

Na podlagi 35. člena Uredbe (EU) 2016/679 Evropskega parlamenta in sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), zavod Osnovna šola Trzin, ki ga zastopa ravnatelj Matejka Chvatal, dne 27.03.2023 sprejme

OCENO UČINKA V ZVEZI Z IZVAJANJEM VIDEONADZORA V OŠ TRZIN

1. člen

Ocena učinka pomeni oceno izvora, narave, posebnosti in resnosti tveganja pri obdelavi osebnih podatkov ter ukrepe za omejitev tveganja pri obdelavi osebnih podatkov.

Izvajalec izdelava in sprejme Oceno učinka v zvezi z varstvom podatkov z namenom pravočasne identifikacije tveganj in z namenom sprejema ustreznih ukrepov za obvladovanje tveganj, da se v največji možni meri prepreči, da bi prišlo do kršitve zakonodaje iz področja varstva podatkov.

Ocena učinka v zvezi z varstvom podatkov je preventivni ukrep varstva osebnih podatkov za zagotavljanje načela zakonitosti in odgovornosti pri obdelavi osebnih podatkov, ki poudarja in obenem zahteva preventivno in proaktivno ravnanje upravljavcev in obdelovalcev podatkov.

2. člen

1. OPIS PROJEKTA – IZVAJANJE VIDEONADZORA V OŠ TRZIN - opis predvidenih dejanj obdelave in namenov obdelave

OPIS DEJANJA OBDELAVE	OBRAZLOŽITEV IN SMERNICE	V PRAKSI IZVAJALCA
NABOR OSEBNIH PODATKOV	Nabor osebnih podatkov, ki se bodo obdelovali je potrebno čimbolj natančno določiti. Pri tem je potrebno paziti, da: • obdelava pomeni kakršnokoli ravnanje z osebnimi podatki; • je osebni podatek katera koli informacija v zvezi z določenim ali določljivim posameznikom; • osebni podatek se nanaša na posameznika in sicer ne glede na obliko, v kateri je izražen; • na določljivost osebe vpliva tudi, ali bi kdo drug brez nesorazmerno veliko naporov,	Vrste osebnih podatkov, ki jih OŠ Trzin obdeluje za potrebe izvajanja videonadzora so naslednji: • posnetek prostorov in posameznikov, šole, šolske ploščadi, vhodov v šolo in enoto vrtca, službenega vhoda, kolesarnice

	časa, ali sredstev lahko ugotovil, na koga se podatek nanaša; • za obdelavo osebnih podatkov je potrebno zagotoviti ustrezno pravno podlago.	
NAMEN OBDELAVE/OMEJITEV NAMENA OBDELAVE	Osebni podatki se obdelujejo samo za namen, za katerega so bili pridobljeni in na ustrezni pravni podlagi.	Osebni podatki, pridobljeni na podlagi uvedenega ukrepa – izvajanje videonadzora za namen: 1. <u>zunaj objekta</u> • zagotavljanje varnosti premoženja in ljudi; • nadzor nad opremo večje vrednosti, ki je lahko podvržena vandalizmu; • odkrivanju oz. preprečevanju nastanka poškodb; • uveljavljanje pravnih zahtevkov v primeru poškodovanja premoženja, ki je v lasti oz. upravljanju zavoda Pravna podlaga za uvedbo ukrepa – sprejet interni akt: Pravilnik o izvajanju videonadzora, ki določa namene snemanja, hranjenje posnetkov, ukrepe za zavarovanja osebnih podatkov, odgovorne in pooblaščne osebe.
ZAKONITOST OBDELAVE OSEBNIH PODATKOV	Osebnosti podatke se obdeluje samo, če za to obstaja ustrezna pravna podlaga kot to določa člen 6 Splošne uredbe.	Pravilnik o izvajanju videonadzora, ki določa namene snemanja, hranjenje posnetkov, ukrepe za zavarovanja osebnih podatkov, odgovorne in pooblaščne osebe. Kot ena temeljnih pravnih podlag za obdelavo osebnih podatkov se po Splošni uredbi o varstvu podatkov šteje zakonit interes (točka f člena 6(1)). V konkretnem primeru izvajanja videonadzora gre za snemanje zaposlenih, učencev in drugih posameznikov ter objektov za namen zagotavljanja varovanja in varnosti učencev, zaposlenih in obiskovalcev ter premoženja zavoda in njegove okolice, zaradi česar pride v poštev 76., 77. in 78. člen ZVOP-2, saj gre za obdelavo osebnih

