

TEHNIČNO POROČILO za lokacije, kjer bosta vzpostavljena sistem registracije delovnega časa in kontrole dostopa

1. Uvod

Za investitorja Finančna uprava Republike Slovenije, Šmartinska cesta 55, 1000 Ljubljana je izdelana projektna dokumentacija za izvedbo gradnje (PZI) za sistem kontrole pristopa in za sistem registracije delovnega časa za naslednje lokacije:

- Generalni finančni urad, Šmartinska cesta 55, 1000 Ljubljana,
- Finančni urad Brežice, Cesta prvih borcev 39a, 8250 Brežice,
- Finančni urad Celje, Aškerčeva ulica 12, 3102 Celje,
- Finančni urad Celje, Kidričeva ulica 36, 3102 Celje,
- Finančni urad Dravograd, Mariborska cesta 3a, 2370 Dravograd,
- Finančni urad Hrastnik, Log 9, 1430 Hrastnik,
- Finančni urad Kočevje, Ljubljanska cesta 10, 1330 Kočevje,
- Finančni urad Koper, Vojkovo nabrežje 36, 6104 Koper,
- Finančni urad Koper, Vojkovo nabrežje 38, 6104 Koper,
- Finančni urad Koper, Partizanska cesta 81, 6210 Sežana,
- Finančni urad Kranj, Spodnji plavž 6c, 4270 Jesenice,
- Finančni urad Ljubljana, Kolodvorska 4, 1290 Grosuplje,
- Finančni urad Maribor, Titova cesta 10, 2502 Maribor,
- Finančni urad Maribor, Tržaška cesta 49, 2000 Maribor,
- Finančni urad Maribor - mejni prehod Gruškovje, Zgornje Gruškovje 1, 2286 Podlehnik,
- Finančni urad Murska Sobota, Slomškova ulica 1, 9001 Murska Sobota,
- Finančni urad Murska Sobota, Slomškova ulica 2, 9001 Murska Sobota,
- Finančni urad Murska Sobota, Nemčavci 1d, 9000 Murska Sobota,
- Finančni urad Novo mesto, Kandijska cesta 21, 8001 Novo mesto,
- Finančni urad Novo mesto, Obrežje 26 (objekta št. 33 in 15), 8261 Jesenice na Dolenjskem,
- Finančni urad Novo mesto, Selska cesta 16, 8257 Dobova,
- Finančni urad Novo mesto, Cesta bratstva in enotnosti 97, 8330 Metlika,
- Finančni urad Novo mesto, Kočevarjeva ulica 1, 8000 Novo mesto,
- Finančni urad Ptuj, Trstenjakova ulica 2a, 2250 Ptuj,
- Finančni urad Velenje, Kopališka cesta 2a, 3320 Velenje,
- Posebni finančni urad, Gospodinjska cesta 8, 1001 Ljubljana.

Dokumentacija je izdelana na osnovi:

- prejetih tlorisnih podlog,
- zahtev predstavnikov investitorja,
- ogleda objekta.

Pri izdelavi projektne dokumentacije so bili uporabljeni sledeči zakoni, uredbe in tehnične smernice:

- Gradbeni zakon – GZ-1 (Uradni list RS, št. 199/21),
- Zakon o varstvu pred požarom (Uradni list RS, št. 3/07 – UPB, 9/11, 83/12, 61/17 – GZ, 189/20 – ZFRO in 43/22).
- Zakon o varnosti in zdravju pri delu – ZVZD-1 (Ur. list RS 43/11),
- Zakon o zasebnem varovanju – ZZasV-1, (Uradni list RS, št. 17/11),
- Zakon o varstvu osebnih podatkov – ZVOP-2, (Uradni list RS, št. 163/22),
- Uredba o razvrščanju objektov (Uradni list RS, št. 37/18, 199/21 – GZ-1 in 96/22),
- Uredba (EU, št. 2016/679 - GDPR) o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES,
- Pravilnik o projektni in drugi dokumentaciji ter obrazcih pri graditvi objektov (Uradni list RS, št. 30/23),

