PAM Pokrajinski arhiv Maribor

Moderna arhivistika

Časopis arhivske teorije in prakse
Journal of Archival Theory and Practice

Letnik 2 (2019), št. 1 / Year 2 (2019), No. 1

Maribor, 2019

Moderna arhivistika

Časopis arhivske teorije in prakse

Journal of Archival Theory and Practice

Letnik 2 (2019), št. 1 / Year 2 (2019), No. 1

ISSN 2591-0884 (online)
ISSN 2591-0876 (CD_ROM)

Izdaja / Published by:
Pokrajinski arhiv Maribor / Regional Archives Maribor

Glavni in odgovorni urednik / Chief and Responsible editor:
Ivan Fras, prof., Pokrajinski arhiv Maribor, Glavni trg 7, SI-2000 Maribor,
telefon/ Phone: +386 2228 5017; e-pošta/e-mail: ivan.fras@pokarh-mb.si

Glavna urednica / Editor in chief:
mag. Nina Gostenčnik

Recenziranje / Peer review process:
Prispevki so recenzirani. Za objavo je potrebna pozitivna recenzija. Proces recenziranja je anonimen. / All articles for publication in the conference proceedings are peer-reviewed. A positive review is needed for publication. The review process is anonymous.

Lektoriranje / Proof-reading:
mag. Boštjan Zajšek, mag. Nina Gostenčnik

Prevajanje:
mag. Boštjan Zajšek (slovenščina), mag. Nina Gostenčnik (slovenščina, angleščina), Lučka Mlinarič (bosanščina, hrvaščina, srbščina)

Oblikovanje in prelom / Design and typesetting:
mag. Nina Gostenčnik

http://www.pokarh-mb.si/si/p/3/49/moderna-arhivistika.html

Prejeto / Received: 20. 1. 2019

1.01 Izvirni znanstveni članek *1.01 Scientific Article*

SPLOŠNA UREDBA O VARSTVU PODATKOV IN UPORABA VIDEONADZORA ZA VAROVANJE KRITIČNE INFRASTRUKTURE

mag. Marko POTOKAR
Fakulteta za informacijske študije,
Novo mesto, Slovenija
marko.potokar@ifit.si

Danilo BURNAČ
Mariborski vodovod, j.p., d.d.,
Maribor, Slovenija
danilo.burnac@mb-vodovod.si

Sanja ANDROIĆ
Mariborski vodovod, j.p., d.d.,
Maribor, Slovenija
sanja.androic@mb-vodovod.si

dr. Milka PUNGARTNIK
Mariborski vodovod, j.p.,d.d.,
Maribor, Slovenija
milka.pungartnik@mb-vodovod.si

Izvleček:

S 25. majem 2018 je v veljavo stopila nova evropska uredba o varstvu osebnih podatkov (Splošna uredba o varstvu podatkov, angl.: GDPR), ki dviguje nivo varovanja zasebnosti posameznikov in hkrati bolj zavezuje upravljavce in obdelovalce osebnih podatkov. Upravljavci bodo dolžni poskrbeti za strožje varnostne kontrole pred in med obdelavo osebnih podatkov. Zadostiti bodo morali načelu vgrajenega in privzetega varstva osebnih podatkov. Dodano je tudi načelo odgovornosti, ki od upravljavcev osebnih podatkov zraven ustreznega zavarovanja terja tudi zmožnost dokazovanja skladnosti s Splošno uredbo. Upravljavci bodo morali preveriti ustreznost že pridobljenih privolitev in razmisliti o morebitni določitvi pooblaščene osebe za varovanje osebnih podatkov. Novost so tudi določila Splošne uredbe, ki od obdelovalcev zahtevajo višji standard pri obdelavi osebnih podatkov. Tudi ti bodo po novem dolžni voditi evidenco obdelav, zagotoviti bodo morali zadostna jamstva za tehnične in organizacijske ukrepe, v primeru zaposlitve dodatnih obdelovalcev pa bodo morali pridobiti soglasje upravljavca. Enake pa zaenkrat ostajajo določbe področnih ureditev, med drugim tudi videonadzora, v kolikor niso v nasprotju s katero od določb Splošne uredbe.

V prispevku bomo na primeru podjetja Mariborski vodovod prikazali, kako vzpostaviti zakonsko skladen videonadzor vodooskrbnih objektov in naprav, ki so eden izmed bistvenih delov kritične infrastrukture. Podjetje je največji enovit vodooskrbni sistem ter regionalni vodovod v Sloveniji in z izvajanjem javne službe distribucije vode predstavlja enega izmed najpomembnejših deležnikov kritične infrastrukture.

