# Politika obrade osobnih podataka korištenjem sustava za video nadzor

## Povijest dokumenta

| *Voditelj obrade* | *Obrada* |
|---|---|
| Učenički dom Lovran | video nadzor |
| *Datum izrade* | *Izradio* |
| | William Bello |
| *Datum zadnje provjere* | *Provjerio* |
| 01.09.2025. | Maja Voštan Kadić |
| *Datum sljedeće provjere* | *Odgovoran* |
| 01.03.2026. | Ravnateljica Nataša Tomić |

| Datum | Komentar | Autor |
|---|---|---|
| 01.09.2025. | Izrada Politike i priloga | William Bello |
| | | |
| | | |

# Sadržaj

**6) Registar zadržavanja i prijenosa podataka**

**7) Sigurnosna politika video nadzora**

**8) Obavijest da je objekt pod video nadzorom**

**9) Obavijest o prikupljanju i obradi osobnih podataka putem video nadzora**

**10) Odluka o davanju prava pristupa**

**11) Izjava o povjerljivosti**

**12) Infografika 12 principa**

**13) Procjena opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA)**

**14) Procjena učinka na zaštitu podataka (PIA)**

**15) Pohrana podataka (video snimke)**

**16) Evidencija aktivnosti obrade (video nadzora)**

**17) SOP održavanje sustava video nadzora**

**18) SOP uvid u video snimke**

**19) SOP izdavanje video snimke**

**20) SOP uništavanje snimke i ostalih podataka nastalih unutar sustava video nadzora**

**21) SOP poštivanje prava ispitanika prilikom incidenta u sustavu video nadzora**

**22) Dodatak SOP odgovor na zahtjev ispitanika**

**23) SOP za provedbu interne provjere usklađenosti video nadzora**

**24) Zapisnik o uvidu u sustav video nadzora**

**25) Zapisnik o izuzimanju snimke video nadzora**

**26) Zapisnik o brisanju**

**27) Ugovor o izvođenju sustava video nadzora**

**28) Ugovor o obradi podataka s tvrtkom za održavanje sustava video nadzora**

**29) Ugovor s tvrtkom za ovlašteno uništavanje podataka**

# 1 Svrha i područje politike video nadzora

U svrhu zaštite imovine i ljudi, naša organizacija je uspostavila sustav video nadzora. Ova Politika obrade osobnih podataka korištenjem sustava za video nadzor, zajedno s prilozima, opisuje naš sustav kao i organizacijske i tehničke mjere koje smo poduzeli kako bi zaštitili osobne podatke, privatnost, osnovna prava i legitimni interes pojedinaca snimljenih ovim kamerama i pohranjenim u ovaj sustav.

# 2 Kako osiguravamo da je naš sustav postavljen i da se njime upravlja vodeći računa o privatnosti i zaštiti podataka i to sukladno Općoj uredbi o zaštiti podataka?

## 2.1 Dorada postojećeg sustava.

Sustav video nadzora je bio operativan i prije početka primjene Opće uredbe o zaštiti podataka EU 2016/679 i Zakona o provedbi opće uredbe NN 42/2018. Međutim, naše politike i procedure su u međuvremenu ažurirane kako bi se obrada u svrhu video nadzora uskladila sa spomenutim zakonima.

## 2.2 Status usklađenosti

Organizacija obrađuje snimke sukladno Pravilniku o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003), Općom uredbom o zaštiti podataka EU 2016/679 i Zakonom o provođenju opće uredbe o zaštiti podataka NN 42/18 i Zakonom o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka od strane nadležnih tijela u svrhu sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija (NN 68/18).

Prilikom usklađivanja uzete su u obzir preporuke EDPB i EDPS te mišljenje AZOP-a. Pri tome se koristi i dobra praksa stranih nacionalnih nadzornih tijela (posebno ICO UK i CNIL FR), kao i odgovarajućih stručnih tijela industrije zaštite i video nadzora.

Tehnički, sustav video nadzora izveden je od strane ovlaštene tvrtke prema Pravilniku o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003) i ostalim relevantnim zakonima i pravilnicima RH. Izvedbena tehnička dokumentacija projekta predstavlja poslovnu tajnu naše organizacije i dostupna je na zahtjev ovlaštenih osoba u zakonom predviđene svrhe.

## 2.3 Interna provjera

Sustav video nadzora se redovno, najmanje jednom godišnje, provjerava internim nadzorom. Izvješće o provedenoj internoj provjeri nalazi se u prilogu "Izvješće o provedenoj provjeri s rezultatima redovnih pregleda".

## 2.4 Opravdanost legitimnog interesa i procjena učinka

Proveli smo procjenu opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA) i procjenu učinka na zaštitu podataka (PIA).

Procjena opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA) provedena je kroz test u tri koraka: test svrhovitosti, test neophodnosti i test ravnoteže. Pokazalo se da (1) postoji opravdana svrha a to je osiguranje sigurnosti i zaštite imovine i ljudi, (2) da je neophodno korištenje sustava video nadzora kao jedinog adekvatnog tehničkog rješenja za postizanje navedene svrhe, kao i (3) da uvedene organizacijske i tehničke mjere osiguravaju poštivanje

privatnosti i zaštitu osobnih podataka pojedinaca koje dolaze u perimetar snimanja, čime je opravdan naš legitimni interes za provođenjem obrade video nadzora. Rezultati procjene nalaze se u prilogu "Procjena opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA)"

Proveli smo analizu rizika u vidu Procjene učinka na zaštitu podataka (PIA) kroz analizu (1) sadržaja obrade, (2) načela koja smo primijenili prilikom procjene uvedenih kontrola u našoj organizaciji, a kojima jamčimo proporcionalnost i nužnost obrade i zaštitu prava pojedinaca te (3) rizike informacijske sigurnosti. Rezultati procjene nalaze se u prilogu "Procjena učinka na zaštitu podataka (PIA)"

## 2.5 Obavijest nadzornom tijelu

Uzimajući u obzir ograničeno područje upotrebe sustava video nadzora te zaključke provedene analize opravdanosti legitimnog interesa za provođenje video nadzora (LIA) i procjene učinka zaštite podataka (PIA), nije bilo potrebno tražiti mišljenje AZOPa.

## 2.6 Odluka odgovorne osobe i savjetovanje

Odgovorna osoba naše organizacije ravnateljica mr.sc. Nataša Tomić donijela je odluku o korištenju sustava video nadzora i uvođenja organizacijskih i tehničkih mjera zaštite kako je to opisano u ovoj Politici obrade osobnih podataka korištenjem sustava za video nadzor. Pri tome se savjetovala sa:

- službenikom za zaštitu podataka
- sindikalnim povjerenikom koji je preuzeo ulogu radničkog vijeća

Tijekom procesa donošenja odluke:

- procijenili smo opravdanost legitimnog interesa naše organizacije za video nadzorom
- proveli smo procjenu učinka na zaštitu podataka
- sagledali smo preporuke AZOPa, EDPB i EDPS kao i ostalih relevantnih organizacija u svezi obrade osobnih podataka putem video nadzora
- razgovarali o alternativama te na kraju donijeli zaključak da se održi postojeći sustav video nadzora nakon uspostave odgovarajućih organizacijskih i tehničkih mjera zaštite

## 2.7 Transparentnost

Politika obrade osobnih podataka korištenjem sustava za video nadzor napisana je u dvije verzije, verzija za ograničenu upotrebu i javna verzija dostupna na internet stranicama [www.ucenicki-dom-lovran.hr]. Ova javna verzija može sadržavati sažete podatke u odnosu na određene teme ili priloge. Kada je to slučaj, biti će jasno rečeno. Informacije je izostavljena iz javne verzije samo onda kada je neophodno sačuvati povjerljivost iz opravdanih razloga (npr. iz sigurnosnih razloga, čuvanje tajnosti ili komercijalno osjetljivih podataka ili da bi se sačuvala privatnost pojedinaca).

## 2.8 Redovni pregledi

Redovni pregled o zaštiti podataka provest će osoba ovlaštena od strane ravnateljice barem jednom godišnje. Tijekom redovnog pregleda, ponovit će se procjena:

- da i dalje postoji potreba za sustavom video nadzora

- da sustav i dalje ima navedenu svrhu
- da i dalje nema odgovarajuće alternative.

Redovni pregled će također obraditi ostala otvorena pitanja na koja je dan odgovor u prvom izvješću, posebno je li Politika obrade osobnih podataka korištenjem sustava za video nadzor i dalje usklađena s Općom uredbom o zaštiti podataka (provjera podudarnosti) te je li primijenjena u praksi (provjera usklađenosti). Kopije redovnih pregleda priložene su ovoj Politici u prilogu "Izvješće o provedenoj provjeri s rezultatima redovnih pregleda".

# 3 Koje područje se nadzire?

Sustav video nadzora sastoji se od 48 fiksnih kamera. Mapa s lokacijama pojedine kamere nalazi se u prilogu "Raspored postavljenih kamera".

Od 46 kamera, njih 11 je postavljeno na ulazno izlaznim dijelovima zgrade, parkiralištu i okolišu zgrade i dvorištu.

Kamere ne prate i ne snimaju prostor za koji se očekuje veće poštivanje privatnosti, poput pojedinačnih ureda, prostora za odmor, toalet i sl. Lokacije kamera su pažljivo razmotrene kako bi se u najvećoj mjeri smanjilo praćenje prostora koji nije relevantan za navedenu svrhu.

# 4 Koje osobne podatke prikupljamo i u koju svrhu?

## 4.1 Sažeti opis i detaljna tehnička specifikacija sustava

Sustav video nadzora je konvencionalni statički sustav. Zapisuje digitalnu snimku s kamere i opremljen je detektorom pokreta. Bilježi svaki pokret kojega uoči kamera na području pod nadzorom, zajedno s vremenom, datumom i lokacijom. Sve kamere su operativne 24 sata na dan, sedam dana u tjednu. Kvaliteta slike u većini slučajeva omogućava identifikaciju onih koji se zateknu u području snimanja. Kamere su fiksne (nema pan-tilt-and-zoom kamera) tako da operator ne može zumirati nekoga ili pratiti pojedinca kroz lokaciju.

Ne koristimo high-tech ili inteligentne video-surveillance tehnologije, ne spajamo se s drugim sustavima i ne koristimo prikriveni nadzor, snimanje zvuka ili "talking CCTV".