- Pravilnik o zahtevah za nizkonapetostne električne inštalacije v stavbah (Uradni list RS, št. 41/09, 02/12 in 140/21),
- Pravilnik o izvajanju Zakona o zasebnem varovanju (Uradni list RS, št. 100/11),
- SIST EN 13637: 2015, Električno krmiljeni sistemi izhodov za evakuacijske poti,
- SIST EN 60839-11-1:2013, Alarmni sistemi, Elektronski sistemi kontrole dostopa - Zahteve za sisteme in sestavne dele,
- SIST EN 60839-11-2:2013, Alarmni sistemi, Elektronski sistemi kontrole dostopa - Smernice za uporabo
- SIST EN 13633: 2009, Električno krmiljeni sistemi izhodov za evakuacijske poti ob paniki,
- SIST EN 50575: 2014/A1: 2016, Elektroenergetski, krmilni in komunikacijski kabli - Kabli za splošno uporabo za gradbena dela glede na zahteve za odpornost proti požaru,
- Tehnična smernica TSG-1-001: 2019, Požarna varnost v stavbah,
- Tehnična smernica TSG-N-002: 2021, NN električne inštalacije,
- Smernica SZPV 408/20, Požarnovarnostne zahteve za električne in cevne napeljave v stavbah.
- Smernica SZPV 413/17, Zahteve za avtomatska vrata na evakuacijskih poteh (v kolikor so v objektih avtomatska drsna ali krilna vrata),
- Smernica SZPV 411/12, Električni sistemi za zaklepanje vrat na evakuacijskih poteh (v kolikor je predvidena kontrola pristopa v smeri evakuacije).

2. Kontrola pristopa za lokacije

Naloga sistema kontrole pristopa je samostojno nadzorovanje gibanja oseb v posameznih delih objektov in v prostorih, kjer je gibanje omejeno.

Sistem kontrole pristopa zagotavlja, da imajo dostop na določena varovana območja samo pooblaščen osebe, onemogoča dostop (prehod) nepooblaščenim osebam, javi poizkus takega prehoda ter ga zabeleži.

Sistem kontrole pristopa v osnovi vključuje strojno opremo (krmilne enote, čitalniki identifikacijskih sredstev), različne zaklepne elemente, komponente za napajanje in programsko opremo, ki povezuje delovanje komponent. Kot del sistema štejemo tudi identifikacijska sredstva, s katerimi uporabniki komunicirajo s sistemom.

Krmilne enote so osrednji element sistema kontrole pristopa. Preko priključenih čitalnikov prepoznajo uporabnike identifikacijskih sredstev, krmilijo sprostivne mehanizme, zagotavljajo napajanje čitalnikom in rezervno baterijsko napajanje, komunicirajo z računalniškim delom sistema in drugimi napravami ter beležijo vse za sistem pomembne dogodke. So avtonomne naprave z lokalnim spominom dogodkov, zato lahko delujejo tudi v primeru prekinitve povezave z računalniškim delom sistema. Po ponovni vzpostavitvi komunikacije se podatki v računalniški del sistema prenesejo samodejno. V primeru izpada omrežnega napajanja je število prehodov omejeno s kapaciteto vgrajene baterije.

S posamezno krmilno enoto je mogoče nadzorovati več vrat oz. prehodov (čitalnikov in zaklepnih mehanizmov). Razdalja med krmilno enoto in vrati ne sme presegati fizikalnih omejitev napajalnih napetosti za končne naprave (čitalnike, električne ključavnice, ipd.) V krmilno enoto je vgrajen napajalnik 230V AC / 12V DC in baterija za zanesljivo delovanje v primeru izpada omrežne napetosti. Da bi bilo teh primerov karseda malo, se krmilne enote kontrole pristopa priklapljajo na zanesljive vire napajanja, kot so UPS in DIZEL agregat. V primerih, ko priključene naprave presegajo omejitve vgrajenega napajalnika, je potrebno vgraditi dodatni napajalnik.

Krmilno enoto se namesti v bližini vrat, po možnosti na varni strani prehodov, na mesto, ki je težje dosegljivo (pod strop, nad spuščnim stropom) oz. v prostore, ki niso prosto dostopni (komunikacijsko vozlišče, sistemski prostor).

Omrežno napajanje 230V AC za krmilne enote se izvede iz lokalnih elektro razdelilnikov, po možnosti z vgradnjo novih varovalnih elementov.