Ključne besede:

Splošna uredba o varstvu podatkov, videonadzor, kritična infrastruktura, varovanje, upravljavci, obdelovalci

Abstract:

General Data Protection Regulation and Use of Video Surveillance to Protect Critical Infrastructure

On 25 May 2018, a new European regulation on the protection of personal data (the General Data Protection Regulation (GDPR)), which raises the level of protection of individuals' privacy came into force. GDPR is more binding on the controllers and processors of personal data. Controllers will be obliged to provide stricter security controls before and when processing personal data. They will have to satisfy the principle of embedded and default protection of personal data. The principle of liability is also added, which also requires, among eligible data controllers, the appropriate insurance, the ability to demonstrate compliance with the General Regulation. Controllers will have to verify the appropriateness of the consent already obtained and consider the possible identification of an authorized person for the protection of personal data. New features are also the provisions of the General Regulation, which require a higher standard in the processing of personal data from processors. They will also be obliged to keep track of the processing, they will have to provide sufficient guarantees for the provision of technical and organizational measures, and in the case of additional processors, they will need to obtain the consent of the controller. However, for the time being, the provisions of sectoral arrangements remain, including video surveillance, insofar as they do not conflict with any of the provisions of the General Regulation.

In the article we will show how to establish a legally compliant video surveillance of water supply facilities and devices in Mariborski vodovod, which is one of the essential parts of the critical infrastructure. The company is the largest unified water supply system and regional water supplier in Slovenia, and with the implementation of the public water distribution service is one of the most important stakeholders in critical infrastructure.

Key words:

General Data Protection Regulation, Video Surveillance, Critical Infrastructure, Security, Controllers, Processors

1. SPLOŠNA UREDBA O VARSTVU PODATKOV IN ZAKON O VARSTVU OSEBNIH PODATKOV

S 25. majem 2018 je v veljavo stopila nova evropska uredba o varstvu osebnih podatkov (Splošna uredba o varstvu podatkov, angl.: Regulation (EU) 2016/679 of the European parliament and of the council - GDPR, 2016), ki dviguje nivo varovanja zasebnosti posameznikov in hkrati bolj zavezuje upravljavce in obdelovalce osebnih podatkov. Splošna uredba predstavlja prvo večjo prenovo evropskega zakonodajnega okvira za varstvo osebnih podatkov in je nastala z namenom zagotavljanja pravice do zasebnosti v dobi hitrega tehnološkega razvoja in pospešene digitalizacije, v kateri je obdelava osebnih podatkov postala vseprisotna, hitra in globalna. Splošna uredba vpeljuje nekatere novejše pristope in elemente, med katere sodijo ocene učinkov na zasebnost, privzeto in vgrajeno varstvo osebnih podatkov, pooblaščene osebe za varstvo osebnih podatkov ter obveščanje o varnostnih incidentih in kodeksi ravnanja. Ne glede na novosti pa varstvo osebnih podatkov še vedno temelji na osnovnih načelih, ki so:

- zakonitost, pravičnost in preglednost;
- omejitev namena;
- najmanjši obseg podatkov;
- točnost;
- omejitev shranjevanja;
- celovitost in zaupnost;

- odgovornost.

Klasičnim načelom je dodano načelo odgovornosti oziroma odgovornega upravljanja (angl. accountability), ki zavezuje upravljavca, da mora biti skladnost z navedenimi načeli tudi zmožen dokazati. Upravljavci so dolžni poskrbeti za strožje varnostne kontrole pred in med obdelavo osebnih podatkov. Zadostiti morajo načelu vgrajenega in privzetega varstva osebnih podatkov. Upravljavci morajo tudi preveriti ustreznost že pridobljenih privolitev in razmisliti o morebitni določitvi pooblaščene osebe za varovanje osebnih podatkov. Novost so tudi določila Splošne uredbe, ki zahtevajo višji standard pri obdelavi osebnih podatkov od obdelovalcev. Tudi ti so po novem dolžni voditi evidenco obdelav, zagotoviti morajo zadostna jamstva za tehnične in organizacijske ukrepe, v primeru zaposlitve dodatnih obdelovalcev pa bodo morali pridobiti soglasje upravljavca. Splošna uredba daje poseben poudarek tudi zavarovanju osebnih podatkov, in tako med drugim poudarja varnostni kontroli psevdonimizacijo in šifriranje osebnih podatkov. Varnostni ukrepi naj bi upoštevali najnovejši tehnološki razvoj, stroške izvajanja, naravo, obseg, okoliščine in namen obdelave pa tudi tveganja za pravice in svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti. Upravljavci in obdelovalci naj bi z izvajanjem ustreznih tehničnih in organizacijskih ukrepov zagotovili ustrezno raven varnosti, in to predvsem z naslednjimi ukrepi:

- zagotovitev zaupnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev za obdelavo podatkov;
- psevdonimizacija in šifriranje osebnih podatkov;
- zmožnost pravočasne povrnitve razpoložljivosti in dostopa do osebnih podatkov v primeru fizičnega ali tehničnega incidenta;
- postopek rednega testiranja, ocenjevanja in vrednotenja učinkovitosti, tehničnih in organizacijskih ukrepov za zagotavljanje varnosti obdelave.