Tehnička specifikacija kamera i video sustava u cjelini (uključujući hardware i software) nalazi se u prilogu "Tehnička specifikacija kamera i cjelovitog sustava video nadzora"

## 4.2 Svrha video nadzora

Sustav video nadzora koristimo isključivo u svrhu zaštite imovine i ljudi. Sustav video nadzora pomaže kontroli pristupa zgradi i pomaže prilikom osiguranja zgrade, sigurnosti zaposlenika, stalno prisutnih i posjetitelja, kao i imovine i informacija koje su smještene ili pohranjene na lokaciji. Sustav video nadzora nadopunjava ostale mjere tehničke zaštite kao što je evidencija ulaza i protuprovalna zaštita. Sustav čini dio ukupnih mjera koje poduzimamo kako bi podržali našu širu politiku sigurnosti i pomogli u sprečavanju, otklanjanju te ukoliko je potrebno istraživanju neovlaštenog fizičkog ulaska, uključujući neovlaštenog ulaska u sigurne prostore i zaštićene sobe, IT infrastrukturu ili operativne podatke. Dodatno, sustav video nadzora pomaže prevenciji, uočavanju i istraživanju krađe opreme i imovine naše organizacije,

zaposlenika ili posjetitelja kao i prijetnji sigurnosti posjetitelja ili zaposlenika koji rade u uredu (npr. požar, fizički napad).

### 4.3 Ograničenje svrhe

Sustav se ne koristi u druge svrhe, npr. za praćenje rada zaposlenika ili prisutnosti na radu, niti se koristi kao istražni alat (osim u slučajevima istraživanja fizičkog sigurnosnog incidenta poput krađe ili neovlaštenog ulaska). Samo u izuzetnim okolnostima snimka može biti predana istražnom tijelu u okviru disciplinskih ili kriminalističkih istraga kako je to opisano u odjeljku 6.5.

### 4.4 Nisu planirana ad-hoc snimanja

Nemamo u vidu ad-hoc snimanja koja bi trebalo unaprijed planirati.

### 4.5 Webcam

Ne koristimo webcam uređaje.

### 4.6 Ne prikupljamo posebne kategorije osobnih podataka

Tijekom video nadzora ne prikupljamo posebne kategorije osobnih podataka.

## 5 Koja je pravna osnova i zakonitost prikupljanja podataka?

Korištenje našeg sustava video nadzora nužno je potrebno za upravljanje i rad naše organizacije (u svrhu zaštite osoba i imovine kako je to opisano u odjeljku 4.2). Stoga imamo legitimnu osnovu po članku 6. stavak 1. (f) GDPR za obradu osobnih podataka korištenjem sustava za video nadzor. Procjena opravdanosti legitimnog interesa detaljnije je obrazložena u prilogu "Procjena opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA)".

Politika obrade osobnih podataka korištenjem sustava za video nadzor koja detaljno argumentira pravnu osnovu i zakonitost prikupljanja podataka dio je šire sigurnosne politike koju provodi naša organizacija.

## 6 Tko ima dostup do informacija i kome su one dostupne?

### 6.1 Ovlaštene osobe

Snimka s kamere dostupna je samo ovlaštenim osobama, dakle odgovornoj osobi osoba koju je odgovorna osoba ovlastila, kako je to određeno u Članku 28 Zakona o provedbi Opće uredbe o zaštiti podataka NN 42/2018. Uvid u kameru (živa slika) dostupna je vrataru, odgajateljima i noćnim paziteljima.

### 6.2 Prava pristupa

Naša politika sigurnosti u dijelu za video nadzor (vidi odjeljak 7 i prilog "Sigurnosna politika video nadzora") jasno određuje i dokumentira tko ima pristup do snimki video nadzora i/ili tehničke arhitekture sustava video nadzora, u koju svrhu te od čega se pravo pristupa sastoji. Posebno, dokument određuje tko ima pravo:

- pogledati kamere u realnom vremenu
- pogledati snimljeni materijal, ili
- kopirati
- presnimiti
- brisati, ili

- mijenjati snimku

## 6.3 Obuka za zaštitu podataka

Osoblje koje ima ovlasti i pravo pristupa sustavu video nadzora dobilo je obuku o tome, a obuka se provodi za svakog novog člana osoblja uključenog u video nadzor. Redovne radionice na temu zaštite podataka provode se svake godine za sve ovlašteno osoblje.

## 6.4 Mjere povjerljivosti

Pri zaposlenju svaki radnik potpisuje izjavu o povjerljivosti. Kopije potpisanih izjava o povjerljivosti nalaze se u prilogu "Primijenjene sigurnosne mjere"

## 6.5 Prijenos i davanje.

Svaki prijenos i davanje snimki van ustanove dokumentira se i podvrgnut je strogoj procjeni neophodnosti takvog prijenosa kao i sukladnosti svrhe prijenosa s polaznom svrhom obrade. Registar pohrane i prijenosa sadržan je u prilogu "Registar zadržavanja i prijenosa podataka". U svakom slučaju se traži mišljenje službenika za zaštitu podataka.

Lokalnoj policiji i sudu može se dozvoliti pristup za potrebe provođenja istrage ili sankcioniranja kriminalnih radnji uz obavezno predočenje odgovarajućeg službenog naloga.

# 7 Kako štitimo i čuvamo podatke?

Kako bi zaštitili sigurnost sustava video nadzora, uključujući osobne podatke, primijenjene su određene organizacijske i tehničke mjere. Detaljno su opisane u prilogu "Sigurnosna politika video nadzora" koja opisuje sigurnosne mjere specifične za tu vrstu obrade.

Naša sigurnosna politika za video nadzor uspostavljena je prema EDPS vodiču za sustav video nadzora.

Između ostaloga, poduzete su sljedeće mjere:

- Osiguran je pristup prostoriji video nadzora, zaštićen fizičkim mjerama zaštite, smještajem servera koji pohranjuje snimke; mrežni firewall štiti logički perimetar IT infrastrukture; glavni računalni sustav koji pohranjuje podatke posebno je sigurnosno ojačan.
- Administrativne mjere uključuju obvezu da je svaki pojedini član vanjskog osoblja koje ima pristup sustavu (uključujući i ono koje održava opremu i sustav) sigurnosno provjeren.
- Cjelokupno osoblje potpisalo je Izjavu o povjerljivosti.
- Pravo pristupa dano je pojedincima samo na one resurse koji su zaista nužno potrebni za obavljanje njihovih zadaća.
- Jedino sistem administrator kojega je posebno za ovu namjenu odredio voditelj obrade može dozvoliti, promijeniti ili poništiti pravo pristupa pojedinoj osobi. Svako izdavanje, izmjena ili poništavanje prava pristupa obavlja se prema kriterijima koji su uspostavljeni u prilogu "Sigurnosna politika video nadzora".
- Sigurnosna politika video nadzora sadrži ažurni popis svih osoba koje imaju ili su ikad imale pristup sustavu s detaljnim opisom pristupnih prava.

# 8 Kako dugo čuvamo podatke?

Snimke se čuvaju ne duže od 6 mjeseci. Nakon toga roka se brišu. Ovisno o intenzitetu snimanja, taj period može biti i kraći kada tehnički sustav automatski briše najstarije snimke.

Ukoliko se neka snimka treba pohraniti radi daljnjih istražnih radnji ili kao dokazni materijal nastavno na sigurnosni incident, pohrana može trajati koliko je to vremenski potrebno. U tom slučaju se zadržavanje strogo dokumentira, a potreba za zadržavanjem redovito provjerava. Kopija zapisa se nalazi u prilogu "Registar zadržavanja i prijenosa podataka".

Sustav se također promatra u živo od strane vratara, odgajatelja i noćnih pazitelja.

# 9 Na koji način informiramo javnost?

## 9.1 Višeslojni pristup

Javnost obavještavamo o provođenju video nadzora na učinkovit i sveobuhvatni način. Za sada koristimo višeslojni pristup koji se sastoji od kombinacije sljedeće dvije metode:

obavijest na licu mjesta kako bi obavijestili javnost da obavljamo video nadzor i kako bi im pružili osnovne informacije o obradi njihovih osobnih podataka, i

objava ove politike video nadzora na našim internet stranicama za one koji žele znati više o tome kako obrađujemo osobne podatke putem sustava video nadzora.

Štampane verzije ove Politike su dostupne u tajništvu Doma. Telefonski broj i elektronička adresa objavljeni su za slučaj dodatnih informacija.

Također objavljujemo proširenu obavijest na glavnom ulazu u zgradu.

## 9.2 Posebne pojedinačne obavijesti

Dodatno, pojedincima također dajemo zasebne obavijesti ukoliko ih identificiramo na kameri u slučajevima kada:

- njihov identitet je zabilježen u datoteci ili zapisu
- video snimka se koristi u postupku prema pojedincu
- snimka se zadržava dulje od redovnog perioda pohrane
- snimka je prenesena van službe zaštite, ili
- identitet pojedinca je otkriven osobama koje nemaju ovlasti po članku 28 (ZPOU NN42/2018).

Davanje obavijesti može biti privremeno odgođeno, primjerice ukoliko je to potrebno radi sprečavanja, provođenja istrage, utvrđivanja činjeničnog stanja ili obrade kriminalnih prijetnji. U takvim situacijama će se zatražiti mišljenje Službenika za zaštitu podataka kako bi se osiguralo poštivanje prava pojedinca.

# 10 Na koji način pojedinac može provjeriti, ispraviti ili izbrisati svoje podatke?

Pojedinac ima pravo pristupa svojim osobnim podacima koje smo prikupili te na njihov ispravak ili dopunu. Svaki zahtjev za pristup, provjeru, blokiranje i/ili brisanje osobnih podataka treba biti upućeno na ravnateljicu Doma preko e-maila:

ravnatelj@ucenicki-dom-lovran.hr. Navedena osoba se također može kontaktirati u slučaju drugih pitanja povezanih s obradom osobnih podataka.

Kada god je to moguće, odgovoriti ćemo bez nepotrebnog odgađanja i u svakom slučaju u roku od mjesec dana od zaprimanja zahtjeva, posebno ukoliko pojedinac istakne žurnost zahtjeva. Taj se rok može prema potrebi produljiti za dodatna dva mjeseca, uzimajući u obzir složenost i broj zahtjevâ. Pojedinca ćemo obavijestiti o svakom takvom produljenju u roku od mjesec dana od zaprimanja zahtjeva, zajedno s razlozima odgađanja. Ako pojedinac podnese zahtjev elektroničkim putem, informacije se pružaju elektroničkim putem ako je to moguće, osim ako ispitanik zatraži drugačije.