TCP/IP komunikacijski vmesnik, ki je vgrajen v krmilno enoto, omogoča priklop neposredno v računalniško omrežje. Krmilne enote se na mrežna stikala povežejo preko priključnega panela. Vsaka krmilna enota zaseda svoja vrata na mrežnem stikalu in potrebuje lokalni statični IP naslov. Izvajalec poskrbi za izvedbo mrežnih povezav med krmilnimi enotami in mrežnimi stikali, investitor pa zagotovi proste priključke na mrežnih stikalih in poskrbi za konfiguracijo mrežnih stikal oz. za ustrezne nastavitve omrežja.

Čitalniki z brezkontaktnim branjem identifikacijskih sredstev omogočajo hitro in varno identifikacijo oseb v sistemu kontrole pristopa. Uporabljajo se za vse vrste prehodov in podpirajo branje podatkov s kartic, obeskov in pametnih telefonov (Android in iOS).

Projektna rešitev kot primarno identifikacijsko sredstvo predvideva uporabo brezkontaktnih kartic, ki delujejo na osnovi MIFARE DESFire EV3 (13,56 MHz) tehnologije. Prenos podatkov na celotni komunikacijski poti med identifikacijsko kartico in krmilno enoto je kriptiran. Enako velja tudi za prenos podatkov iz krmilne enote do računalniškega dela sistema.

Brezkontaktni čitalnik deluje na fizikalnem principu indukcije, zato se je potrebno izogibati namestitvi na ali v neposredno bližino kovinskih podlag, ki močno omejijo ali onemogočijo domet. Oddaljenost čitalnikov od električnih stikal naj bo najmanj 15 cm. Čitalniki se namestijo na višini približno 120-130 cm in minimalno 10 cm od roba podboja vrat.

Krmilna enota lahko krmili različne zapiralne, zaklepne in pridržalne mehanizme (električni prijemnik, elektromagnet), avtomatska krilna, drsna, dvizna vrata, dvigala, omarice za hranjenje ključev, druge omejitelne naprave na točki vstopa (triogeltnik, zapornica).

Za klasična krilna vrata se uporabi električni prijemnik, ki se poveže s krmilno enoto. Napajanje električnega prijemnika se izvede iz krmilne enote. Odpiranje posameznih vratnih kril oz. prehodov je možno po predhodni sprostitvi mehanske blokade električnega prijemnika z dovodom električne energije.

Predpogoj za ustrezno delovanje kontrole dostopa na krilnih vratih je ustrezno mehansko okovje - notranja ključavnica s povratnim mehanizmom, slepa kljuka (bunka) na vstopni strani in kljuka na izstopni oz. slepa kljuka (bunka) na obeh straneh v primeru dvosmerne kontrole dostopa ter hidravlično samozapiralo za zanesljivo zapiranje vrat.

V primeru nastanka nevarnih razmer v objektu (požar, splošna panika, potres, poplava ipd.) je potrebno omogočiti hitro in varno evakuacijo oseb iz vseh prostorov. Izvedba kontrole pristopa mora omogočati hitro in zanesljivo odpiranje vseh evakuacijskih prehodov in izhodov. Vrata na evakuacijski poti, na katerih je predvidena kontrola pristopa v smeri evakuacije, se opremijo s terminalom za izhod v sili. Na vratih, ki so uporabljena za ločitev požarnih sektorjev, je v primeru vgradnje električnega prijemnika potrebno uporabiti električne prijemnike s požarno odpornostjo, ki je enaka ali višja od požarne odpornosti požarnih vrat.

Sestavni del sistema kontrole pristopa je tudi računalniška oprema vključno z ustrezno programsko opremo.

Programska oprema sistema kontrole pristopa omogoča programiranje in konfiguriranje sistema, upravljanje z uporabniki in identifikacijskimi sredstvi, nastavljanje pravic na posameznih prehodih, kreiranje registracijskih skupin, spremljanje dogajanja v sistemu, izpis in tiskanje filtriranih poročil o dogodkih v sistemu, izvajanje diagnostike v smislu zagotavljanja uspešne odprave napak.

Programska oprema sistema kontrole pristopa bo nameščena na virtualnem strežniku, ki ga bo zagotovil investitor na izbrani lokaciji.

