerimi je dovoljeno vzpostaviti in izvajati videonadzor. Na delovnem mestu je to predvsem jasno izražena zakonita potreba delodajalca, ob pogoju, da istega cilja ne more doseči na manj invaziven način. V večstanovanjskih stavbah je to soglasje večine vseh stanovalcev, v želji živeti v urejenem in varnem bivanjskem okolju. Pri zasebnem videonadzoru pa je to samoomejevanje pri takšni rabi, ki bi pretirano posegla v interese drugih posameznikov oziroma javnosti.