Ukoliko ne postupimo po zahtjevu pojedinca, bez odgađanja i najkasnije jedan mjesec od primitka zahtjeva izvijestit ćemo ispitanika o razlozima zbog kojih nismo postupili i o mogućnosti podnošenja pritužbe nadzornom tijelu i traženju pravnog lijeka.

Ukoliko se to posebno zatraži, moguće je dogovoriti pregled snimke ili podnositelj zahtjeva može dobiti kopiju snimke na DVD ili nekom drugom mediju. U slučaju takvog zahtjeva, podnositelj mora označiti svoj identitet van svake sumnje (npr. donijeti osobnu iskaznicu prilikom dolaska na pregled snimke) i, kad god je to moguće, također odrediti datum, vrijeme, mjesto i okolnosti kada su snimljeni kamerom. Također je potrebno donijeti vlastitu nedavnu fotografiju koja će omogućiti ovlaštenoj osobi da identificira pojedinca tijekom pregleda snimke.

U pravilu ne naplaćujemo podnositeljima zahtjeva pregledavanje ili kopiranje snimki. Međutim, zadržavamo pravo da zatražimo razumnu naknadu u slučaju povećanog broja takvih zahtjeva.

Zahtjev za pristupom može biti odbijen pod okolnostima koje predviđa Opća uredba o zaštiti podataka. Zahtjev može biti odbijen i kada je potrebno zaštiti prava i slobode drugih osoba koje se nalaze na snimci a nije dobivena njihova privola za prijenos njihovih osobnih podataka ili nije moguće provesti uređivanje snimke kako bi se te osobe uklonile sa snimke.

# 11 Pravo na prigovor

Svaki pojedinac ima pravo na prigovor nadzornom tijelu ukoliko smatra da su njegova prava zajamčena Općom uredbom o zaštiti podataka EU 2016/679 povrijeđena. Za nas je relevantna Agencija za zaštitu podataka koja se može kontaktirati na poštanskoj adresi: AZOP, Martićeva ulica 14, 10000 Zagreb, ili elektroničku adresu azop@azop.hr odnosno telefon: +385 (0)1 460 9080.

Prije toga, preporučamo da prvo kontaktirate:

- ovlaštenu osobu ravnateljicu Doma preko e-maila: ravnatelj@ucenicki-dom-lovran.hr, i/ili
- našeg službenika za zaštitu podataka [William Bello, dpo@bello.hr, +385 98 211686]

Zaposlenici također imaju pravo zatražiti provjeru temeljem ugovora o radu i drugim pravnim aktima naše organizacije.

# Prilozi

1) Izvješće o provedenoj provjeri s rezultatima redovnih pregleda
2) Raspored postavljenih kamera
3) Tehnička specifikacija kamera i cjelovitog sustava video nadzora
4) Ugovor o obavljanju video nadzora s izvršiteljem obrade
5) Primijenjene sigurnosne mjere
6) Registar zadržavanja i prijenosa podataka
7) Sigurnosna politika video nadzora
8) Obavijest da je objekt pod videonadzorom.docx
9) Obavijest o prikupljanju i obradi osobnih podataka putem video nadzora.docx
10) Odluka o davanju prava pristupa.docx
11) Izjava o povjerljivosti.docx
12) Infografika 12 principa.pdf
13) Procjena opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA)
14) Procjena učinka na zaštitu podataka (PIA)
15) Pohrana podataka (video snimke)
16) Evidencija aktivnosti obrade (videonadzora)
17) SOP održavanje sustava video nadzora
18) SOP uvid u video snimke
19) SOP izdavanje video snimke
20) SOP uništavanje snimke i ostalih podataka nastalih unutar sustava video nadzora
21) SOP poštivanje prava ispitanika prilikom incidenta u sustavu video nadzora
22) Dodatak SOP odgovor na zahtjev ispitanika
23) SOP za provedbu interne provjere usklađenosti video nadzora
24) Zapisnik o uvidu u sustav video nadzora
25) Zapisnik o izuzimanju snimke video nadzora
26) Zapisnik o brisanju
27) Ugovor o izvođenju sustava video nadzora
28) Ugovor o obradi podataka s tvrtkom za održavanje sustava video nadzora
29) Ugovor s tvrtkom za ovlašteno uništavanje podataka

# 1.Izvješće o provedenoj provjeri s rezultatima redovnih pregleda – 01.09.2025. godine

Sljedeći upitnik sastavni je dio Izvješća o provjeri usklađenosti sustava video nadzora

**Popuniti za svaku kameru:**

- Oznaka kamere: **popis svih kamera i njihovih lokacija nalazi se u prilogu 2. – Raspored postavljenih kamera**
- Organizacijski dio poslovne jedinice
- Naziv organizacije: **Učenički dom Lovran**
- Ime i prezime osobe odgovorne za popunjavanje Upitnika: **Maja Voštan Kadić**

1. Pitanje
   - Gdje se koriste kamere, lokacija? (npr. hodnik, prodajni salon, servis, pročelje zgrade itd.) **- popis svih kamera i njihovih lokacija nalazi se u prilogu 2. – Raspored postavljenih kamera**
2. Pitanje
   - Koja je svrha korištenja CCTV kamere i drugih povezanih uređaja na toj lokaciji? **Zaštita osoba i imovine**
3. Pitanje
   - Jesu li pojedinci obaviješteni da su snimljeni video nadzorom i postoji li objavljena kontaktna točka za pristup informacijama i pritužbe pojedinaca? **Obavijesti o prikupljanju osobnih podataka putem sustava video nadzora nalaze se prije ulaska u perimetar snimanja i to su tzv. video naljepnice koje prikazuju sliku video kamere te navode voditelja obrade i kontakt podatke.**
4. Pitanje
   - Da li se podaci (snimke) koriste u neku drugu svrhu (osim navedene u Pitanju 2) **Ne**
   - Ako je potrebna dodatna bilješka
5. Pitanje
   - Ako se koristi video nadzor da li se snima i zvuk? Da/**Ne**
6. Pitanje
   - Postoje li redoviti pregledi / postupci kako bi se osigurala opravdana uporaba video nadzora?

**Redovni pregled o zaštiti podataka provodi osoba ovlaštena od strane ravnateljice barem jednom godišnje. Tijekom redovnog pregleda, ponovit će se procjena:**

- **da i dalje postoji potreba za sustavom video nadzora**
- **da sustav i dalje ima navedenu svrhu**
- **da i dalje nema odgovarajuće alternative.**
- **Redovni pregled će također obraditi ostala otvorena pitanja, posebno je li Politika obrade osobnih podataka korištenjem sustava za video**

**nadzor i dalje usklađena s Općom uredbom o zaštiti podataka (provjera podudarnosti) te je li primijenjena u praksi (provjera usklađenosti)**

7. Pitanje
    - Može li se snimke video nadzora lako izvući / prebaciti s lokacije? **Da**
    - Može li se preuzeti on-line drugdje? **Ne**
    - Dodatne bilješke Opišite proceduru prije izvršenja ovog tipa zahtjeva - **Nakon pisanog zahtjeva pojedinca ravnateljica odlučuje o postupanju po istome. Ukoliko se odobri moguće je dogovoriti pregled snimke ili kopiranje snimke na DVD**
8. Pitanje
    - Koliko se dugo čuvaju snimke video nadzora? **6 mjeseci**
    - Dodatne napomene
9. Pitanje
    - Je li ikada do sada bilo potrebno zadržati informacije duže od zadanog razdoblja čuvanja? **Ne**
    - Dodatne napomene. Molim opišite te okolnosti. Imate li te snimke još uvijek?
10. Pitanje
    - Može li se snimka trajno izbrisati (uključujući bilo koju arhivu)? **Da**
    - Ako je tako, je li ručni proces, može li se jednostavno ponoviti? **Da**
    - Dodatne bilješke. Opišite proceduru prije ispunjenja ovog zahtjeva za brisanjem.- **Nakon pisanog zahtjeva pojedinca ravnateljica odlučuje o postupanju po istome.**
11. Pitanje
    - Vezano uz pitanja 8 i 10, prema vašem znanju, da li su podaci ikad bili očišćeni ili izbrisani? (pod pretpostavkom da podaci više nisu potrebni) **Ne**
12. Pitanje
    - Kako se upravlja sustavima video nadzora i slikama? **Pomoću lozinke za pristup**
13. Pitanje
    - Naziv svih trećih osoba uključenih u video nadzor. Navedite popis svih trećih strana ovdje. – **River solutions d.o.o.**
    - Uloga treće strane? Koje usluge oni pružaju? **Održavanje i servisiranje postojećeg video nadzora**
    - Ako ste identificirali treću stranu, molimo Vas da to prijavite na dokumentu Evidencije trećih strana kod DPO platforme
14. Pitanje
    - Jesu li snimke s video nazora ikada podijeljene s trećom stranom ili kojima je pristupila treća strana u svrhu pružanja neke usluge unutar EEA? Postoje li ugovori? **Ne**
    - Dodatne napomene. Navedite popis takvih trećih strana i zašto se s njima dijele podaci.
    - Lokacija te treće strane
15. Pitanje
    - Jesu li snimke s video nadzora podijeljene s trećom stranom ili im pristupa treća strana u svrhu potpore izvan EEA? Postoje li ugovori? **Ne**

- Dodatne napomene. Navedite popis takvih trećih strana izvan EEA i zašto se s njima dijele podaci."
- Lokacija te treće strane izvan EEA

16. Pitanje
    - Gdje se snimke video nadzora snimaju i spremaju? **Hard disk sustava**
17. Pitanje
    - Navedite općeniti opis tehničkih sigurnosnih mjera koje su trenutno na snazi : **videonadzor, evidencija ulaza, protuprovalna zaštita**
    - Kako kontrolirate i čuvate pristup i korištenje osobnih podataka povezanih s vašim nadzornim sustavom? **šifriranje**
    - Dodatne napomene. Pošaljite ili omogućite link na bilo koju dokumentaciju/pravilnik koji imate da se bavi CCTV i video nadzorom.