Sistem kontrole pristopa deluje popolnoma avtonomno, tudi v primeru izpada lastnega omrežja ali strežnika. Operacije pošiljanja informacij za potrebe odločitev o veljavnosti (avtentičnosti) identifikacijskih sredstev, preverjanja pravilnosti delovanja krmilnih enot, sabotažnega nadzora, se izvajajo na lokalnem nivoju. To pomeni, da sistem deluje z enako stopnjo zanesljivosti in varnosti tudi če pride do okvare ali fizičnega uničenja strežnika, saj se podatki zapisujejo lokalno (pomnilniki krmilnih enot), po vzpostavitvi normalnega stanja pa se izvede prenos v podatkovno bazo. Neglede na to pa je potrebno programsko opremo ustrezno vzdrževati in posodabljati skozi celotno obdobje uporabe, strežnik pa redno nadzorovati in preverjati ali deluje pravilno.

Programska oprema sistema za kontrolo pristopa ni predmet tega načrta.

3. Registracija delovnega časa

Naloga sistemov za registracijo delovnega časa je zagotavljanje učinkovite in ustrezne podpore vodenju evidenc v zvezi z izrabo delovnega časa - natančno beleženje prihodov zaposlenih na delo oz. njihovih odhodov z dela, porabljen čas za malico, trajanje odsotnosti zaradi službenih ali privatnih zadev, zamude, prezgodnje odhode z dela, koriščenje ur, dopustov, bolniško odsotnost itd.. Tipi registracij so prilagodljivi in jih je mogoče nastaviti tako, da ustrezajo načinu dela v določenem okolju. Sistem za registracijo delovnega časa zagotavlja zakonsko usklajeno evidenco vseh oblik delovnega časa, omogoča dostop zaposlenim do teh podatkov ter pošiljanje urnih listov zaposlenim. Razen tega zagotavlja revizijsko sled, samodejne izračune in avtomatski izvoz podatkov za obračun plač ter njihovo arhiviranje.

Registracijo delovnega časa je mogoče izvajati na več načinov. Osnovni predvideni način je registracija delovnega časa na terminalu za registracijo z uporabo identifikacijskega sredstva. Dodatni možnosti sta registracija delovnega časa s pomočjo mobilne aplikacije in s pomočjo brskalnika oz. spletne aplikacije.

Predvideni terminal za registracijo omogoča uporabo različnih kartičnih tehnologij ter tehnologiji NFC in BLE, kar omogoča identifikacijo tudi s pametnimi telefoni.

Projektna rešitev kot identifikacijsko sredstvo za registracijo delovnega časa predvideva uporabo istih identifikacijskih kartic kot sistem kontrole pristopa (Mifare DESFire EV3; 13,56 MHz).

Registracija delovnega časa poteka tako, da uporabnik ob rednem ali izrednem prihodu/odhodu približajo svojo brezkontaktno kartico terminalu, ki dogodek ustrezno zabeleži.

Terminal za registracijo delovnega časa je povezan s strežnikom, na katerem je nameščena programska oprema sistema za registracijo delovnega časa. Terminal se priključi na računalniško omrežje, preko katerega se tudi napaja. PoE injektor, ki se uporabi za napajanje, se namesti v komunikacijsko omaro, v kateri se zaključi mrežni kabel, ki služi pa povezavo s terminalom za registracijo. Izvajalec poskrbi za izvedbo mrežnih povezav med terminali za registracijo in mrežnimi stikali, investitor pa zagotovi proste priključke na mrežnih stikalih in poskrbi za konfiguracijo mrežnih stikal oz. za ustrezne nastavitve omrežja.

Programska oprema sistema registracije delovnega časa bo nameščena na virtualnem strežniku, ki ga bo zagotovil investitor na izbrani lokaciji.

Programska oprema sistema za registracijo delovnega časa ni predmet tega načrta.

4. Električne inštalacije in izvedba del

Napajanje opreme z omrežno napetostjo 230 V AC se izvede z energetske kablom. Tokokrogi se varujejo z instalacijskimi odklopniki. Praviloma se uporabijo tokokrogi rezervirani za ta namen oziroma rezervni tokokrogi. Na te tokokroge ni dovoljeno priklopiti drugih porabnikov.

Inštalacije za prenos različnih tipov signalov se izvedejo s signalnimi kablji. Tipi predvidenih kablov so razvidni iz grafičnega dela tega načrta. Izvajalec mora pred izvedbo v skladu s ponujeno opremo preveriti, ali v načrtu predvideni tipi kablov ustrezajo in jih določiti v skladu s potrebami ponujene opreme.

