VIDEONADZOR & GDPR

Informativni vodič

Feralis Privacy Center

VIDEONADZOR I GDPR

UVOD

U današnje vrijeme brzog razvoja modernih tehnologija zahtjev za zaštitom osobnih podataka postaje jedan od temeljnih zahtjeva suvremenog društva. Opća uredba o zaštiti osobnih podataka (General Data Protection Regulation - GDPR) kao regulatorni okvir Europske unije znatno je promijenio način postupanja s osobnim podacima, dao je veća prava građanima (ispitanicima) kako bi ostvarili bolju kontrolu nad svojim podacima te istodobno nametnuo nove obveze poslovnim subjektima koji takve podatke obrađuju.

Zanimljivo pitanje povezano sa zaštitom osobnih podataka svakako je pitanje o načinu korištenja sustava video nadzora.

Kamere videonadzora danas su uobičajeni element našeg okruženja i možemo ih vidjeti gotovo svugdje od ulaska u neku od institucija, terase kafića, parkirališta, javne površine ili pak na ulazu u stambenu zgradu. Zahvaljujući sve većoj primjeni pametne videoanalitike videonadzor je postao visokoučinkovit u zaštiti ljudi i imovine. Međutim, takve tehnike mogu zadirati u privatnost u većoj mjeri (npr. složene biometrijske tehnologije) ili manjoj mjeri (npr. jednostavni algoritmi za prebrojavanje). Premda pojedinci u pravilu nemaju ništa protiv videonadzora kada je postavljen u određene sigurnosne svrhe, zbog njihove sve veće rasprostranjenosti povećava se strah od gubitka privatnosti. Nužno voditi računa da je sustav videonadzora zakonit, transparentan i u skladu s zahtjevima GDPR a ujedno se time i smanjuje bojazan od prekomjernog zadiranja u privatnost pojedinca.

ŠTO JE SVE POTREBNO UREDITI DA BI VIDEONADZOR BIO VALJAN?

Kako bi sustav videonadzora bi u skladu sa zahtjevima Opće uredbe potrebno je:

- utvrditi svrhu videonadzora
- utvrditi zakonitu osnovu za provođenje videonadzora i poduzeti mjere i postupke u skladu s tom osnovom
- provesti test razmjernosti legitimnog interesa kada se obrada temelji na toj osnovi
- utvrditi mjesto postave kamera i vrijeme praćenja

- osigurati ostvarivanje prava ispitanika
- utvrditi rok pohrane i brisanje videozapisa
- utvrditi ovlaštene osobe za pristup snimkama videonadzora
- ukoliko angažiramo zaštitarsku tvrtku radi uspostave i održavanja sustava videonadzora potrebno je sklopiti valjani ugovor kojim se uređuje obrada osobnih podataka uz prethodno utvrđivanje usklađenost postupanja izvršitelja
  u skladu sa zahtjevima GDPR istaknuti upozorenje o video nadzoru
- pružiti obavijest o obradi osobnih podataka putem videonadzora
- uspostaviti adekvatne tehničke i organizacijske mjere zaštite

ZAKONITOST PROVOĐENJA VIDEONADZORA

Obrada osobnih podataka putem videonadzora može se provoditi samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine ako ne prevladavaju interesi ispitanika koji su u suprotnosti s obradom podataka putem videonadzora.

SVRHA VIDEONADZORA → ZAŠTITA OSOBA I IMOVINE

Zakonitu osnovu za provođenje videonadzora radi zaštite osoba i imovine možemo imati u legitimnom interesu.

Međutim, Opća uredba propisuje šest zakonitih osnova za obradu

osobnih podataka te ovisno o situaciji osnovu za provođenje takvog nadzora možemo imati i u drugim osnovama. Primjerice, zakonitu osnovu možemo imati u privoli u slučaju kada npr. sportaš zatraži nadzor tijekom pojedinačnog vježbanja u svrhu analize tehnika i uspješnosti te kada je takva obrada osobnih podataka nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti.

Legitimni interes

Legitimni interes može predstavljati valjanu osnovu za provođenje videonadzora pod uvjetom da interesi ili temeljna prava i slobode ispitanika nemaju prednost, uzimajući u obzir razumna očekivanja ispitanika koja se temelje na njihovom odnosu s voditeljem obrade.