Veljavna Splošna uredba, katere namen je med drugim tudi harmonizacija na področju obveznosti upravljavcev ter v nadzorni praksi in pristojnosti nadzornih organov, pa dopušča tudi implementacijo nekaterih določb v nacionalni zakonodaji. Tako je bil s strani Ministrstva za pravosodje pripravljen osnutek Zakona o varstvu osebnih podatkov (ZVOP-2), ki pa v tem trenutku še ni sprejet. Tako do sprejema novega zakona ostajajo v veljavi tiste določbe ZVOP-1, ki niso v neposrednem nasprotju s Splošno uredbo, npr. določbe področnih ureditev, med katere sodijo določbe o neposrednem trženju, biometriji, evidenci vstopov in izstopov iz prostorov ter določbe o izvajanju videonadzora. To pomeni, da je do sprejema ZVOP-2 potrebno upoštevati tako Splošno uredbo kot (večji) del ZVOP-1.

2. UPORABA VIDEONADZORA V SLOVENSKIH PODJETJIH

Ker videonadzor v Splošni uredbi ni eksplicitno obravnavan, zanj veljajo določbe ZVOP-1. Za videonadzor se šteje uporaba videokamer za sistematično snemanje, prenos in shranjevanje žive slike z ene lokacije na drugo predvsem za namene zagotavljanja varnosti. Tudi t. i. »podaljšano oko«, rešitev, ki zajema zgolj prenos žive slike brez snemanja, se šteje kot videonadzor. Videonadzor je v ZVOP-1 uravnavan v členih 74 do 77. Tako je v 74. členu določeno, da mora oseba javnega ali zasebnega sektorja objaviti obvestilo v primeru izvajanja videonadzora, ki mora biti vidno in razločno objavljeno na način, da se posameznik seznani s izvajanjem videonadzora najkasneje, ko se le-ta začne izvajati. Obvestilo mora vsebovati naslednje informacije:

»1. da se izvaja videonadzor;

2. naziv osebe javnega ali zasebnega sektorja, ki ga izvaja;

3. telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema.« (Informacijski pooblaščenec, 2015).

Z razvojem videonadzorne opreme in obenem tudi lažjo cenovno dostopnostjo se je posledično uporaba videonadzora v podjetjih povečala. Podjetja videonadzorne naprave postavljajo večinoma za nadzor dostopa v poslovne prostore, izjemoma pa tudi za nadzor samih poslovnih prostorov, kjer delajo zaposleni. Videonadzor dostopa v službene prostore se lahko uporablja za varnost ljudi ali varnost premoženja ali zagotavljanja nadzora vstopa ali izstopa v poslovne prostore oziroma iz njih ali če obstaja možnost ogroženosti zaposlenih zaradi njihove narave dela (Zakon o varstvu osebnih podatkov, 2007).

V raziskavi Potokar M. in Androič S. (2014), ki je bila izvedena v letu 2013 na vzorcu 166 slovenskih podjetij, je razvidno, da visok, 78-odstotni delež slovenskih podjetij uporablja videonadzor. Glede na hiter tehnološki razvoj, nižje cene zaradi večje konkurence na trgu in sprememb zakonodaje predvidevamo, da je ta odstotek podjetij danes že višji, najverjetneje v kombinaciji s še kakšno drugo tehnično rešitvijo nadzora.

Raziskava iz leta 2013 (Potokar in Androič, 2014) nam kaže tudi naslednje zanimive ugotovitve:

- reprezentativni vzorec je pokazal, da so vlomi v poslovne prostore podjetja zaenkrat redki;
- večina slovenskih podjetij uporablja videonadzor samo za varovanje, se pa že vidi prihajajoč razvoj, ki povezuje videonadzor z drugimi varnostnimi rešitvami za nadzor poslovnih procesov;
- uporaba videonadzora odvrača morebitne storilce od nedovoljenih in zlonamernih dejanj, kar povečuje število rešenih varnostnih incidentov;
- zaposleni videonadzor občasno dojemajo kot vdor v zasebnost in se posledično obnašajo bolj previdno;
- uporaba videonadzora povečuje občutek varnosti zaposlenih in obiskovalcev oziroma strank;
- v času raziskave je imela slaba večina slovenskih podjetij predpisano varnostno politiko ali kakršnakoli navodila o upravljanju in uporabi videonadzora.