# 2) Raspored postavljenih kamera

**Popis kamera sustava video nadzor:**

Za svaku kameru navesti:

- Oznaka kamere: 1
- Gdje se koristi: parkiralište
- kamera je u funkciji: da

- Oznaka kamere: 2
- Gdje se koristi: ugao zgrade koji gleda na prilaz Domu (gleda na kontejnere)
- kamera je u funkciji: da

- Oznaka kamere: 3
- Gdje se koristi: ulaz u kuhinju
- kamera je u funkciji: da

- Oznaka kamere: 4
- Gdje se koristi: nadstrešnica za pušače
- kamera je u funkciji: da

- Oznaka kamere: 5
- Gdje se koristi: prostor ispred zgrade Doma, od prilaza prema ulazu u zgradu
- kamera je u funkciji: da

- Oznaka kamere: 6
- Gdje se koristi: prostor ispred zgrade Doma, od ulazu u zgradu prema izlazu iz dvorišta
- kamera je u funkciji: da

- Oznaka kamere: 7
- Gdje se koristi: ulaz u zgradu
- kamera je u funkciji: da

- Oznaka kamere: 8
- Gdje se koristi: vrt Doma
- kamera je u funkciji: da

- Oznaka kamere: 9
- Gdje se koristi: igralište
- kamera je u funkciji: da

- Oznaka kamere: 10
- Gdje se koristi: plinski spremnici
- kamera je u funkciji: da

- Oznaka kamere: 11
- Gdje se koristi: porta
- kamera je u funkciji: da

- Oznaka kamere: 12
- Gdje se koristi: hodnik ispred ulaza ravnatelja
- kamera je u funkciji: da

- Oznaka kamere: 13
- Gdje se koristi: praonica
- kamera je u funkciji: da

- Oznaka kamere: 14
- Gdje se koristi: prostor za peglanje
- kamera je u funkciji: da

- Oznaka kamere: 15
- Gdje se koristi: čajna kuhinja u prizemlju
- kamera je u funkciji: da

- Oznaka kamere: 16
- Gdje se koristi: tv sala u prizemlju
- kamera je u funkciji: da

- Oznaka kamere: 17
- Gdje se koristi: blagovaonica
- kamera je u funkciji: da

- Oznaka kamere: 18
- Gdje se koristi: kuhinja – prerada mesa
- kamera je u funkciji: da

- Oznaka kamere: 19
- Gdje se koristi: kuhinja – prostor za kuhanje
- kamera je u funkciji: da

- Oznaka kamere: 20
- Gdje se koristi: kuhinja – prostor za obradu povrća
- kamera je u funkciji: da

- Oznaka kamere: 21
- Gdje se koristi: kuhinja – ulaz u garderobu
- kamera je u funkciji: da

- Oznaka kamere: 22
- Gdje se koristi: unutarnji ulaz u kuhinju
- kamera je u funkciji: da

- Oznaka kamere: 23
- Gdje se koristi: skladište u kuhinji
- kamera je u funkciji: da

- Oznaka kamere: 24
- Gdje se koristi: stepenište ispred zbornice
- kamera je u funkciji: da

- Oznaka kamere: 25
- Gdje se koristi: ulaz u zbornicu
- kamera je u funkciji: da

- Oznaka kamere: 26
- Gdje se koristi: 1. kat desno– od učionice br. 17 prema zbornici
- kamera je u funkciji: da

- Oznaka kamere: 27
- Gdje se koristi: 1. kat desno- od učionice br.17 prema sobi 15 B
- kamera je u funkciji: da

- Oznaka kamere: 28
- Gdje se koristi: 1. kat desno – od sanitarija desno prema učionici br. 17
- kamera je u funkciji: da

- Oznaka kamere: 29
- Gdje se koristi: 1. kat lijevo – od učionice br. 21 prema zbornici
- kamera je u funkciji: da

- Oznaka kamere: 30
- Gdje se koristi: 1. kat lijevo – od učionice br. 21 prema sobi 24B
- kamera je u funkciji: da

- Oznaka kamere: 31
- Gdje se koristi: knjižnica
- kamera je u funkciji: da

- Oznaka kamere: 32
- Gdje se koristi: fitness sala
- kamera je u funkciji: da

- Oznaka kamere: 33
- Gdje se koristi: 1. kat lijevo - od sanitarija lijevo prema učionici br.21
- kamera je u funkciji: da

- Oznaka kamere: 34
- Gdje se koristi: 2. kat – stepenište ispred sobe 30
- kamera je u funkciji: da

- Oznaka kamere: 35
- Gdje se koristi: 2. kat desno – od tv sale prema sobi 31
- kamera je u funkciji: da

- Oznaka kamere: 36
- Gdje se koristi: 2. kat desno – od tv sale prema sobi 35A
- kamera je u funkciji: da

- Oznaka kamere: 37
- Gdje se koristi: 2. kat desno -od sanitarija desno prema tv sali
- kamera je u funkciji: da

- Oznaka kamere: 38
- Gdje se koristi: 2. kat lijevo – od učionice 46 prema sobi 30
- kamera je u funkciji: da

- Oznaka kamere: 39
- Gdje se koristi: 2. kat lijevo – od učionice 46 prema sobi 44
- kamera je u funkciji: da

- Oznaka kamere: 40
- Gdje se koristi: 2. kat lijevo – od sanitarija lijevo prema učionici 46
- kamera je u funkciji: da

- Oznaka kamere: 41
- Gdje se koristi: 3. kat – desno – od sobe 57 prema stepeništu
- kamera je u funkciji: da

- Oznaka kamere: 42
- Gdje se koristi: 3. kat desno – od sobe 57 prema sobi 55
- kamera je u funkciji: da

- Oznaka kamere: 43
- Gdje se koristi: 3. kat desno – čajna kuhinja i soba 54
- kamera je u funkciji: da

- Oznaka kamere: 44
- Gdje se koristi: 3. kat lijevo – od sobe 67 prema stepeništu
- kamera je u funkciji: da

- Oznaka kamere: 45
- Gdje se koristi: 3. kat lijevo – od sobe 66 prema stepeništu
- kamera je u funkciji: da

- Oznaka kamere: 46
- Gdje se koristi: 3. kat lijevo – od sobe 66 prema sanitarijama
- kamera je u funkciji: da

- Oznaka kamere: 47
- Gdje se koristi: 3. kat lijevo – od sanitarija prema sobi 66
- kamera je u funkciji: da

- Oznaka kamere: 48
- Gdje se koristi: iznad ulaza u zgradu, gleda na dvorište ispred ulaza
- kamera je u funkciji: da

**Izvadak iz Projekta izvedenog stanja** (Pravilnik o uvjetima i načinu provedbe tehničke zaštite članak 4) s tlocrtima i ucrtanim pozicijama kamera.

# 3) Tehnička specifikacija kamera i cjelovitog sustava video nadzora

Sukladno Pravilniku o uvjetima i načinu provedbe tehničke zaštite članak 4 dokumentacija koju treba isporučiti ovlašteni izvođač radova i koju treba uvrstiti u ovaj prilog je slijedeća:

1. Snimka postojećeg stanja štićenog objekta i analiza problema s ocjenom
2. Prosudba ugroženosti
3. Sigurnosni elaborat
4. Definicija projektnog zadatka
5. Projekt sustava tehničke zaštite
6. Zapisnik izvedbe sustava tehničke zaštite
7. Ovjera od strane stručnog nadzora nad izvedbom radova
8. Zapisnik o obavljenom tehničkom prijamu sustava video nadzora
9. Plan održavanja i servisiranja sustava tehničke zaštite
10. Procedura s uputama za uporabu sustava video nadzora

# 5) Primijenjene sigurnosne mjere

- **Fizičke mjere zaštite kamera – kamere su postavljene na visini te im se ne može lako pristupiti; kamere su antivandal (otporne na udarce)**
- **Fizičke mjere zaštite računalnog sustava snimanja – prostorije su pod ključem**
- **Fizičke mjere zaštite ulaska u prostor – zaključana vrata, vratar, alarm**
- **Fizičke mjere zaštite prijenosnih medija koji sadrže snimke uključujući backup - /**
- **Informatičke mjere zaštite računalnog sustava snimanja – firewall, lozinke**
- **Informatičke mjere zaštite prijenosnih medija koji sadrže snimke uključujući backup - /**
- **Informatičke mjere zaštite prijenosa slike od kamere do sustava - firewall**

# 6) Registar zadržavanja i prijenosa podataka

Registar zadržavanja i prijenosa podataka sadrži zapise koji nastaju u svakom dijelu životnog ciklusu osobnog podatka koji je prikupljen korištenjem sustava video nadzora. Meta podaci koji se pri tome zapisuju su sljedeći:

- Datum i vrijeme nastanka zapisa
- Autor zapisa
- Opis zapisa
- Kategorija zapisa (prijenos slike, stvaranje snimke, pregled snimke, izuzimanje snimke, zapis snimke na prijenosni medij, slanje medija, prijenos medija s udaljenog snimača, bežični prijenos s kamere, uništavanje zapisa i sl.)
- Prilozi

# 7) Sigurnosna politika video nadzora

Istaknute tehničke i organizacijske mjere

- istaknuta upozorenja o snimanju
- odluka odgovorne osobe o davanju ovlasti za uvid u snimke
- prijenosni mediji na kojima se nalaze snimke su enkriptirani
- svi mediji na kojima se nalaze snimke nalaze se u zaštićenom i sigurnom prostoru
- server sa snimkama je unutar zaštićene zone i nije dostupan putem interneta, nema RDP (tzv. "bastion" server)
- politika obrane servera, backup i procedura povrata backupa je na razini 3 (1-najniža / 3-najviša)
- koristi se "role based" pristup davanju ovlasti pristupa (samo gledanje žive snimke, samo pregledavanje, izuzimanje snimke)
- svaki pristup i rad sa snimkama evidentira se računalno i papirnato
- uništavanje se provodi na siguran i povjerljiv način

Jasno se određuje i dokumentira tko ima pristup do snimki video nadzora i/ili tehničke arhitekture sustava video nadzora, u koju svrhu te od čega se pravo pristupa sastoji. Posebno se određuje tko ima pravo:

- pogledati kamere u realnom vremenu
- pogledati snimljeni materijal, ili
- kopirati
- presnimiti
- brisati, ili
- mijenjati snimku

Postavljene kontrole informacijske sigurnosti za sustav video nadzora grupirane su prema ISO27002.

Napomena: predložene kontrole potrebno je prilagoditi stvarnoj situaciji i specifičnostima sustava video nadzora.

**A.5 Politika informacijske sigurnosti**

A.5.1.1 Politika informacijske sigurnosti odobrena je od strane Domskog odbora dana 20.06.2018. godine.

A.5.1.2 Provjera politika informacijske sigurnosti provodi se najmanje jednom godišnje.