Legitiman interes voditelja obrade uistinu treba i postojati te mora upućivati na postojeći problem **(ne smije biti fiktivne ili špekulativne prirode)**.
Ono može biti opravdano stvarnom neprilikom kao što su nanesena

ZAKONITA OSNOVA → LEGITIMNI INTERES

šteta ili ozbiljan incident u prošlosti.

U skladu s načelom odgovornosti savjetuje se evidentirati relevantne incidente (zabilježiti podatke kao što je datum, način počinjenja, financijski gubitak) i povezane kaznene prijave. Takvi evidentirani incidenti mogu biti snažni dokazi o postojanju legitimnog interesa. Situacije neposredne opasnosti također mogu predstavljaju valjani legitimni interes. Takvim situacijama izložene su primjerice banke ili trgovine koje prodaju skupocjenu robu (npr. draguljarnice) ili područja poznata po čestim kaznenim djelima protiv imovine (npr. benzinske postaje).

→ STVARNA NEPRILIKA
→ SITUCIJA NEPOSREDNE OPASNOSTI

Za valjanost legitimnog interesa važno je razmotriti i razumna očekivanja ispitanika. Odlučujući kriterij treba se temeljiti na pitanju može li objektivna treća strana razumno očekivati da će biti predmet nadzora u određenoj situaciji i može li takva objektivna treća strana to zaključiti.

→ RAZUMNA OČEKIVANJA

Primjer: Klijent banke razumno može očekivati da ga se nadzire unutar banke ili za vrijeme korištenja bankomata dok isto tako neće očekivati nadzor u prostorima koji služe za opuštanje kao npr. u kinu ili restoranu.

OPRAVDANOST LEGITIMNOG INTERESA

- incidenti u prošlosti
- situacije neposredne opasnosti
- razumna očekivanja ispitanika
- test razmjernosti

Test razmjernosti

Kako bi dokazao svoj legitiman interes, prije početka same obrade, voditelj obrade bi trebao provesti test razmjernosti.

Test razmjernosti (ravnoteže) sastoji se od 7 koraka kojima je potrebno utvrditi:

1. postojanje legitimnog interesa
2. da li je obrada nužna za postizanje svrhe u koju se osobni podaci obrađuju
3. je li obrada nužna za ostvarivanje interesa zaštite osoba i imovine
4. prevladavaju li prava i slobode ispitanika nad legitimnim interesom voditelja obrade
5. zaštitne mjere
6. dokazati usklađenost sa zahtjevima Opće uredbe osigurati transparentnost obrade
7. odrediti postupanje u slučaju da osoba čiji se podaci obrađuju (ispitanik) ostvaruje svoje pravo na prigovor

Test razmjernosti je obavezan.

Postojanje legitimnog interesa te nužnost nadzora potrebno je iznova ocjenjivati u redovitim vremenskim razmacima (npr. jednom godišnje, ovisno o okolnostima).

Pravo na prigovor

Kad je riječ o videonadzoru koji se temelji na legitimnom interesu ispitanik ima pravo podnijeti prigovor. Voditelj obrade dužan je odgovoriti na svaki zahtjev ispitanika bez nepotrebnog odgađanja i u roku od najviše jednog mjeseca osim u posebnim okolnostima kada taj rok može produžiti.

Pravo na pristup osobnim podatcima

Imamo pravo od voditelja obrade zatražiti da nam se potvrdi obrađuju li se naši osobni podatci.

Ukoliko se podaci obrađuju ili se nalaze u sustavima pohrane, možemo zatražiti pristup tim podacima, dobiti informacije o obradi ali i zatražiti kopiju snimke videozapisa na kojoj se nalazimo.

MOGUĆA IZUZEĆA

Međutim, postoje i određena ograničenja radi kojih takav pristup nećemo moći ostvariti:

- onda kada ispitanik želi kopiju materijala a to bi moglo negativno utjecati na prava i slobode drugih ispitanika čiji su podatci zabilježeni u tom materijalu;
- onda kada voditelj obrade nije u mogućnosti utvrditi identitet ispitanika;
- kada na videosnimci nije moguće pretraživati osobne podatke tj. voditelj obrade vjerojatno bi trebao pregledati veliku količinu pohranjenog materijala kako bi pronašao dotičnog ispitanika ili kada ispitanika nije moguće identificirati na videozapisu;
- ako su zahtjevi ispitanika pretjerani ili očito neutemeljeni, pri tome Voditelj obrade treba moći dokazati očiglednu neutemeljenost ili pretjeranost zahtjeva.