Skladno s standardom SIST EN 50575 morajo imeti kablji za posamezna področja lastnosti ob požaru najmanj B2ca - s1, d1, a1, na zaščitnih evakuacijskih poteh (stopnišča in hodniki) ter Cca - s1, d2, a1, v ostalih prostorih.

Skladno s smernico SZPV 408/20 se lahko, ne glede na navedene zahteve, v vseh primerih uporabljajo kablji razreda Eca/Cca, če so položeni:

- pod ometom z debelino najmanj 15mm,
- pod estrihi, če je izolacija pod estrihom in okoli kablov v širini najmanj 100mm negorljiva,
- v stenah ali medetažnih ploščah, zaščitnih z mineralnimi ploščami z debelino najmanj 15mm,
- v stenah ali medetažnih ploščah, zaščitnih z mavčno-kartonskimi ploščami, z debelino najmanj 20mm in z negorljivo izolacijo, z debelino 50mm in gostoto najmanj 40kg/m³,
- v ustrezno požarno odporne instalacijske jaške ali kanale.

Za odcepe kablov iz plošč ali sten so dovoljeni kablji razreda Eca/Cca, če je prosta dolžina kablov, ki so položeni po enem od zgoraj navedenih načinov, krajša od 2m.

Kabelske inštalacijske povezave po objektu se izvedejo večinoma podometno in delno nadometno s polaganjem na kabelske police PK ali v PVC NIK kanalih oz. PN ceveh.

Pri polaganju kablov je treba posebno pozornost posvetiti sili vzdolžnega potega (vleke), ki ne sme biti večja od predpisane. Radij ukrivljenega kabla po notranji strani krivljenja ne sme v nobenem primeru biti manjši od predpisanega. Lom kablov pod pravim kotom ni dovoljen.

Ob polaganju kablov se na vseh razvodnih točkah izvedejo ustrezne rezerve v dolžini kablov.

Označevanje elementov in instalacij naj se izvede kvalitetno. Oznake morajo biti dobro vidne, trajne in razumljive.

Zaščitni elementi (instalacijski odklopnik, talilni vložek), ki ščitijo tokokroge 230 V AC naprav za kontrolo pristopa, morajo biti ustrezno označeni in obvezno pobarvani, da se vidno ločijo od ostalih zaščitnih naprav.

Posebno pozornost je treba posvetiti trajni in kvalitetni mehanski pritrditvi vseh ohišij naprav in elementov ter ustrezni ozemljitvi ohišij naprav, ki bi pri delovanju lahko prišli pod napetost. Vsa kovinska ohišja in prevodni kovinski deli naprav in opreme se povežejo s sistemom za izenačevanje

potencialov, kot določajo predpisi. Enako je treba posebno pozornost posvetiti kvalitetni izvedbi tesnjenja kabelskih uvodov ali cevi skozi kabelske uvodnice.

Odprtine na mejah požarnih sektorjev, skozi katere potekajo inštalacije, morajo biti ustrezno požarno zatesnjene, da se ob morebitnem požaru prepreči širjenje ognja in dima. Pri navedenem mora biti požarna odpornost tesnjenih odprtin najmanj enaka požarni odpornosti, ki je zahtevana za gradbene elemente, v katerih so te odprtine izvedene. Priporoča se, da sistem požarnega tesnjenja vzdržuje ustrezno strokovno usposobljen izvajalec z licenco. Stanje in ustreznost požarnega tesnjenja je treba preverjati z rednimi periodičnimi pregledi (npr. skupaj s pregledom javljalnikov požara).

Po izvedbi del in poskusnem obratovanju se obvezno z meritvijo ugotovita (i) tok mirovne porabe in (ii) tok alarmne porabe vseh naprav z AKU rezervnim napajanjem, na osnovi katerih se preveri ustreznost kapacitete AKU baterij.

Izvajalec del mora za vsa odstopanja od dokumentacije in spremembe v opremi, materialu in tehnični izvedbi, pridobiti soglasje strokovnega nadzora in/ali predstavnika investitorja ter pooblaščenega inženirja. Spremembe je izvajalec dolžan vnesti v delovni izvod projektne dokumentacije PZI, ki ga pripravi tako, da bo služil za izdelavo dokumentacije PID.

=====

VGRADI SE LAHKO SAMO OPREMA IN INŠTALACIJE Z USTREZNIMI CERTIFIKATI.