**A.6 Organizacija informacijske sigurnosti**

A.6.1.1 Uloge i odgovornosti za informacijsku sigurnost sustava video nadzora su dodijeljene pojedincima i oni su toga svjesni.

A.6.1.2 Izvršena je raspodjela dužnosti i utvrđene su osobe koje su odgovorne za sigurnost sustava video nadzora i one su toga svjesne

A.6.1.3 Kontakti s nadležnim tijelima

A.6.1.4 Kontakti s posebnim interesnim grupama

A.6.1.5 Informacijska sigurnost u upravljanju projektima

**A.7 Sigurnost ljudskih resursa**

A.7.1.1 Provjera kandidata

A.7.1.2 Trajanje i uvjeti zaposlenja

A.7.2.1 Odgovornosti uprave

A.7.2.2 Podizanje svijesti i edukacija o informacijskoj sigurnosti

A.7.2.3 Disciplinski proces

A.7.3.1 Prekid ili promjena odgovornosti

**A.8 Upravljanje imovinom**

A.8.1.1 Registar imovine

A.8.1.2 Vlasništvo nad imovinom

A.8.1.3 Prihvatljiva uporaba imovine

A.8.1.4 Povratak imovine

A.8.2.1 Klasifikacija informacija

A.8.2.2 Označavanje informacija

A.8.2.3 Rukovanje imovinom

A.8.3.1 Upravljanje uklonjivim medijima

A.8.3.2 Odbacivanje medija

A.8.3.3 Prijenos fizičkih medija

**A.9 Kontrola pristupa**

A.9.1.1 Politika kontrole pristupa

A.9.1.2 Pristup mrežama i mrežnim servisima

A.9.2.1 Registracija i deregistracija korisnika

A.9.2.2 Dodjela korisničkih prava

A.9.2.3 Upravljanje privilegiranim pravimma za pristup

A.9.2.4 Upravljanje tajnim autentikacijskim informacijama korisnika

A.9.2.5 Provjera korisničkih prava pristupa

A.9.2.6 Uklanjanje ili prilagodba korisničkih prava pristupa

A.9.3.1 Upotreba tajnih autentikacijskih informacija

A.9.4.1 Ograničenja pristupa informacijama

A.9.4.2 Procedure za siguran log-on

A.9.4.3 Sustav upravljanja zaporkama

A.9.4.4 Korištenje privilegiranih pomoćnih programa

A.9.4.5 Kontrola pristupa izvornom kodu programa

**A.10 Kriptografija**

A.10.1.1 Politika uporabe kriptografskih kontrola

A.10.1.2 Upravljanje ključevima

**A.11 Fizička i sigurnost okruženja**

A.11.1.1 Perimetar fizičke sigurnosti

A.11.1.2 Fizičke kontrole ulaza

A.11.1.3 Osiguranje ureda, prostorija i opreme

A.11.1.4 Zaštita od vanjskih prijetnji i prirodnih nepogoda

A.11.1.5 Rad u sigurnim područjima

A.11.1.6 Područja za isporuku i utovar

A.11.2.1 Smještaj i zaštita opreme

A.11.2.2 Pomoćna oprema i servisi

A.11.2.3 Sigurnost ožičenja

A.11.2.4 Održavanje opreme

A.11.2.5 Uklanjanje imovine

A.11.2.6 Sigurnost opreme i imovine izvan prostora organizacije

A.11.2.7 Sigurno odbacivanje i ponovno korištenje opreme

A.11.2.8 Korisnička oprema bez nadzora

A.11.2.9 Politika čistog stola i praznog zaslona

**A.12 Sigurnost operacija**

A.12.1.1 Dokumentirane operativne procedure

A.12.1.2 Upravljanje promjenom

A.12.1.3 Upravljanje kapacitetom

A.12.1.4 Razdvajanje razvojnog, testnog i produkcijskog okruženja

A.12.2.1 Kontrole protiv zlođudnih programa

A.12.3.1 Sigurna pohrana informacija

A.12.4.1 Logiranje događaja

A.12.4.2 Zaštita log informacija

A.12.4.3 Logovi administratora i operatera

A.12.4.4 Sinkronizacija satova

A.12.5.1 Instalacija softvera na operativne sustave

A.12.6.1 Upravljanje tehničkim ranjivostima

A.12.6.2 Ograničenja instalacije softvera

A.12.7.1 Kontrole audita informacijskih sustava

**A.13 Sigurnost komunikacija**

A.13.1.1 Mrežne kontrole

A.13.1.2 Sigurnost mrežnih usluga
A.13.1.3 Segregacija u mrežama
A.13.2.1 Politike i procedure za prijenos informacija
A.13.2.2 Ugovori o prijenosu informacija
A.13.2.3 Elektroničke poruke
A.13.2.4 Ugovori o povjerljivosti

**A.14 Nabavka, razvoj i održavanje sustava**

A.14.1.1 Analiza i specifikacija sigurnosnih zahtjeva
A.14.1.2 Osiguranje aplikativnih servisa na javnim mrežama
A.14.1.3 Zaštita transakcija aplikativnih servisa
A.14.2.1 Politika sigurnog razvoja
A.14.2.2 Procedure za kontrolu promjena na sustavu
A.14.2.3 Tehnička provjera aplikacija nakon promjena operativne platforme
A.14.2.4 Ograničenja promjena softverskih paketa
A.14.2.5 Principi sigurnog sistem inženjeringa
A.14.2.6 Sigurno razvojno okruženje
A.14.2.7 Eksternalizirani razvoj
A.14.2.8 Testiranje sigurnosti sustava
A.14.2.9 Testiranje prihvatljivosti sustava
A.14.3.1 Zaštita testnih podataka

**A.15 Odnosi s dobavljačima**

A.15.1.1 Politika informacijske sigurnosti u odnosima s dobavljačima
A.15.1.2 Adresiranje sigurnosti u ugovorima s dobavljačima
A.15.1.3 Lanac dobavljača informacijske i komunikacijske tehnologije
A.15.2.1 Nadzor i provjera usluga dobavljača
A.15.2.2 Upravljanje promjenama u uslugama dobavljača

**A.16 Upravljanje incidentima informacijske sigurnosti**

A.16.1.1 Odgovornosti i procedure
A.16.1.2 Prijavljivanje događaja informacijske sigurnosti
A.16.1.3 Prijavljivanje slabosti informacijske sigurnosti
A.16.1.4 Procjena i odlučivanje o događajima informacijske sigurnosti
A.16.1.5 Odgovor na incidente informacijske sigurnosti
A.16.1.6 Učenje na incidentima informacijske sigurnosti
A.16.1.7 Prikupljanje dokaza

**A.17 Aspekti informacijske sigurnosti u upravljanju kontinuitetom poslovanja**

A.17.1.1 Planiranje kontinuiteta informacijske sigurnosti

A.17.1.2 Implementacija kontinuiteta informacijske sigurnosti

A.17.1.3 Verifikacija, pregled i evaluacija kontinuiteta informacijske sigurnosti

A.17.2.1 Raspoloživost opreme za obradu informacija

**A.18 Sukladnost**

A.18.1.1 Identifikacija primjenjivih pravnih i ugovornih zahtjeva

A.18.1.2 Prava intelektualnog vlasništva

A.18.1.3 Zaštita zapisa

A.18.1.4 Privatnost i zaštita osobnih informacija

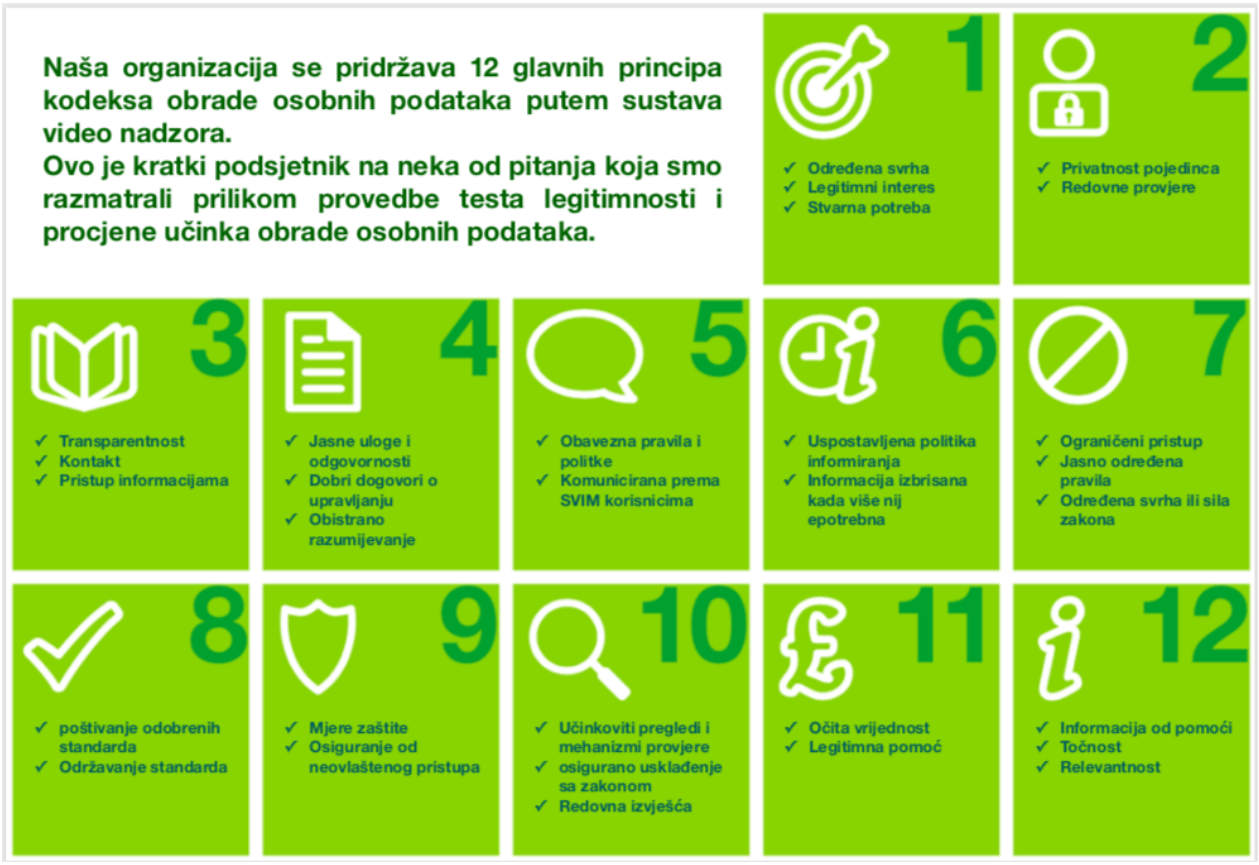
A.18.1.5 Reguliranje kriptografskih kontrola

A.18.2.1 Neovisan pregled informacijske sigurnosti

A.18.2.2 Sukladnost sa sigurnosnim politikama i standardima

A.18.2.3 Pregled tehničke sukladnosti

## 12) Infografika 12 principa



# 13) Procjena opravdanosti legitimnog interesa za obradu osobnih podataka u svrhu video nadzora (LIA)

Procjena legitimnog interesa (LIA)

Napomena: ukoliko je zakonitost obrade zasnovana na legitimnom interesu, tada je potrebno provesti i dokumentirati procjenu opravdanosti legitimnog interesa (LIA) kako bi se donijela odluka je li moguće koristiti legitimni interes kao pravnu osnovu svrhe obrade.