Na podlagi ugotovitev prej omenjene raziskave domnevamo, da bo zaradi tehnološkega razvoja vedno več podjetij uporabljalo videonadzor in ga povezovalo z drugimi varnostnimi rešitvami, ki jih je vedno več na voljo na trgu. Zaradi spremembe zakonodaje na področju varstva podatkov pa predvidevamo, da bo občutek varnosti na področju zasebnosti zaposlenih višji in da bo še več podjetij uredilo interne pravne akte, predvsem pravilnike o videonadzoru in zakonsko skladne pogodbe o obdelavi osebnih podatkov, ki nastajajo tudi na področju videonadzora. Zato bo tudi več strokovno odgovornih oseb za to področje ali več povezanih področij, kot je npr. varstvo osebnih podatkov. Pričakovati je, da bodo odgovorne osebe za varstvo osebnih podatkov (t. i. DPO) prevzele tudi področje videonadzora.

3. UPORABA VIDEONADZORA IN VAROVANJE KRITIČNE INFRASTRUKTURE

Pojem kritične infrastrukture je v slovenski zakonodaji določen v Zakonu o kritični infrastrukturi (ZKI, 2017), ki v 3. odstavku 4. člena določa, da »*/k/ritična infrastruktura obsega tiste zmogljivosti in storitve, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne 22 posledice na nacionalno varnost, gospodarstvo, ključne družbene funkcije, zdravje, varnost in zaščito ter družbeno blaginjo*. « Posredna definicija se pojavlja v poglavju VIII Zakona o zasebnem varovanju (ZzasV-1, 2011), ki določa obvezno organiziranje varovanja, in sicer v 69. členu, kjer je v 1. odstavku določeno, da vlada na predlog ministrstva, pristojnega za posamezno področje, s sklepom določi gospodarske družbe, samostojne podjetnike posameznike, zavode, državne organe, javne agencije, organizacije ter druge pravne in fizične osebe (v nadaljnjem besedilu: zavezanci), ki morajo organizirati varovanje, po potrebi pa tudi konkretne varnostne ukrepe, če:

- *»uporabljajo ali hranijo radioaktivne snovi, jedrska goriva, odpadke in druge ljudem in okolju nevarne snovi in naprave;*
- *upravljajo zmogljivosti, sisteme ali njihove dele, ki so bistveni za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi ter katerih okvara ali uničenje bi imela resne posledice na nacionalno varnost Republike Slovenije zaradi nezmožnosti vzdrževanja teh funkcij (promet, energija, telekomunikacije);*
- *hranijo arhivsko gradivo in predmete, ki predstavljajo kulturno dediščino;*
- *upravljajo javna letališča ali morska pristanišča za mednarodni javni promet ali izvajajo prevoze v mednarodnem letalskem in morskem prometu ali*
- *je iz posebnih varnostnih razlogov nujno potrebno.«*

Subjekte, ki morajo organizirati varovanje, vladi predlaga posamezno resorno ministrstvo, ki lahko v določenih primerih predlaga tudi tudi konkretne varnostne ukrepe.

Navedeni subjekti so tako zaradi občutljivosti dejavnosti, ki jo izvajajo, dolžni organizirati varovanje na način, da sami pridobijo licenco po ZZasV-1, ali pa varovanje izvajajo tako, da sklenejo pogodbo o varovanju s profesionalno zasebno varnostno službo, ki ima licenco (72. člen ZZasV-1). Imetnik licence je dolžan izdelati načrt varovanja, pri čemer določi obseg varovanja, upoštevajoč oceno stopnje tveganja. Glede na vsebino del, ki jih opravlja, in zadolžitve, pripravi načrt varovanja varnostni menedžer, ki pri imetniku licence načrtuje in organizira zasebno varovanje. Načrt varovanja obsega fizično in tehnično varovanje, potrebno za operativno izvajanje zasebnega varovanja.

Podrobnejša ureditev glede obveznega varovanja je določena z vladno Uredbo o organiziranju službe varovanja, v kateri so določeni način in obseg varovanja, vsebina programa varovanja, načrt varovanja, ocena stopnje tveganja ter varnostni ukrepi na varovanem območju. V Uredbi je določen nadzor nad izvajanjem uredbe, navedene pa so tudi kazenske določbe.