Pravo na brisanje

Imamo pravo zatražiti brisanje svojih osobnih podataka ako su ispunjene pretpostavke za brisanje sukladno Općoj uredbi i ne postoji niti jedna od prednje navedenih iznimki.

Zamagljivanje slike bez mogućnosti retroaktivnog obnavljanja osobnih podataka koje je ta slika prethodno sadržavala, osobni podatci u skladu s Općom uredbom o zaštiti podataka smatrati će se izbrisanima.

KOJE POVRŠINE MOGU BITI OBUHVAĆENE VIDEONADZOROM I VRIJEME PROVOĐENJA

Prije uvođenja sustava kamera voditelj obrade dužan je ocijeniti na kojim su mjestima i u koje vrijeme mjere videonadzora uistinu nužne.

Videonadzorom mogu se obuhvatiti prostorije, dijelovi prostorija, vanjska površina objekta u vlasništvu odnosno najmu/zakupu voditelja obrade.

Općenito govoreći, uporaba videonadzora u svrhu zaštite objekata voditelja obrade smatra se nužnom samo unutar granica posjeda voditelja obrade.

Videonadzor ne smije obuhvaćati prostorije za odmor, osobnu higijenu i presvlačenje.

ROK POHRANE VIDEOZAPISA

Snimke video nadzornog sustava mogu se čuvati najviše do šest (6) mjeseci od dana prikupljanja
Odgovornost je voditelja obrade internim aktom utvrditi točno razdoblje zadržavanja podataka unutar navedenog roka u skladu s načelima nužnosti i proporcionalnosti te dokazati usklađenost

s odredbama Opće uredbe o zaštiti podataka.

Općenito govoreći takav rok trebao bi biti što kraći.

72 sata → 1 tjedan → MAX 6 mjeseci

Što je razdoblje pohrane dulje (posebno ako premašuje 72 sata), to će se trebati iznijeti jači dokazi o legitimnosti svrhe i nužnosti pohrane

Naravno, videozapisi mogu se čuvati i duže od maksimalnog roka pohrane ako je zakonom propisan duži rok čuvanja ili ako su dokaz u sudskom, upravnom, arbitražnom ili drugom istovrijednom postupku.

PREPORUKA

- utvrdite rok za brisanje
- prilikom utvrđivanja roka vodite se svrhom i nužnosti pohrane
- dokumentirajte utvrđivanje roka
- rokove i način utvrđivanja dobro je navesti u Politici videonadzora

TKO SMIJE PRISTUPITI SNIMKAMA VIDEONADOZRA?

Snimkama videonadzora može pristupiti odgovorna osoba tvrtke

(npr. direktor) koja provodi videonadzor (voditelja obrade) ili izvršitelja obrade (npr. zaštitarska tvrtka) i osoba koju on ovlasti.

Osobe koje pristupaju snimkama videonazora moraju biti obvezane na povjerljivost te je nužno uspostaviti automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora (tzv. logove) koji će sadržavati vrijeme i mjesto pristupa, kao i oznaku osoba koje su izvršile pristup podacima prikupljenim putem videonadzora.

- IZJAVA O POVJERLJIVOSTI
- AUTMATIZIRANI SUSTAV ZAPISA ZA EVIDENTIRANJE PRISTUPA SNIMKAMA

Zapisima videonadzora može se pristupati samo radi ostvarenje svrhe radi koje se videonadzor i provodi odnosno, radi ostvarivanja zaštite osoba i imovine kao primjerice, u slučaju provale.

Osim navedenih ovlaštenih osoba pravo pristupa podacima iz video nadzornih snimki imaju i nadležna državna tijela u okviru obavljanja poslova iz svojeg zakonom utvrđenog djelokruga (npr. policija prilikom provođenja izvida u svezi počinjenog kaznenog djela ...).