Korak 1: Test svrhovitosti

Potrebno je procijeniti postoji li legitiman interes za obradom:

- Zašto želite obraditi podatke?
- Koje prednosti očekujete od obrade?
- Imaju li treće strane koristi od obrade?
- Postoji li širi javni interes za obradu?
- Koliko su važne prednosti koje ste identificirali?
- Koji bi bio utjecaj ako ne možete nastaviti s obradom?
- Pridržavate li se nekih posebnih pravila o zaštiti podataka koja se primjenjuju na vašu obradu (npr. Zahtjevi za profiliranje ili e-privatnost)?
- Pridržavate li se drugih relevantnih zakona?
- Jesu li u skladu s industrijskim smjernicama ili kodeksom ponašanja?
- Postoje li neki drugi etički problemi s obradom?

Korak 2: Test neophodnosti

Potrebno je procijeniti je li obrada neophodna u svrhu koju ste identificirali.

- Hoće li ta obrada stvarno pomoći da postignete njezinu svrhu?
- Je li obrada razmjerna svrsi?
- Možete li postići istu svrhu bez obrade?
- Možete li postići istu svrhu obrađivanjem manje podataka ili obradom podataka na očitiji ili manje nametljiv način?

Korak 3: Test ravnoteže

Morate razmotriti utjecaj na interese i prava i slobode pojedinaca i procijeniti je li to prešlo vaše legitimne interese.

Prvo provedite procjenu potrebe za DPIA. Ako bilo koji kriterij na toj procjeni bude pozitivan, provedite DPIA umjesto detaljnije procjene rizika.

Priroda osobnih podataka

- Je li to posebna kategorija podataka ili podaci o kaznenim djelima?
- Jesu li to podaci koje će ljudi vjerojatno smatrati osobito "privatnima"?
- Obrađujete li podatke o djeci ili podatke drugih ranjivih skupina?
- Jesu li to osobni ili profesionalni podaci o pojedinoj osobi?

Razumna očekivanja

- Imate li već postojeći odnos s ispitanikom?
- Koja je priroda tog odnosa i kako ste ranije koristili te podatke?
- Jeste li podatke prikupili izravno od ispitanika? Što ste im tada rekli?
- Ako ste dobili podatke od treće strane, što su oni rekli ispitaniku o daljnjoj uporabi kod treće strane za druge svrhe i je li to odgovara i za vašu obradu?
- Koliko ranije ste prikupili podatke? Postoje li od tada kakve promjene u tehnologiji ili sadržaju obrade što bi moglo utjecati na očekivanja ispitanika?
- Je li vaša svrha i način obrade razumljiva svima?
- Namjeravate li učiniti nešto novo ili inovativno?
- Imate li kakvih pokazatelja o očekivanjima - npr. kroz istraživanje tržišta, specijalističke grupe ili neke druge informativne oblike?
- Postoje li drugi čimbenici u konkretnim okolnostima, koji pokazuju da bi ispitanici očekivali ili ne bi očekivali konkretnu obradu?

Moguće posljedice

- Koji su mogući utjecaji obrade na ispitanika?
- Hoće li ispitanik izgubiti kontrolu nad upotrebom svojih osobnih podataka?
- Kolika je vjerojatnost i ozbiljnost bilo koje moguće posljedice?
- Postoji li mogućnost da neki ljudi daju prigovor na obradu ili da ju smatraju neprikladnom?
- Jeste li spremni objasniti obradu ispitanicima?
- Možete li primijeniti bilo kakve zaštitne mjere kako biste smanjili moguće posljedice?
- Možete li ponuditi pojedincima izuzimanje od obrade? Da / Ne

Odlučivanje

Ovdje donesite zaključak na osnovu odgovora iz prethodna tri koraka, kako biste odlučili možete li koristiti legitimni interes kao pravnu osnovu svoje obrade.

Možete li se osloniti na legitimni interes kao pravnu osnovu obrade? Da / Ne

Imate li dodatnih komentara koji će potkrijepiti vaše odgovore?

Ime i prezime autora LIA testa

datum

napomena

# 14) Procjena učinka na zaštitu podataka (PIA)

Sukladno GDPR Članak 35 AZOP je donio slijedeću Odluku provođenja DPIA u slijedećim obradama:

Na temelju članka 35. stavka 4. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), članka 1. i 4. Zakona o provedbi Opće uredbe o zaštiti podataka (Narodne novine br. 42/18), članka 12. Statuta Agencije za zaštitu osobnih podataka te uzimajući u obzir Smjernice o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679 (WP 248 rev. 01) donesene 4. travnja 2017. godine, te posljednji put revidirane i donesene 4. listopada 2017. godine i Mišljenje Europskog odbora za zaštitu podataka 25/2018 na nacrt popisa Agencije za zaštitu osobnih podataka o vrstama postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka ravnatelj Agencije za zaštitu osobnih podataka donio je

ODLUKU o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka.

Pored slučajeva predviđenih člankom 35. stavkom 3. Opće uredbe o zaštiti podataka, uzimajući u obzir izuzetak predviđen u članku 35. stavku 10. Opće uredbe o zaštiti podataka, provedba procjene učinka na zaštitu osobnih podataka obvezna je uz ostalo i kod obrade osobnih podataka u sljedećim slučajevima:

- Obrada osobnih podataka korištenjem sustavnog nadzora javno dostupnih mjesta u velikom opsegu (video nadzor koji obuhvaća npr. kolodvore, autobuse, ulaze u poslovne zgrade i sl.)
- Uporaba novih tehnologija ili tehnoloških rješenja za obradu osobnih podatka ili sa mogućnošću obrade osobnih podataka (npr. primjena „interneta stvari", poput pametnih televizora, pametnih kućanskih aparata, komunikacijski povezanih igračaka, sustava „pametni gradovi", pametnih mjerača energije, itd.) koji služe za analizu ili predviđanje ekonomske situacije, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja fizičkih osoba; (videonadzor koji obuhvaća korištenje dronova za potrebe snimanja ili stalne kamere u vozilima ("dash cams")
- Obrada osobnih podataka na način koji uključuje praćenje lokacije ili ponašanja pojedinca u slučaju sustavne obrade komunikacijskih podataka (metapodaci) nastalih uporabom telefona, interneta ili drugih komunikacijskih kanala, kao što je GSM, GPS, Wi Fi, praćenje ili obrada podataka o lokaciji; (metapodaci o videonadzoru poput IP adrese, GSM pozicije vozila u pokretu i sl.)
- Obrada osobnih podataka zaposlenika uporabom aplikacija ili sustava za praćenje (npr. kao što je obrada osobnih podatka za praćenje rada, kretanja, komunikacije i sl.).

Napomena: Predložena metodologija izrade procjene učinka rađena je po predlošku CNIL i ICO te je dostupna kao zasebni dokument - predložak.

Sadržajno se u njemu nalaze slijedeće teme:

1 Analiza sadržaja obrade

1.1 Pregled obrade

1.1.1 Opis promatrane obrade podataka

1.1.2 Specifični standardi koji se primjenjuju obzirom na narav obrade

1.2 Podaci, postupci i potrebna sredstva

1.2.1 Opis podataka, primatelji i trajanje pohrane

1.2.2 Opis obrada i potrebnih sredstava

2 Analiza načela obrade

2.1 Procjena kontrola koje jamče proporcionalnost i nužnost obrade

2.1.1 Pojašnjenje i obrazloženje zakonitosti obrade

2.1.2 Pojašnjenje i obrazloženje smanjenje količine podataka5

2.1.3 Pojašnjenje i obrazloženje kvalitete podataka

2.1.4 Pojašnjenje i obrazloženje trajanja pohrane

2.1.5 Procjena kontrola

2.2 Procjena kontrola koje štite prava ispitanika

2.2.1 Određivanje i opis kontrola za pružanje informacija ispitaniku

2.2.2 Određivanje i opis kontrola za dobivanje privola

2.2.3 Određivanje i opis kontrola prava pristupa i prenosivosti podataka

2.2.4 Određivanje i opis kontrola prava na ispravak i brisanje

2.2.5 Određivanje i opis kontrola prava na ograničenje obrade i prigovora

2.2.6 Određivanje i opis kontrola koje se primjenjuju na izvršitelja obrade

2.2.7 Određivanje i opis kontrola koje se primjenjuju na izvršitelja obrade

2.2.8 Procjena kontrola

3 Analiza rizika informacijske sigurnosti

3.1 Procjena sigurnosnih kontrola

3.1.1 Opis i procjena provedenih kontrola za tretiranje rizika vezanih uz sigurnost podataka

3.1.2 Opis i procjena općih sigurnosnih kontrola

# 15) Pohrana podataka (video snimke)

Osobni podaci prikupljeni prilikom obrade sustava video nadzora čuvaju se sukladno politici informacijske sigurnosti za sustav video nadzora u slijedećim rokovima:

- Dokumenti koji su nastali tijekom obrada (odluke, evidencije, zapisnici, očevidnici, izvješća i sl.) čuvaju se 2 godine nakon datuma nastanka, osim ukoliko se ne koriste u druge svrhe predviđene Politikom.
- Snimka pohranjena s kamere sustava video nadzora čuva se najdulje 6 mjeseci, osim ako to tehnički kapaciteti uređaja ne dozvoljavaju te se iste brišu po FIFO principu.
- Snimka koja je izuzeta iz sustava te je pohranjena na zasebnom vanjskom mediju ili kao zasebna datoteka na hard disku servera čuva se 2 godine osim ukoliko se ne koristi u druge svrhe predviđene Politikom.
- Registar zadržavanja i pohrane čuva se doživotno.