V ZZasV-1 in v Uredbi o obveznem organiziranju službe varovanja ni posebej določeno varovanje z uporabo videonadzora. Uporaba videonadzora pri varovanju kritične infrastrukture se lahko interpretira na podlagi 3. odstavka 72. člena ZZasV-1, ki določa, da se obseg varovanja določi glede na oceno stopnje tveganja z načrtom varovanja. Pri pripravi načrtov varovanja za zahtevnejše objekte mora tako sodelovati tudi pooblaščeni inženir varnostnih sistemov, ki se ukvarja predvsem s projektno in tehnično dokumentacijo, izdelavo načrtov alarmnega varovanja, požarnega varovanja,

mehanskega varovanja in drugih tehničnih varnostnih sistemov, med katere sodi tudi videonadzorni sistem. V Uredbi je tehnično varovanje, kamor sodijo tudi videnadzorni sistemi, omenjeno kot eden izmed obveznih elementov načrta fizičnega varovanja, in to v 1. odstavku 11. člena.

Tako se glede načrtovanja in izvedbe videonadzornih sistemov z vidika funkcionalnosti in varnosti izvajalci lahko oprejo na tehnične standarde (npr. SIST EN 50132), z vidika zagotavljanja skladnosti z zakonodajo pa na ZVOP-1 in smernice Informacijskega pooblaščenca Republike Slovenije.

4. PRIMER IZ PRAKSE - VIDEONADZOR V PODJETJU MARIBORSKI VODOVOD D. D.

Podjetje Mariborski vodovod je največji enovit regionalni vodooskrbni sistem v Sloveniji. Kot izvajalec obvezne gospodarske lokalne javne službe oskrbe z vodo predstavlja enega izmed najpomembnejših deležnikov upravljavca kritične infrastrukture v državi. Sistem Mariborskega vodovoda zajema 19 lokalnih skupnosti in v 16 lokalnih skupnostih izvaja javno službo distribucije in oskrbe s pitno vodo. V tem območju upravlja s 1615 km vodovodnega omrežja in 304 objekti in napravami, to je 128 prečrpalnimi objekti, 127 vodohrani in 49 vodnjaki, ki sodijo pod komunalne objekte, namenjene za oskrbo s pitno vodo (Uredba o klasifikaciji vrst objektov in objektih državnega pomena, 2011). Na podlagi določil Zakona o kritični infrastrukturi (ZKI, 2017) in določil Zakona o informacijski varnosti (ZInfV, 2018) lahko rečemo, da gre za objekte posebnega državnega pomena, torej imajo tudi poseben pomen pri obvladovanju vseh vrst tveganj. Omeniti je potrebno še, da danes Mariborski vodovod upravlja s 7530 hidranti, ki zagotavljajo osnovno požarno varnost v vseh oskrbovanih lokalnih skupnostih. Vsi navedeni objekti kritične infrastrukture Mariborskega vodovoda oskrbujejo več kot 200.000 prebivalcev v 212 naseljih severovzhodne Slovenije (Burnač, Pungartnik, 2017, str. 18–21). Voda je najbolj pomembna strateška surovina, zato lahko vsako dejanje, ki v sistemu oskrbe s pitno vodo ni nadzorovano, povzroči nepredstavljive oblike in vrste tveganj ali škode. Lastniki vodovodne infrastrukture so lokalne skupnosti, medtem ko je izvajalec javne službe oskrbe s pitno vodo Mariborski vodovod zgolj najemnik vodovodne infrastrukture. V tem delu prihaja do kolizije interesov, kjer lokalne skupnosti ne prepoznavajo potencialne oblike tveganj in nevarnosti, na katero Mariborski vodovod kot izvajalec javne službe opozarja (Uredba o metodologiji za oblikovanje cen storitev obveznih občinskih gospodarskih javnih služb varstva okolja, 2012). Izvajalci in najemniki vodovodne infrastrukture nimajo na voljo zadostnih finančnih sredstev, da bi lahko zagotovili maksimalno obvladovanje nevarnosti. Kar nekaj od teh bi lahko zmanjšali ali celo preprečili z uvedbo videonadzora še na več lokacijah kritične infrastrukture ali z uvedbo naprednejših sistemov.