IZVRŠITELJI OBRADE (ZAŠTITARSKE TVRTKE)

Tvrtka ili druga organizacija koja provodi videonadzor u pravilu najčešće angažira zaštitarsku tvrtku za uvođenje i održavanje tog sustava. Zaštitarska tvrtka smatra se izvršiteljem obrade **s kojim je voditelj obrade u obvezi sklopiti ugovor u pisanom i elektronskom obliku** koji sadrži sve nužne klauzule o obradi osobnih podataka sukladno zahtjevima Opće uredbe. Europska komisija je u lipnju ove godine usvojila set standardnih ugovornih klauzula za upotrebu između voditelja i izvršitelja obrade.
Takvim ugovorom voditelj obrade trebao bi postići određen stupanj kontrole i sigurnosti nad obradom koju za njega provodi izvršitelj obrade.

- UGOVOR KOJIM SE UREĐUJE ZAŠTITA OSOBNIH PODATAKA IZMEĐU TVRTKE KOJA PROVODI VIDEONADZOR I ZAŠTITARSKE TVRTKE KOJA PRUŽA USLUGU VIDEONADZORA
- UGOVOR MORA BITI U PISANOM I ELEKTRONSKOM OBLIKU

Važno je imati na umu da ukoliko izvršitelj obrade (zaštitarska tvrtka) krši GDPR da i sam voditelj obrade tj. organizacija koja je angažirala zaštitarsku tvrtku može odgovarati nadzornom tijelu ali i ispitanicima u slučaju naknade štete.

Voditelj obrade dužan je angažirati samo onog izvršitelja obrade koji u dovoljnoj mjeri jamči provedbu odgovarajućih tehničkih i organizacijskih mjera zaštite na način da je obrada u skladu sa zahtjevima GDPR i da se osigurava zaštita prava ispitanika te je isto dužna redovno preispitivati.

GDPR KAZNE

Nadzorno tijelo početkom ove godine izreklo je upravnu novčanu kaznu u iznosu od pola milijuna kuna zaštitarskoj tvrtki upravo zbog nedovoljnih mjera zaštite koje su dovele do neovlaštenog otkrivanja videozapisa.

OBAVIJEST O OBRADI OSOBNIH PODATAKA PUTEM VIDEONADZORA

Mjesto koje je pokriveno videonadzorom mora biti adekvatno označeno pomoću oznake o videonadzoru da je objekt odnosno pojedina prostorija u njemu te vanjska površina objekta pod videonadzorom, a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja.

Zakonom o provedbi opće uredbe utvrđen je sadržaj oznake dok su opće obveze u pogledu *transparentnosti i dostavljanja informacija* o obradi osobnih podataka utvrđene Općom uredbom.

OBAVIJEST O OBRADI OSOBNIH PODATAKA

1. ZNAK UPOZORENJA (1. sloj)
2. OBAVIJEST O OBRADI OSOBNIH PODATAKA PUTEM VIDEONADZORA (2. sloj)

Način pružanja informacija

Uzimajući u obzir količinu informacija koja se mora dostaviti ispitaniku, voditelji obrade mogu primjenjivati višeslojni pristup.

Prvi sloj: znak upozorenja

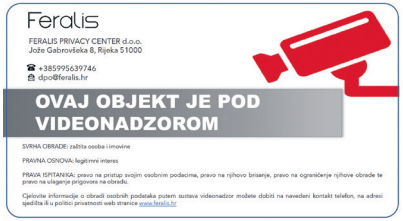
Znak upozorenja koji mora sadržavati informacije:

I.

✓da je prostor pod video nadzorom (grafička oznaka i natpis)
✓ podatke o voditelju obrade,
✓ podatke za kontakt putem kojih ispitanik može ostvariti svoja prava
✓ informacije gdje se nalazi drugi sloj informacija, odnosno cjelovite

informacije o obradi osobnih podataka putem videonadzora.

ZNAK UPOZORENJA, PRIMJER



Drugi sloj: obavijest o obradi
Drugi sloj treba sadržavati informacije o
II.
✓svrsi obrade
✓pravima ispitanika
✓kontakt podatke službenika za zaštitu podataka
✓razdoblje pohrane
✓informacije za slučaj da se podaci prenose trećim stranama, posebno ako se prenose izvan EU

Informacije drugog sloja moraju se nalaziti na mjestu koje je lako dostupno ispitaniku, na primjer, kao cjelovito navedene na informativnom letku ili politici videonadzora dostupnoj na centralnom mjestu kao na primjer na informacijskom pultu, recepciji ili blagajni ili na web stranici voditelja obrade.
Navođenje broja telefona na kojem se mogu dobiti sve informacije o obradi, također se smatra prikladnim načinom pružanja informacija.