# 16) Evidencija aktivnosti obrade (video nadzora)

Evidencija aktivnosti obrade treba sadržavati najmanje sljedeće podatke o samoj obradi:

- Kategorije osobnih podataka
- Svrha obrade
- Zakonitost obrade
- Kategorije ispitanika
- Kategorije primatelja
- Vrijeme pohrane
- Tehničke i organizacijske mjere

Obrada osobnih podataka prikupljenih putem sustava video nadzora sastoji se od slijedećih aktivnosti:

a) praćenje u živo kamera koje čine sustav video nadzora
b) pregledavanje snimke od strane ovlaštene osobe
c) izuzimanje snimke od strane ovlaštene osobe
d) uništavanje snimke od strane ovlaštene osobe
e) tehničko održavanje sustava

| | |
|---|---|
| Kategorije osobnih podataka | • osnovni podaci ispitanika poput imena, prezimena<br>• kontakt podaci ispitanika poput adresa stanovanja, email, telefon<br>• identifikacijski podaci ispitanika poput OIB, broj osobne iskaznice, broj policijske značke<br>• ostali podaci poput tvrtka iz koje dolazi |
| Svrha obrade | zaštita osoba i imovine |
| Zakonitost obrade | legitimni interes voditelja obrade (vidi LIA) |
| Kategorije ispitanika | zaposlenik, posjetitelj, učenik |
| Kategorije primatelja | MUP RH, Sud RH |
| Vrijeme pohrane | 2 godine dokumentacija, do 6 mjeseci snimke |
| Tehničke i organizacijske mjere | • istaknuta upozorenja o snimanju<br>• odluka odgovorne osobe o davanju ovlasti za uvid u snimke<br>• prijenosni mediji na kojima se nalaze snimke su enkriptirani |

| | |
|---|---|
| | • svi mediji na kojima se nalaze snimke nalaze se u zaštićenom i sigurnom prostoru<br>• server sa snimkama je unutar zaštićene zone i nije dostupan putem interneta, nema RDP (tzv. "bastion" server)<br>• politika obrane servera, backup i procedura povrata backupa je na razini 3 (1-najniža / 3-najviša)<br>• koristi se "role based" pristup davanju ovlasti pristupa (samo gledanje žive snimke, samo pregledavanje, izuzimanje snimke)<br>• svaki pristup i rad sa snimkama evidentira se računalno i papirnato<br>• uništavanje se provodi na siguran i povjerljiv način |

# 17) SOP održavanje sustava video nadzora

Ovaj dokument sadrži opis standardne operativne procedure za redovno održavanje sustava video nadzora usklađeno s Općom uredbom o zaštiti podataka EU 2016/679.

1. Sustav video nadzora čine komponente koje su opisane u prilogu "Tehnička specifikacija kamera i cjelovitog sustava video nadzora "
   1.1. Predmet održavanja je cjelokupni sustav video nadzora
2. Održavanje može biti redovito i izvanredno:
   2.1. redovito održavanje je planirano i obavlja se najmanje jednom godišnje
   2.2. izvanredno održavanje se obavlja u slučaju tehničkog incidenta na sustavu video nadzora
3. Sustav održava osoba koja je ovlaštena za uvid u sustav ili pod nadzorom ovlaštene osobe.
   3.1. o postupku održavanja sastavlja se zapisnik koji će posebno specificirati postupke i osobe koje su sudjelovale u popravku i koji ulazi u Registar zadržavanja i prijenosa
4. Održavanje sustava može biti povjereno trećoj strani
   4.1. Zbog tehničke prirode sustava i rizika po prava i slobodu pojedinaca koje može snimiti sustav video nadzora, treća strana koja obavlja poslove održavanja smatra se izvršiteljem obrade
   4.2. S izvršiteljem obrade sklopit će se ugovor o obradi podataka koji sadrži elemente obvezujuće povjerljivosti (tzv. DPA i NDA); obvezujući dijelovi tog ugovora nalaze se u prilogu "Ugovor o obradi podataka s tvrtkom za održavanje sustava video nadzora"
5. Niti jedna komponenta koja može sadržavati zapise osobnih podataka posebno snimke, ne smije napustiti zaštićeni prostor u kojemu se nalazi sustav za video nadzor.
   5.1. Iznimno, ukoliko ne postoji način da se izvrši popravak ili održavanje komponenta se može prenijeti u prostore izvršitelja obrade na siguran način a popravak će se obaviti na povjerljiv način; o prijenosu se sastavlja zapisnik koji ulazi u Registar zadržavanja i prijenosa; o popravku će se sastaviti zapisnik koji će posebno specificirati postupke i osobe koje su sudjelovale u popravku
   5.2. Iznimno, ukoliko komponentu nije moguće popraviti, treba poduzeti svaku razumnu mjeru kako bi se osobni podaci na njoj uništili; o tome se sastavlja zapisnik koji ulazi u Registar zadržavanja i prijenosa; komponenta se upućuje na uništavanje prema propisanoj proceduri o uništavanju snimke

# 18) SOP uvid u video snimke

Ovaj dokument sadrži opis standardne operativne procedure za uvid u snimke učinjene sustavom video nadzora usklađeno s Općom uredbom o zaštiti podataka EU 2016/679.

1. Svaka osoba - ispitanik - koja opravdano vjeruje da je snimljena sustavom video nadzora ima pravo zatražiti uvid u snimku.
   1.1. Zahtjev za uvid u snimku sadrži: datum podnošenja zahtjeva, kontakt podatke i identifkacijske podatke, nedavnu fotografiju osobe i podatke koji određuju vrijeme, mjesto i okolnosti snimke.
   1.2. Nakon pripreme snimke, ovlaštena osoba dogovara uvid i obavlja prezentaciju isječka snimke ispitaniku
2. Uvid u snimku obavlja osoba koja ima valjanu ovlast odgovorne osobe voditelja obrade.
   2.1. Odmah po zaprimanju zahtjeva za uvidom, ovlaštena osoba izuzima traženi period snimke kako bi osigurala istu od uništavanja.
   2.2. Pretragom se utvrđuje identitet osobe na snimci
   2.3. Osigurava se zaštita privatnosti drugih osoba na snimci
   2.4. Bilježi se točni period koji sadrži snimku osobe
   2.5. Zabilježeni isječak se pohranjuje u posebnu datoteku na hard disku servera radi dokumentiranja i prezentiranja ispitaniku
3. U slučaju kada policija ili sud traži uvid u snimku, potrebno je provesti jednaku proceduru uz predočenje identifikacije službene osobe i kopije službenog naloga

# 19) SOP izdavanje video snimke

Ovaj dokument sadrži opis standardne operativne procedure za izdavanje snimke učinjene sustavom video nadzora na prijenosnom mediju usklađeno s Općom uredbom o zaštiti podataka EU 2016/679.

1. Svaka osoba - ispitanik - koja opravdano vjeruje da je snimljena sustavom video nadzora ima pravo zatražiti prijenos isječka snimke na kojoj se nalazi na prijenosni medij.
   1.1. Prije toga potrebno je da ispitanik prođe proceduru uvida u video snimku
   1.2. Ispitanik na zahtjevu za uvid označava i rubriku da želi snimku na prijenosnom mediju
2. Ovlaštena osoba pohranjenu snimku presnimi i uruči ispitaniku ili službenoj osobi
   2.1. o predaji medija bilježi se zapisnik koji sadrži podatke sa Zahtjeva za uvidom i podatke o isječku (vrijeme i mjesto nastanka, početak i trajanje zapisa, komentar ima li drugih osoba na snimci)
   2.2. u registar zadržavanja i prijenosa zapisuje se taj događaj i prilaže zapisnik
3. Policija ili sud imaju pravo zatražiti snimku te se provodi ista procedura kao i kod ispitanika

# 20) SOP uništavanje snimke i ostalih podataka nastalih unutar sustava video nadzora

Definicije:

Footage# - jedinstveni broj koji označava pojedinačnu snimku; ukoliko se dio snimke izuzima, taj dio snimke dobiva novi Footage# broj koji se sastoji od izvornog i dodatka u obliku GGMMDDHHMM koji označava vrijeme izuzimanja snimke ([Footage#]-[GGMMDDHHMM]).

Medij - papirnata dokumentacija, diskovi, magnetne trake, video ili mikro filmovi koji sadrže osobne podatke ispitanika prikupljene putem sustava video nadzora

Batch# - jedinstveni broj koji označava jedan ili više medija koji će biti uništeni; Batch# broj nastaje kada se jedan ili više medija koji će biti uništeni ulaže u sigurni spremnik

Lot# - jedinstveni broj koji označava jedan ili više medija koji će biti uništeni; Lot# broj nastaje kada se jedan sigurni spremnik otpremi na uništenje (koji sadrži jedan ili više Batch#)

Registar zadržavanja i prijenosa podataka - centralni registar u kojemu se bilježi svaka faza životnog ciklusa snimke odn. osobni podaci povezani sa sustavom za video nadzor

Nalog za uništavanje - dokument koji sadrži poveznicu na jedan ili više medija na kojima se nalaze osobni podaci namijenjen za uništenje

Popratnica za uništavanje - zbirni dokument koji sadrži popis medija povezan s jednim ili više Naloga poslanih na uništenje

Potvrda o povjerljivom i sigurnom uništavanju - dokument kojim se utvrđuje da su mediji dostavljeni na jednoj ili više Popratnica uništeni

Postupci:

Mediji (papirnata dokumentacija, diskovi, magnetne trake, video ili mikro filmovi) koji sadrže osobne podatke ispitanika prikupljene putem sustava video nadzora moraju biti uništeni na siguran i povjerljiv način u skladu sa DIN 66399 međunarodnom normom.

Ovlaštena osoba popunjava Nalog za uništavanje koji sadrži popis i opis medija za uništavanje s jedinstvenim brojem Batch#. Taj broj se zapisuje u Registar zadržavanja i prijenosa podataka uz svaki Footage# zapis koji se nalazi na medijima za uništavanje. Time se osigurava sljednost zapisa od njegovog nastanka do uništavanja.

Nalog za uništavanje sadrži slijedeće podatke:

- Batch#
- Broj Footage# zapisa (jedan ili više)
- Datum izdavanja

- Ovlaštena osoba
- Razlog za uništavanje
- Posebna napomena za uništavanje

Mediji namijenjeni za uništavanje pohranjuju se u sigurnosne spremnike koji su zaštićeni od neovlaštenog pristupa u prisutnosti najmanje dvije osobe od kojih je jedna Ovlaštena osoba.