Za družbo Mariborski vodovod izvaja tehnično in fizično varovanje primerno kvalificiran in usposobljen zunanji izvajalec po navodilih naročnika in skladno z veljavno zakonodajo. V podjetju so na cca. 20 lokacijah postavljene videonadzorne kamere na posameznih objektih. Postavljene so opozorilne table z obvestilom o videonadzoru, ki je skladno z veljavno zakonodajo s področja varstva osebnih podatkov: obvestila so objavljena na primerno veliki tabli, postavljeni na vidnem mestu, npr. pri vhodu, ograji ali drugem primernem delu varovanega območja ali objekta, kjer se izvaja videonadzor. Obvestila vsebujejo vse zahtevane informacije iz 74. člena ZVOP-1. S tem je o obdelavi osebnih podatkov obveščen tudi posameznik. Ostale določbe o izvajanju videonadzora so zapisane v Pravilniku o videonadzoru in Pravilniku o varstvu osebnih podatkov ter ostalih internih pravnih aktih podjetja, s čimer je zadoščeno določbam ZVOP-1, in sicer 75. členu ZVOP-1, tako, da se izvaja videonadzor dostopa v službene oziroma poslovne

prostore zaradi zagotavljanja varnosti ljudi in premoženja ter varovanja informacij. Odločitev o izvajanju videonadzora je sprejel direktor. V pisni odločitvi so bili obrazloženi razlogi za uvedbo videonadzora. Zbirka osebnih podatkov videonadzornega sistema vsebuje posnetek posameznika ter datum in čas vstopa in izstopa iz prostora. Osebni podatki videonadzornega sistema se hranijo največ 30 dni po nastanku, nato se zbrišejo razen v primeru predaje posnetkov policiji.

Pri načrtovanju in izvajanju videonadzornih sistemov je ključno dobro poznavanje tako funkcionalnih zahtev kot zakonskih predpisov. Tako je najprej potrebno ugotoviti, ali obstaja rešitev, ki je manj invazivna od uporabe videonadzora, določiti poslovni razlog vzpostavitve videonadzora in pri izvajanju slediti le definiranemu namenu. Priporočljivo je sprejeti politiko o uporabi videonadzora, ki med drugim določa:

- utemeljitev in namen nadzornega sistema;
- lokacijo in vidno polje kamer;
- posebne zmogljivosti sistema, na primer zvok, zoom, prepoznavanje obraza ali funkcije za nočno gledanje;
- utemeljitev in namen določenih lokacij kamer in njihovega vidnega polja;
- osebje, pooblaščeno za upravljanje sistema in dostop do informacij;
- časovni interval izvajanja nadzora;
- ali in kdaj se bo snemanje zgodilo;
- lokacijo, kjer bodo sprejeti in nadzorovani signali iz opreme;
- smernice za upravljanje videonadzornih posnetkov, vključno z varnostjo, uporabo, razkritjem in hranjenjem;
- postopke za varno uničenje posnetkov;
- postopek, ki ga je treba upoštevati, če obstaja nepooblaščeno razkritje posnetkov;
- postopki, ki posameznikom omogočajo dostop do zajetih osebnih podatkov;
- sankcije za zaposlene v podjetju in izvajalce v primeru kršitve politike.

Uporabo posnetkov in njihovo pregledovanje je potrebno kolikor le mogoče omejiti. Zelo pomembno je tudi ustrezno (za)varovanje videonadzornih sistemov in posnetkov ter omejitev dobe hranjenja le-teh. Posnetke videonadzornih kamer je treba shraniti na varno mesto, dostop pa mora biti omejen na pooblaščene posameznike. Vsak dostop do posnetkov mora biti zabeležen, s tem zagotovimo upoštevanje načela sledljivosti. Posnetke je treba hraniti samo toliko časa, kolikor je potrebno za izpolnitev namena, zaradi katerega se izvaja videonadzor, po preteku roka hrambe pa jih varno uničiti.

Ena izmed možnih rešitev je tudi vzpostavitev integriranega varnostnega sistema. Primer takega sistema bi bil povezani videonadzorni in alarmni sistem na ključnih črpališčih. Tako povezan sistem bi operaterju omogočil boljšo zaznavo varnostnega dogodka in ustrezno reagiranje nanj. Možna je tudi uporaba t. i. inteligentne videoanalitike, ki na podlagi računalniških algoritmov zaznava sumljive dogodke, od gibanja v prepovedanem območju do sumljivih predmetov. Integrirana varnostna rešitev lahko zmanjša stroške in zagotovi donosnost naložb z odpravo dragih ročnih procesov, vendar je glavna prednost izboljšana varnost in s tem zmanjšanje varnostnih tveganj. Koristi, ki jih omogočajo integrirani sistemi lahko vključujejo možnost ogleda alarmov iz vseh sistemov z uporabo enega uporabniškega vmesnika in zmožnost povezovanja varnostih dogodkov, npr. nepooblaščenega vstopa z videonadzornim sistemom, kar olajša raziskavo in analizo situacije. S povezovanjem videonadzornega sistema z

drugimi varnostnimi sistemi, npr. s sistemom pristopne kontrole, povečamo učinkovitost posameznih varnostnih sistemov in razvijemo uporabnejšo rešitev za končnega uporabnika. Na primer:

- Posnetki kamere v živo se lahko integrirajo v programsko opremo za nadzor dostopa, enako se lahko tudi podatki nadzora dostopa ali drugih varnostnih sistemov integrirajo v sistem videonadzora.
- Nadzor dostopa in drugi varnostni sistemi zaznavanja lahko sprožijo snemanje videoposnetkov pred dogodkom in po njem ter povezovanje videoposnetkov z informacijami o dogodku, kar omogoča učinkovitejše iskanje in analiziranje varnostnih dogodkov.
- Sledenje sumljivim uporabam identifikacijskih kartic in beleženje podrobnosti dostopov s pomočjo posnetkov videonadzornih kamer.
- Prednastavitve snemanja, ko se pojavijo določeni dogodki: npr. ob vstopu v objekt se aktivira tudi zoom kamere, ki omogoča prepoznavo posameznika.
- Ugotavljanje nepooblaščenega vstopa več oseb hkrati z uporabo ene same identifikacijske kartice.

Glede na obširnost sistema kritične infrastrukture Mariborskega vodovoda je namestitev videonadzornega sistema na vseh lokacijah, vključno z vodohrani, ki so prostorsko oddaljeni in razpršeni, poseben izziv, ustrezne rešitve bo šele potrebno najti in preizkusiti.

5. ZAKLJUČEK

Videonadzor se je s časom izkazal kot uporabna tehnologija pri varovanju ljudi in premoženja ter preprečevanju kriminala in kot pomoč pri preiskavi varnostnih dogodkov. Predstavlja enega izmed temeljnih sredstev tehničnega varovanja. S spremljanjem dogajanja na daljavo omogoča učinkovitejše varovanje in ustreznejše reagiranje v primeru varnostnih dogodkov, še preden se ti razvijejo v varnostni incident ali škodni dogodek. Čeprav videonadzor prispeva k višji stopnji varovanja in uresničevanju varne skupnosti, pa se pri njegovi uporabi izpostavlja tudi zasebnost posameznika na videoposnetku. Tako je potrebno pri načrtovanju in izvajanju videonadzornih sistemov poleg funkcionalnih zahtev upoštevati tudi zakonitost uporabe.

Uporabo posnetkov in njihovo pregledovanje je potrebno kolikor le mogoče omejiti. Zelo pomembno je ustrezno varovanje videonadzornih sistemov in posnetkov. Posnetke videonadzornih kamer je treba shraniti na varno mesto, dostop pa mora biti omejen na pooblaščene posameznike. Vsak dostop do posnetkov mora biti zabeležen, s čimer zagotovimo upoštevanje načela sledljivosti. Posnetke je treba hraniti samo toliko časa, kolikor je potrebno za izpolnitev namena, zaradi katerega se izvaja videonadzor, po preteku roka hrambe pa jih je potrebno varno uničiti.

Čeprav uporaba videonadzora pri varovanju kritične infrastrukture ni eksplicitno določena v področni zakonodaji, je na voljo dovolj informacij o ustrezni in zakonsko skladni uporabi teh sistemov. Prav tako obstaja veliko ustreznih tehničnih rešitev, ki s pravilno namestitvijo zagotavljajo želeno funkcionalnost, hkrati pa omogočajo dovolj visoko stopnjo zasebnosti posameznikov, ki vstopajo v polje nadzora. Glede na obširnost sistema kritične infrastrukture Mariborskega vodovoda je namestitev videonadzornega sistema na vseh lokacijah, vključno z vodohrani, ki so prostorsko oddaljeni in razpršeni, poseben izziv, ustrezne rešitve bo šele potrebno najti in preizkusiti.

Pri vsem skupaj pa ne smemo pozabiti, da imajo posamezniki pravico vedeti, kdo jih gleda in zakaj, katere informacije o njih so zajete ter kaj se z njimi dogaja. Zato moramo biti pripravljeni na vprašanja s strani javnosti in na omogočanje dostopa do informacij posameznikom. Pri morebitni izdaji posnetkov posameznikom je potrebno zagotoviti, da identiteta drugih na istem posnetku ni razkrita.