=====

=====

BISTVENEGA POMENA ZA IZVEDBO JE, DA SE ZAGOTVI KOORDINIRANO SODELOVANJE IZVAJALCEV VSEH SISTEMOV IN INŠTALACIJ TEHNIČNEGA VAROVANJA TER SODELOVANJE IZVAJALCA SISTEMA ZA JAVLJANJE POŽARA.

=====

=====

TOČEN NAČIN IZVEDBE VSEH KRMILJENJ ELEKTRO-MEHANSKIH ZAKLEPNIH ELEMENTOV SE OBVEZNO PRED IZVEDBO PREVERI TER USKLADI S STROKOVNIM NADZOROM, PREDSTAVNIKOM INVESTITORJA, DOBAVITELJI, IZVAJALCI, SZPV-411 IN SISTEMOM KONTROLE PRISTOPA. OBVEZNO SE PREVERI / UPOŠTEVA TUDI ZADNJE VERZIJE NPV ZA POSAMEZNI OBJEKT.

=====

=====

VGRADNJO SISTEMA ZA KONTROLO PRISTOPA LAHKO IZVEDE LE IZVAJALEC Z VELJAVNO LICENCO MNZ ZA IZVAJANJE SISTEMOV TEHNIČNEGA VAROVANJA.

=====

5. Uporaba in vzdrževanje

Sistemi tehničnega varovanja morajo tudi zaradi svoje narave in narave objektov v vsakem trenutku pravilno delovati.

Lastnik ali uporabnik stanovanjskih, poslovnih ter industrijskih objektov mora skrbeti za stalni tehnični nadzor vgrajenega sistema v skladu s tehničnimi predpisi in navodili proizvajalca oziroma navodili tistega, ki je sistem vgradil.

6. Dokumentacija

Vsi pomembnejši dogodki in posegi na sistemu se vpisujejo v servisno knjigo, ki se hrani na primernem mestu. Priporoča se, da se na istem mestu hrani tudi izvod ali kopija dokumentacije PID, ki služi kot pripomoček pri vzdrževanju in servisiranju sistema.

Dokumentacijo naj uporabljajo samo pooblašene osebe investitorja in pooblašene osebe zunanjih pogodbenih izvajalcev del oz. vzdrževalcev in serviserjev. Investitor naj izdela spisek svojih pooblaščenih oseb in pooblaščenih oseb zunanjih pogodbenih izvajalcev.

Celotna dokumentacija in elektronski podatki, ki obravnava tehnično varovanje, naj se hrani na varnem mestu z omejenim in nadzorovanim dostopom. Varni mesti naj bosta vsaj na dveh lokacijah.

Vsi dostopi do dokumentacije/podatkov za tehnično varovanje morajo biti evidentirani in naj se omogočijo samo za vpogled.

Kopiranje podatkov o sistemu, na pisni ali elektronski način, praviloma ni dovoljeno. Za kopiranje naj se predpišejo ustrezni postopki v skladu z varnostno politiko investitorja.

Pošiljanje dokumentacije/podatkov o sistemu, v pisni obliki ali preko elektronskih komunikacijskih prenosnih poti, praviloma ni dovoljeno. Za pošiljanje naj se predpišejo ustrezni postopki v skladu z varnostno politiko investitorja.

Vsa dokumentacija/podatki za tehnično varovanje se opremi s stopnjo zaupnosti v skladu z varnostno politiko investitorja, npr. najmanj s stopnjo »Interno«.

Dokumentacijo/podatke tehničnega varovanja v pisni obliki, ki niso več potrebni, se komisijsko uniči na varen način (razrez, sežig, varni odvoz, ipd.) in uničenje dokumentira.