TEHNIČKE I ORGANIZACIJSKE MJERE ZAŠTITE

Tvrtka koja provodi videonadzor (voditelj obrade) treba početi s provedbom odgovarajućih tehničkih i organizacijskih mjera povezanih sa zaštitom podataka čim postavi videonadzor – prije nego što počne prikupljati i obrađivati videosnimke.
Organizacijske i tehničke mjere zaštite moraju biti razmjerne rizicima za prava i slobode pojedinaca koji se odnose na slučajno ili nezakonito uništenje, gubitak, izmjenu i neovlašteno otkrivanje podataka dobivenih u okviru videonadzora ili pristup takvim podatcima. Voditelji obrade dužni su provoditi mjere zaštite i kako bi osigurali da se tijekom obrade poštuju sva načela zaštite podataka te utvrditi načine na koje ispitanici mogu ostvariti svoja prava utvrđena Općom uredbom.

Mjere zaštite osobnih podataka potrebno je dokumentirati te moći dokazati da se one uistinu i provode.

Organizacijske mjere zaštite

Voditelji obrade trebali bi donijeti unutarnji okvir i politike kojima se takva provedba osigurava kao što je politika videonadzora te utvrditi i provoditi postupke povezane s videonadzorom kao

što je procjena učinka na zaštitu podataka temeljem ODLUKE o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka koje je donijelo nadzorno tijelo u prosincu 2018. godine.
Osim 1. procjene učinka na zaštitu podataka, 2. izrade politike videonadzora i 3. drugih postupaka povezanih s videonadzorom (test razmjernosti u slučaju legitimnog interesa) potrebno je razmotriti i dati odgovor na slijedeća pitanja:

- tko je odgovoran za upravljanje i rukovođenje sustavom videonadzora
- svrha i opseg videonadzora
- primjerena i zabranjena uporaba (gdje i u kojim je slučajevima dopušteno odnosno nije dopušteno postavljanje videonadzora; npr. uporaba skrivenih kamera i snimanje audiosnimki uz videosnimke)
- mjere koje se odnose na transparentnost (oznaka videonazora i obavijest o obradi)
- kako se snima videosnimka i vrijeme njezina trajanja, uključujući arhivsko pohranjivanje videosnimki povezanih sa sigurnosnim incidentima
- tko mora proći odgovarajuće osposobljavanje i u kojim slučajevima
- tko ima pristup videosnimkama i u koju svrhu
- operativni postupci (npr. tko se služi videonadzorom, gdje je postavljen videonadzor, kako postupiti u slučaju povrede podataka)

- koje postupke vanjske strane moraju slijediti kako bi uspješno podnijele zahtjev za videosnimku te postupci za odbijanje i prihvaćanje takvih zahtjeva
- postupci za nabavu, postavljanje i održavanje sustava videonadzora
- upravljanje incidentima i postupci oporavka.

Tehničke mjere zaštite

Sigurnost sustava odnosi se na fizičku sigurnost svih sastavnica sustava i na cjelovitost sustava, tj. zaštitu od namjernog i nenamjernog ometanja normalnog rada sustava i otpornost na takva ometanja te kontrolu pristupa. Sigurnost podataka odnosi se na povjerljivost (podatci su dostupni samo osobama s odobrenim pristupom), cjelovitost (sprečavanje gubitka podataka ili manipulacije podatcima) i dostupnost (podatcima se može pristupiti prema potrebi).

Sigurnost sustava i podataka, tj. zaštita od namjernog i nenamjernog ometanja normalnog rada može uključivati sljedeće:

- zaštitu čitave infrastrukture sustava videonadzora (uključujući kamere na daljinsko upravljanje, kablove i napajanje) od fizičkog interveniranja i krađe
- zaštitu prijenosa snimki s pomoću komunikacijskih kanala zaštićenih od presretanja
- enkripciju podataka
- primjenu hardverskih i softverskih rješenja kao što su vatrozidovi, antivirusni sustavi ili sustavi za otkrivanje neovlaštenog upada za zaštitu od kiberincidenata
- otkrivanje neispravnosti komponenata, softvera ili međusobnog povezivanja
- sredstva za ponovnu uspostavu dostupnosti sustava i pristupa sustavu u slučaju fizičkog ili tehničkog incidenta.