SUMMARY

GENERAL DATA PROTECTION REGULATION AND USE OF VIDEO SURVEILLANCE TO PROTECT CRITICAL INFRASTRUCTURE

Marko POTOKAR, M. Sc.
Faculty of Information Studies,
Novo mesto, Slovenia
marko.potokar@ifit.si

Danilo BURNAČ
Water Utility Company Maribor, Slovenia
danilo.burnac@mb-vodovod.si

Sanja ANDROIĆ
Water Utility Company Maribor, Slovenia
sanja.androic@mb-vodovod.si

Milka PUNGARTNIK, Ph. D.
Water Utility Company Maribor, Slovenia
milka.pungartnik@mb-vodovod.si

On 25 May 2018, a new European regulation on the protection of personal data (the General Data Protection Regulation (GDPR)), which raises the level of protection of individuals' privacy came into force. GDPR is more binding on the operators and processors of personal data. Operators will be obliged to provide stricter security controls before and when processing personal data. They will have to satisfy the principle of embedded and default protection of personal data. The principle of liability is also added, which also requires, among eligible data controllers, the appropriate insurance, the ability to demonstrate compliance with the General Regulation. Operators will have to verify the appropriateness of the consent already obtained and consider the possible identification of an authorized person for the protection of personal data. New features are also the provisions of the General Regulation, which require a higher standard in the processing of personal data from processors.

The valid General Regulation, one of which goals was also harmonization in the field of obligations of controllers, in the supervisory practice and powers of supervisory authorities, also allows the implementation of certain provisions in national legislation. Thus, a draft Personal Data Protection Act (ZVOP-2) was prepared by the Ministry of Justice, which has not been adopted at the moment. Until the adoption of the new law, the provisions of the ZVOP-1, which are not in direct contradiction with the General Regulation, remains such as provisions of sectoral arrangements, including provisions on direct marketing, biometrics, records of entries and exits from premises, and provisions on the implementation of video surveillance.

The concept of critical infrastructure is defined in the Slovenian legislation in the Critical Infrastructure Act, which stipulates in Article 4, paragraph 3, that ''Critical infrastructure covers those facilities and services that are of key importance for the state and the interruption of their operation or their destruction would be significantly affected and have serious consequences for national security, the economy, key social functions, health, safety and security and social well-being.'' An implicit definition occurs in VIII. chapter of the Private Security Act (ZzasV-1, 2011), which stipulates the obligatory organization of the security in Article 69, where it is stipulated in paragraph 1 that upon

the proposal of the ministry responsible for a particular area, the government determines, by resolution, individual private entrepreneurs, institutions, public authorities, public agencies, organizations and other legal and natural persons (hereinafter: taxpayers), who must organize security and, if necessary, concrete security measures if: "they use or store radioactive materials, nuclear fuels, waste and other people and environmentally hazardous substances and devices; manage the capacities, systems or parts thereof that are essential for the maintenance of key social functions, health, safety, protection, economic and social well-being of people and whose deterioration or destruction would have serious consequences on the national security of the Republic of Slovenia due to the inability to maintain these functions (traffic, energy, telecommunications); store archives and objects that represent cultural heritage; operated by public airports or seaports for international public transport or carrying out transport operations in international aviation and maritime traffic or is strictly necessary for special security reasons.''

In the article we have shown how to establish a legally compliant video surveillance of water supply facilities and devices in Mariborski vodovod, which is one of the essential parts of the critical infrastructure. The company is the largest unified water supply system and regional water supplier in Slovenia, and with the implementation of the public water distribution service is one of the most important stakeholders in critical infrastructure.

Viri in literatura:

Burnač, D. in Pungartnik, M. (2017). Podlage in razlogi, zakaj bi morala biti vodna infrastruktura v Sloveniji vključena v kritično infrastrukturo državnega pomena. *Korporativna varnost, 15,* str. 18–21. Ljubljana: Inštitut za korporativne varnostne študije - ICS Ljubljana.

Informacijski pooblaščenec (2015). *Smernice za izvajanje videonadzora*. Pridobljeno 11. 12. 2018 s spletne strani: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_videonadzoru_web.pdf.

Potokar M. in Androić S. (2014). Video Surveillance and Corporate Security. *Varstvoslovje, Journal of Criminal Justice and Security, 2,* str. 148–163. Ljubljana: Fakulteta za varnostne vede.

Regulation (EU) 2016/679 of the European parliament and of the council (2016). Pridobljeno s spletne strani 20. 11. 2018: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

Uredba o klasifikaciji vrst objektov in objektih državnega pomena (2011). Uradni list RS, št 109.

Uredba o metodologiji za oblikovanje cen storitev obveznih gospodarskih javnih služb varstva okolja (2012). Uradni list RS, št. 87.

Zakon o informacijski varnosti (2018). Uradni list RS, št. 30.

Zakon o kritični infrastrukturi (ZKI) (2017). Uradni list RS, št. 75.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1) (2007). Pridobljeno 13. 12. 2018 s spletne strani: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-01-4690?sop=2007-01-4690.

Zakon o zasebnem varovanju (ZzasV-1) (2011). Pridobljeno 15. 12. 2018 s spletne strani: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/102527.