Prilikom svakog pohranjivanja medija u sigurnosni spremnik unose se slijedeći podaci u Popratnicu za uništavanje:

- Batch# - koji je rastući jedinstveni broj za svako ulaganje u spremnik
- Datum pohrane
- Ovlaštena osoba
- Ostale prisutne osobe
- Posebna napomena za uništavanje

Izdan i ovjeren Nalog za uništavanje ulaže se u Registar zadržavanja i prijenosa podataka. Popratnica za uništavanje pohranjuje se na sigurno mjesto uz spremnik.

Odmah ili nakon određenog vremena, ali ne dulje od 30 kalendarskih dana, sigurnosne spremnike preuzima autorizirana osoba Tvrtke za uništavanje i prevozi osiguranim vozilima do lokacije uništavanja.

Prilikom preuzimanja autorizirana osoba Tvrtke za uništavanje ovjerava Popratnicu za uništavanje te se na istu dodaju slijedeći podaci:

- Datum preuzimanja
- Vrijeme preuzimanja
- Autorizirana osoba Tvrtke za uništavanje ime i prezime, oznaka identifikacije (broj osobne)
- Oznaka vozila
- Primjedbe (ako ih ima)

Popratnica za uništavanje sadrži popis svih Lot# koji su spremljeni u spremnik te popis Footage# (medija) koji se nalaze u njemu s datumom ulaganja i preuzimanja.

Ovjerena Popratnica se kopira. Jedan primjerak uzima autorizirana osoba dok se drugi primjerak ulaže u Registar zadržavanja i prijenosa podataka.

Uništavanje se provodi kroz zatvorene sigurnosne sustave za uništavanje (sigurnosni nivo 3) različitih veličina za sve medije (papirnata dokumentacija, diskovi, magnetne trake, video ili mikro filmovi).

Svaki nivo procesa uništavanja se mora dokumentirati. Na zahtjev, Tvrtka za uništavanje mora biti u mogućnosti dostaviti tu dokumentaciju.

Nakon završenog procesa uništavanja, potrebno je izdati Potvrdu o povjerljivom i sigurnom uništavanju koja je usklađena sa važećom zakonskom regulativom i u skladu sa DIN 66399 međunarodnom normom te povezana s Popratnicom za uništavanje.

Izdana Potvrda s Popratnicom za uništavanje se ulaže u Registar zadržavanja i prijenosa podataka

Uništeni materijal se na primjeren način mora zbrinuti a prema mogućnostima i reciklirati. Posebno, izrezani, otpadni papir treba biti recikliran.

U roku od 30 dana nakon donošenja Politike, sklopit će se Ugovor s tvrtkom za ovlašteno uništavanje podataka kojim će se regulirati obavljanje sigurnog i povjerljivog uništavanja medija koji sadrže osobne podatke ispitanika prikupljene putem sustava video nadzora usklađen s GDPR.

U smislu GDPR, Tvrtka za ovlašteno uništavanje podataka je izvršitelj obrade.

# 21) SOP poštivanje prava ispitanika prilikom incidenta u sustavu video nadzora

Ovaj dokument sadrži opis standardne operativne procedure za poštivanje prava ispitanika prilikom incidenta u sustavu video nadzora usklađeno s Općom uredbom o zaštiti podataka EU 2016/679.

1. Incident u sustavu video nadzora je svaki događaj koji nije planiran ili nije očekivan.
   1.1. voditelj obrade može sastaviti popis događaja koji su planirani i očekivani kao i popis događaja koji svakako predstavljaju incident
2. Kada dođe do incidenta gubitka osobnih podataka potrebno je odmah pokrenuti proceduru odgovara na incident sukladno politici informacijske sigurnosti (SOP postupanje u slučaju incidenta nije u prilogu ove Politike).
   2.1. o incidentu treba bez odlaganja obavijestiti službenika za zaštitu podataka
3. U slučaju gubitka osobnih podataka u vidu medija na kojemu se nalaze osobni podaci:
   3.1. kada su ti podaci enkriptirani (kako to traže mjere informacijske sigurnosti) tada se o incidentu sastavlja zapisnik koji ulazi u Registar. Nije potrebno obavijestiti AZOP.
   3.2. kada podaci nisu enkriptirani, tada se o incidentu sastavlja zapisnik koji ulazi u Registar i o istome treba obavijestiti AZOP korištenjem obrasca Izvješće o povredi osobnih podataka dostupno na https://azop.hr/info-servis/detaljnije/izvjesce-o-povredi-osobnih-podataka.
4. Ovlaštena osoba zajedno sa službenikom za zaštitu podataka obavlja procjenu rizika te donosi odluku o potrebi obavještavanja ispitanika čiji su osobni podaci kompromitirani
   4.1. u slučaju visokog rizika po ispitanika i ukoliko postoje razumni načini da se utvrdi identitet ispitanika tada ga treba obavijestiti na primjeren način (dostupnim kontakt podacima ili javnom informacijom)

# 22) Dodatak SOP odgovor na zahtjev ispitanika

Ovaj dokument sadrži opis standardne operativne procedure za odgovor na postavljeni zahtjev ispitanika čiji se osobni podaci obrađuju u sustavu video nadzora usklađeno s Općom uredbom o zaštiti podataka EU 2016/679.

1. Prilikom postavljanja zahtjeva, ispitanik mora utvrditi vrijeme i lokaciju jedne ili više kamera na koje se odnosi njegov zahtjev.
   1.1. Ispitanik treba u zahtjevu navesti osnovne podatke: ime i prezime, OIB te podatke za kontakt (poštanska adresa, telefon i/ili email adresa).
   1.2. Ispitanik treba uz zahtjev priložiti vlastitu nedavnu fotografiju koja će omogućiti ovlaštenoj osobi da identificira pojedinca tijekom pregleda snimke.
2. Zahtjev se prosljeđuje osobi ovlaštenoj za sustav video nadzora koja s njim postupa sukladno Politici i internim procedurama

# 23) SOP za provedbu interne provjere usklađenosti video nadzora

Ovaj dokument sadrži opis standardne operativne procedure za provedbu početne i kasnije periodičke interne provjere usklađenosti obrade osobnih podataka korištenjem sustava video nadzora s Općom uredbom o zaštiti podataka Eu 2016/679.

1. Prilikom izrade "Politike obrade osobnih podataka korištenjem sustava za video nadzor" potrebno je provesti slijedeće aktivnosti:
   1.1. Prilagoditi predloženi tekst politike vašoj organizaciji
   1.2. Prikupiti dokumentaciju izvedenog stanja video nadzora, posebno:
      1.2.1. popis i lokacije kamera s njihovim opisom i tehničkom specifikacijom
      1.2.2. popis uređaja za snimanje s njihovim opisom i tehničkom specifikacijom
   1.3. Izraditi LIA + PIA/DPIA korištenjem priloženog predloška
   1.4. Napisati i ovjeriti prijenos ovlasti
   1.5. Izraditi i postaviti naljepnice
   1.6. Izraditi i postaviti obavijesti
2. U redovnim razmacima, najmanje jadnom godišnje potrebno je provesti internu provjeru usklađenosti obrade video nadzora.
   2.1. Ukoliko provjeru ne obavlja službenik za zaštitu podataka, potrebno ga je uključiti u istu.

# 24) Zapisnik o uvidu u sustav video nadzora

Zapisnik o uvidu u sustav video nadzora sadrži:

1) Zapis u Registru
    a. datum i vrijeme uvida u snimku
    b. Footage# - jedinstvena oznaka snimke
    c. oznaka perioda snimke (početak i trajanje)
    d. napomena o drugim osobama prisutnim na snimci i poduzetim mjerama zaštite njihove privatnosti
    e. razlog uvida
    f. prisutne osobe na uvidu
    g. poduzete mjere nakon uvida (snimanje, izuzimanje, brisanje i sl.)
    h. odgovarajuća autorizacija ovlaštene osobe
2) Ukoliko je uvid rađen od strane ispitanika, tada se prilaže i Zahtjev za uvid u snimku
    a. datum podnošenja zahtjeva,
    b. kontakt podatke i
    c. identifikacijske podatke,
    d. nedavnu fotografiju osobe i
    e. podatke koji određuju vrijeme, mjesto i okolnosti snimke

# 25) Zapisnik o izuzimanju snimke video nadzora

Zapisnik o izuzimanju snimke iz sustava video nadzora sadrži:

1) Zapis u Registru
    a. datum i vrijeme uvida u snimku
    b. Footage# - jedinstvena oznaka snimke
    c. oznaka perioda snimke (početak i trajanje)
    d. napomena o drugim osobama prisutnim na snimci i poduzetim mjerama zaštite njihove privatnosti
    e. razlog izuzimanja
    f. prisutne osobe na uvidu
    g. medij na koji je snimka izuzeta (DVD, USB, hard disk i sl.)
    h. poduzete mjere zaštite medija
    i. način prijenosa / dostave medija
    j. poduzete mjere zaštite tijekom prijenosa
    k. odgovarajuća autorizacija ovlaštene osobe
2) Ukoliko je uvid rađen od strane ispitanika, tada se prilaže i Zahtjev za uvid u snimku
    a. datum podnošenja zahtjeva,
    b. kontakt podatke i
    c. identifkacijske podatke,
    d. nedavnu fotografiju osobe i
    e. podatke koji određuju vrijeme, mjesto i okolnosti snimke
3) Ukoliko je uvid rađen od strane službene osobe (policija ili sud), tada se prilaže i službeni nalog za izuzimanje snimke
    a. datum podnošenja zahtjeva,
    b. kontakt podatke i
    c. identifkacijske podatke,
    d. podatke koji određuju vrijeme, mjesto i okolnosti snimke
    e. traženi period izuzimanja
    f. kopija službenog Naloga

# 26) Zapisnik o brisanju

Zapisnik o brisanju snimke iz sustava video nadzora sadrži:

1) Zapis u Registru
    a. datum i vrijeme uvida u snimku
    b. Footage# - jedinstvena oznaka snimke
    c. oznaka perioda snimke (početak i trajanje)
    d. napomena o drugim osobama prisutnim na snimci i poduzetim mjerama zaštite njihove privatnosti
    e. razlog brisanja
    f. prisutne osobe na uvidu
    g. odgovarajuća autorizacija ovlaštene osobe