Kontrolom pristupa osigurava se da sustavu i podatcima mogu pristupiti samo ovlaštene osobe, dok su drugi u tome spriječeni.

Mjere kojima se podupire kontrola fizičkog i logičkog pristupa:

- osiguravanje da svi prostori pod videonadzorom i sva mjesta na kojima se pohranjuju videosnimke budu zaštićeni od neovlaštenog pristupa trećih strana
- postavljanje zaslona (posebno ako se nalaze u otvorenim prostorima, kao što je recepcija) na način da pogled na njih imaju samo ovlašteni operatori
- utvrđivanje i provedba postupaka za dodjelu, promjenu i ukidanje fizičkog i logičkog pristupa
- primjena metoda i sredstava za autentifikaciju i ovlašćivanje korisnika, uključujući npr. dužinu lozinke i učestalost njezine

izmjene
- bilježenje i redovito preispitivanje aktivnosti koje obavlja korisnik (povezane sa sustavom i podatcima)
- kontinuirano praćenje i otkrivanje neispravnosti u pogledu pristupa i rješavanje utvrđenih nedostataka u najkraćem mogućem roku.

Voditelj ili izvršitelj obrade koji ne označe objekt, prostorije, dijelove prostorije te vanjsku površinu objekta na propisan način, ne uspostave automatizirani sustav zapisa za evidentiranje pristupa snimkama videonadzora ili ukoliko ovlaštene osobe za pristup videozapisima koriste snimke suprotno utvrđenoj svrsi videonadzora mogu se kazniti do 50.000,00 kn.

VIDEONADZOR NA RADNOM MJESTU

Obrada osobnih podataka zaposlenika putem videonadzora može se provoditi samo ako su ispunjeni uvjeti utvrđeni posebnim zakonom kojim se uređuje zaštita na radu i ako su zaposlenici na primjeren način unaprijed obaviješteni o takvoj mjeri te ako je poslodavac informirao zaposlenike prije donošenja odluke o postavljanju sustava videonadzora.
U slučaju da videonadzor prati tijekom radnog vremena sve pokrete zaposlenika tijekom obavljanja njihovih poslova ili je videonadzor postavljen tako da su zaposlenici čitavo vrijeme tijekom rada u vidnom polju kamera, potrebna je prethodna **suglasnost radničkog vijeća ili sindikalnog povjerenika.**

VIDEONADZORA STAMBENIH ZGRADA

Za uspostavu videonadzora u stambenim zgradama potrebna je suglasnost suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova.

Kamere trebaju biti postavljen tako da obuhvaćaju samo pristup ulascima i izlascima iz stambene zgrade te zajedničke prostorije.

Videonadzor ne smije obuhvaćati prostorije za odmor, osobnu higijenu i presvlačenje.

Zaposlenici moraju biti upoznati s videonadzrom prije sklapanja ugovora o radu.

Zabranjeno je koristiti videonadzor za praćenje radne učinkovitosti domara, spremačica i drugih osoba koje rade u stambenoj zgradi.

VIDEONADZOR JAVNIH POVRŠINA

Praćenje javnih površina putem videonadzora dozvoljeno je samo tijelima javne vlasti, pravnim osobama s javnim ovlastima i pravnim osobama koje obavljaju javnu službu, samo ako je propisano zakonom, ako je nužno za izvršenje poslova i zadaća tijela javne vlasti ili radi zaštite života i zdravlja ljudi te imovine.