7. Pomembnejša zakonska določila za kontrolo pristopa

7.1. Uvod

Področje kontrole pristopa pomembno ureja **Zakon o varstvu osebnih podatkov ZVOP-2 (Uradni list RS, št. 163/22** - v nadaljnjem besedilu: **ZVOP**; velja za trenutno veljavno verzijo!), ki določa pravice, obveznosti, načela in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice (v nadaljnjem besedilu: posameznik) pri obdelavi osebnih podatkov. Osební podatek po zgoraj navedeni zakonodaji je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Zbirka osebnih podatkov je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

Poleg ZVOP področje kontrole pristopa ureja **Zakon o zasebnem varovanju ZZasV-1 (Uradni list RS, št. 17/11** v nadaljnjem besedilu: **ZZasV**; velja za trenutno veljavno verzijo!), ki ureja pravice in obveznosti gospodarskih družb, samostojnih podjetnikov posameznikov, državnih organov, zavodov, javnih agencij ter drugih pravnih in fizičnih oseb (v nadaljnjem besedilu: subjekti) na področju varovanja, ki ga ne zagotavlja država (v nadaljnjem besedilu: zasebno varovanje). Zakon določa zasebno varovanje, oblike varovanja, pristojnosti, pogoje za opravljanje zasebnega varovanja, standarde, strokovno usposabljanje in izpopolnjevanje, ukrepe in dolžnosti varnostnika, oznake in delovno obleko, pogoje za opravljanje zasebnega varovanja tujih oseb, obvezno organiziranje varovanja ter dolžnosti subjektov, nadzor, evidence in kazenske določbe. Na osnovi ZZasV področje uvedbe in uporabe evidentiranja vstopov in izstopov v prostore podrobneje ureja Pravilnik o izvajanju Zakona o zasebnem varovanju (v nadaljnjem besedilu: Pravilnik o izvajanju ZZasV; velja za trenutno veljavno verzijo!).

Povzetek najpomembnejših določil zakonodaje v zvezi s sistemom kontrole pristopa je podan v nadaljevanju.

7.2. Dolžnost zavarovanja osebnih podatkov (ZVOP)

Upravljalci osebnih podatkov in pogodbeni obdelovalci so dolžni zagotoviti zavarovanje osebnih podatkov.

Upravljalci osebnih podatkov v svojih aktih predpišejo postopke in ukrepe za zavarovanje osebnih podatkov ter določijo osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

7.3. Vsebina zavarovanja osebnih podatkov (ZVOP)

Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov. Vsebine zavarovanja so določene v ZVOP.

7.4. Ukrepi varnostnika (ZZasV)

Varnostnik lahko uporablja sisteme tehničnega varovanja v skladu ZZasV in področno zakonodajo, ki ureja sisteme tehničnega varovanja.

Sistemi tehničnega varovanja so posamezna ali funkcionalno povezana tehnična sredstva in mehanske naprave za varovanje, **naprave za** protivlomno in protiropno varovanje, **kontrolno vstopa, izstopa ali gibanja**, pregled oseb, prevoznih sredstev, tovora in prtljage, preprečevanje nasilnega vstopa, samodejno odkrivanje in javljanje nepooblaščenosti prisotnosti, prenos alarmnih sporočil ter sredstva za obdelavo in arhiviranje teh sporočil (video in avdio nadzor, varnostni alarmi, senzorji in detektorji gibanja, sistemi za nadzor alarmov, kamer in senzorjev), električne, elektromagnetne, magnetne ali biometrične naprave za vstopno kontrolo ter drugi sistemi in naprave, ki so namenjeni varovanju po ZZasV.

Za sisteme tehničnega varovanja po ZZasV se štejejo tudi drugi sistemi, ki se neločljivo povezani s sistemi tehničnega varovanja po ZZasV in bi poseg v te sisteme pomenil poseg v sisteme tehničnega varovanja po ZZasV (varstvo pred požarom, javljanje eksplozivnih in drugih plinov, socialni alarmi, sistemi za detekcijsko merjenje eksplozivnih in strupenih snovi, plinov in par, varnostne blagajne, varnostna vrata, ključavnice, trezorji in sefi).

Med sisteme tehničnega varovanja se ne štejejo naprave za nadzor nad zalogami in inventuro ter druge naprave in sistemi, ki niso namenjeni za varovanje v skladu z ZZasV.

7.5. Opravljanje zasebnega varovanja (Pravilnik o izvajanju ZZasV)

Varnostnik lahko na varovanem območju v času opravljanja nalog zasebnega varovanja uporablja sisteme tehničnega varovanja (video in avdio nadzor, tehnična sredstva in mehanske naprave za varovanje, kontrolo pristopa, pregled prtljage ali tovora, nadzor varovanega območja ter odkrivanje in preprečevanje neupravičenega vstopa), če tako določajo pravila na varovanem območju, v skladu z zakonom in zakonom, ki ureja varstvo osebnih podatkov.