Korišteni materijali: Opća uredba o zaštiti podataka, Zakon o provedbi Opće uredbe, Smjernice o provedbi videonadzora - EDPB, Vodič za upotrebu videonadzora namjenjen mikro, malim i srednjim poduzetnicima – ARC, Smjernice radne skupine za zaštitu podataka iz članka 29. upute i savjeti nadzornog tijela objavljeni na www.azop.hr

EUROPEAN FEDERATION
OF DATA PROTECTION OFFICERS

CENTAR FERALIS Hrvatski je predstavnik u Europskoj federaciji službenika za zaštitu podatka (EFDPO)

FERALIS PRIVACY CENTER
SLUŽBENIK ZA ZAŠTITU PODATAKA

KUPON

15% POPUSTA

Kupon se može iskoristiti do 31.12.2021. godine

Kupon se može koristiti za ugovaranje mjesečne funkcije službenika za zaštitu podatka i pojedinačne usluge iz djelokruga službenika za zaštitu podataka

SLUŽBENIK ZA ZAŠTITU PODATAKA

Službenik za zaštitu podataka za male, srednje i velike organizacije obavlja sve poslove sukladno utvrđenim obvezama u Općoj uredbi na način predviđen relevantnim Smjernicama Radne skupine za zaštitu osobnih podataka iz članka 29., Europskog odbora zaštitu podataka te u skladu s uputama i smjernicama nadzornog tijela (AZOP-a) a u skladu s potrebama organizacije.

Usluga, između ostaloga, uključuje i pripremu prijedloga organizacijskih mjera zaštite s provođenjem svih potrebnih postupaka za uspostavu prihvaćenih mjera te slijedeće usluge:

- stručno savjetovanje
- reviziju postojećih mjera zaštite
- usklađivanje organizacijskih mjera zaštite sa zahtjevima GDPR
- ustrojavanje i vođenje evidencije aktivnosti obrade osobnih podataka

- postupanje s izvršiteljima obrade
- provođenje postupka utvrđivanja legitimnog interesa
- provođenje testa razmjernosti i procjene učinka na zaštitu podataka
- komunikaciju s ispitanicima u pitanju rješavanja njihovih prigovora i zahtjeva u svezi s ostvarivanjem prava ispitanika
- postupanje u slučaju incidenta
- komunikaciju s nadzornim tijelom u slučaju nadzora ili drugog postupka
- edukacija zaposlenika

Uslugu vanjskog službenika za zaštitu podataka (DPO) pruža tim stručnjaka sastavljen od pravnika, odvjetnika, stručnjaka za informacijsku sigurnost i stručnjak za upravljanje kontinuitetom poslovanja u krizi na čelu s profesionalnim službenicima za zaštitu podataka Ines i Markom Krečak. Nositelji su međunarodno priznatih certifikata stručnjaka za privatnost CIPP/E, članovi Međunarodnog udruženja stručnjaka za privatnost (IAPP), Europskog udruženja službenika za zaštitu podataka (EADPP), te su RH predstavnici pri Europskoj federaciji službenika za zaštitu podataka (EFDPO) gdje su članovi tri značajna odbora: zaštita osobnih podataka u zdravstvenom sektoru, zaštita osobnih podataka i AI te odbor Članak 39. Opće uredbe - sprječavanje restrikcija nacionalnih zakonodavstva u pitanju pravnog savjetovanja službenika za zaštitu podatka u svezi zaštite osobnih podataka.

SLUŽBENIK ZA ZAŠTITU PODATAKA - FERALIS

KAMERE U AUTOMBILU
Kamere čija je svrha pomoć pri parkiranju nisu predmet GDPR ukoliko ne pohranjuju snimke s registracijama vozila ili prolaznicima

„LIVESTREAMING“
Ukoliko kamera nema sustav pohrane već je putem iste moguće samo uživo pratiti događaje primjerice, s glavnog gradskog trga, terase ugostiteljskog objekta ili slično, tada ne dolazi do primjene GDPR-a.

LAŽNE KAMERA
Opća uredba se ne primjenjuje na fiktivno postavljene kamere (uređaji koji nisu u funkciji)

SNIMANJE DRONOM
U slučaju snimanja drona, GDPR je primjenjiv samo ukoliko se na snimkama može identificirati pojedinac

Jože Grabovšeka 8, Rijeka
www.feralis.hr
feralis@feralis.hr
+385 99 5639746 +385 91 7881535

Feralis
PRIVACY CENTER RIJEKA

WWW.FERALIS.HR

Feralis

FERALIS PRIVACY CENTER d.o.o.
Jože Gabrovšeka 8, Rijeka 51000

☎ +385995639746
dpo@feralis.hr

OVAJ OBJEKT JE POD VIDEONADZOROM

SVRHA OBRADE: zaštita osoba i imovine

PRAVNA OSNOVA: legitimni interes

PRAVA ISPITANIKA: pravo na pristup svojim osobnim podacima, pravo na njihovo brisanje, pravo na ograničenje njihove obrade te pravo na ulaganje prigovora na obradu.

Cjelovite informacije o obradi osobnih podataka putem sustava videonadzor možete dobiti na navedeni kontakt telefon, na adresi sjedišta ili u politici privatnosti web stranice www.feralis.hr

DANAS

DODATAK UZ NOVI LIST

INFORMATIVNI VODIČ

VIDEONADZOR & GDPR

Feralis

PRIVACY CENTER RIJEKA

NOVI LIST

www.novilist.hr

...HO FRANO SUPILO 2. SIJEČNJA 1900.

PONEDJELJAK / RIJEKA / 8. STUDENOGA 2021

...O 1.40 €, EU 1.70 €, 3.70 CHF, 1.70 KM

VRIJEME DHMZ

DANAS max. 12 min. 8

SUTRA max. 13 min. 8

ZABORAVLJE... DONACIJA

Vrh H... ali nij... nova

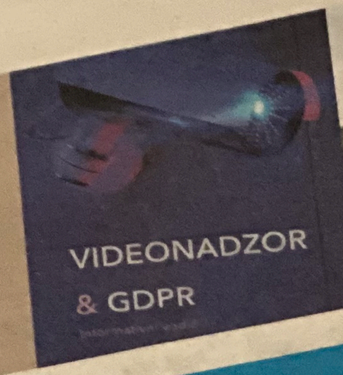
...nja 2016.

DANAS

DODATAK UZ NOVI LIST

INFORMATIVNI VODIČ
VIDEONADZOR & GDPR

Feralis
PRIVACY CENTER RIJEKA



VRIJEME

DANAS

DHMZ
www.meteo.hr

max. 12

min. 8

SUTRA

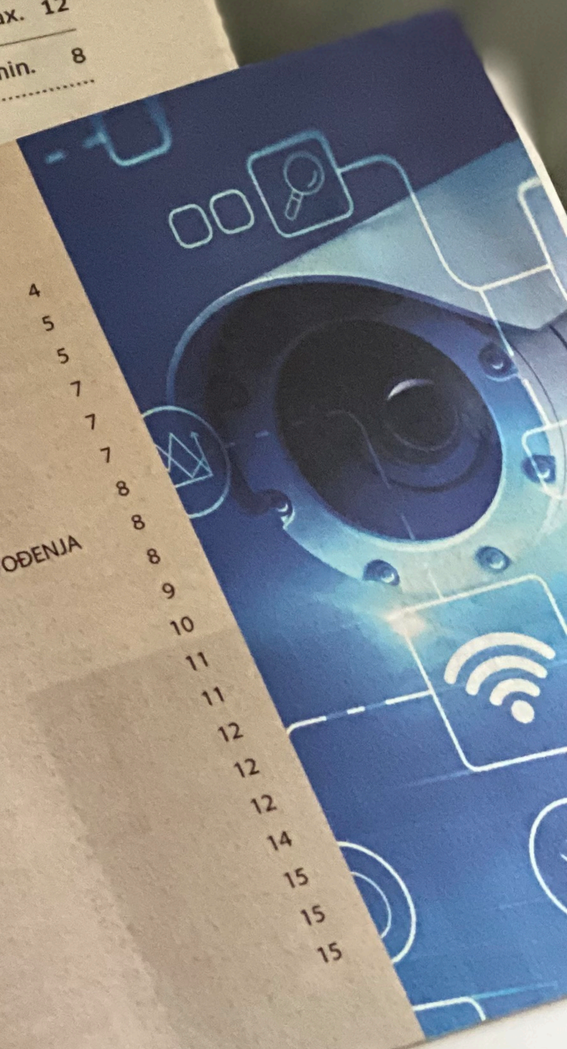
www.novilist.hr

NOVI LIST

UTEMELJIO FRANO SUPILO 2. SIJEČNJA

PONEDJELJAK / RIJEKA / 8. STUDENOG

VIDEONADZOR I GDPR



Luka Ivančić najavljuje da će klub participirati u izradi spomenika posvećenog djeci, žrtvama rata u Vukovaru

IGOR KRALJ/PIXSELL