		podatkov, ki je potrebna za izvrševanje videonadzora.
PREGLEDNOST OBDELAVE OSEBNIH PODATKOV	Za zagotavljanje zakonitosti v procesu obdelave se upošteva: • kako se bodo osebni podatki pridobivali; • kje se bodo hranili; • kako se bodo obdelovali; • komu se bodo posredovali; • kdo bo delal z osebnimi podatki (katere osebe); • kako bodo podatki zavarovani pred naključnimi ali namernimi zlorabami, izgubo ali uničenjem; (tehnično/organizacijsko), • kako dolgo se bodo osebni podatki hranili; • kako se bodo po poteku roka za obdelavo uničili.	Preglednost obdelave osebnih podatkov za potrebe izvajanja videonadzora omogočamo na podlagi: • sprejetega Pravilnika o izvajanju videonadzora, ki določa namene snemanja, hranjenje posnetkov, ukrepe za zavarovanja osebnih podatkov, odgovorne in pooblaščen osebe. • Evidence uporabe videoposnetkov • Zbirke podatkov, ki za ta namen nastaja in je del internega akta Evidence dejavnosti obdelave kot obvezne priloge Pravilnika o zbiranju, obdelavi in zavarovanju osebnih podatkov.
OMEJITEV SHRANJEVANJA	Pri obdelavi osebnih podatkov je potrebno upoštevati načelo omejitve hrambe (točka (e) prvega odstavka 5. člena Splošne uredbe), ki določa, da se osebni podatki hranijo le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo.	Pravilnik o izvajanju videonadzora v 24. členu določa, da se posnetki hranijo do 60 dni za vse kamere, ki so priključene na napravo za snemanje. Posnetki se nato trajno izbrišejo.
SORAZMERNOST	Pri obdelavi osebnih podatkov je potrebno spoštovati načelo sorazmernosti obdelave osebnih podatkov. Osebni podatki, ki se obdelujejo, morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo.	Namena, zaradi katerega se uvaža ukrep izvajanja videonadzora, ni mogoče doseči z milejšimi ukrepi.
TOČNOST IN AŽURNOST OSEBNIH PODATKOV	Osebni podatki, ki se obdelujejo, morajo biti točni in ažurni.	Točnost in ažurnost osebnih podatkov se omogoča na podlagi snemalnih naprav, s katero se izvaja videonadzor.
SPLOŠEN OPIS VAROVANJA ZBIRKE OSEBNIH PODATKOV	Osebni podatki morajo biti med obdelavo ustrezno zavarovani s postopki in ukrepi, s katerimi se preprečuje, da bi bili podatki dostopni nepooblaščenim osebam, bili uničeni, spremenjeni ali na drug način zlorabljeni.	Pri računalniški obdelavi osebnih podatkov varuje podatke vhodna koda. Prostor, v katerem se nahaja zbirka osebnih podatkov ter strojna in aplikativna programska oprema, ki je namenjena za obdelavo osebnih podatkov je varovana z organizacijskimi, fizičnimi in logično-tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do podatkov. Dostop v prostor, kjer se hrani

		zbirka osebnih podatkov je mogoč samo v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja direktorja. Ključni varovanega prostora se uporabljajo in hranijo v skladu z internimi pravili.
UDELEŽENE OSEBE PRI OBDELAVI OSEBNIH PODATKOV	Osebe, ki obdelujejo osebne podatke morajo biti v naprej znane in določene, sicer lahko privede do nezakonite obdelave osebnih podatkov.	Osebe, ki so udeležene pri obdelavi osebnih podatkov so opredeljene v Pravilniku o izvajanju videonadzora, Evidencah uporabe videoposnetkov in v zbirki podatkov, ki za ta namen nastaja in je del internega akta Evidence dejavnosti obdelave kot obvezne priloge Pravilnika o zbiranju, obdelavi in zavarovanju osebnih podatkov.

2. TVEGANJA

Vrsta tveganja:	Obdelava podatkov brez ustrezne pravne podlage.
Verjetnost:	<u>Srednja</u> , ker se večina osebnih podatkov obdeluje na podlagi zakona oz. predhodno sprejetih inertnih aktov.
Resnost:	<u>Velika</u> - v kolikor nastopi situacija, da bi upravljavec osebnih podatkov obdeloval podatke brez podlage v zakonu, so predpisane visoke globe.
Stopnja tveganja:	<u>Nizka</u> , saj se večina podatkov obdeluje na podlagi zakona, sprejetih internih aktov, predhodne seznaitve javnih uslužbencev z uvedbo ukrepa, soglasja sindikata k obdelavi osebnih podatkov.
Ukrep:	Sprejetje internega akta – Pravilnik o izvajanju videonadzora. Omejitev namena obdelave osebnih podatkov. Omejitev hrambe osebnih podatkov. Pridobitev pozitivnega mnenja sindikata k uvedbi ukrepa. Vpogledovanje v osebne podatke pod pogoji kot jih določa Pravilnik o izvajanju videonadzora. Vodenje ustreznih evidenc o vpogledovanju oz. obdelavi osebnih podatkov kot to izhaja iz Pravilnika o izvajanju videonadzora.

Vrsta tveganja:	Posameznik ne poda privolitve za obdelavo osebnih podatkov.
Verjetnost:	<u>Majhna</u> , ker se večina osebnih podatkov obdeluje na podlagi zakona oz. predhodno sprejetih inertnih aktov.
Resnost:	<u>Velika</u> - v kolikor nastopi situacija, da bi upravljavec osebnih podatkov obdeloval podatke brez podlage v zakonu, so predpisane visoke globe.
Stopnja tveganja:	<u>Nizka</u> , saj se večina podatkov obdeluje na podlagi zakona, sprejetih internih aktov, predhodne seznaitve javnih uslužbencev z uvedbo ukrepa, soglasja sindikata k obdelavi osebnih podatkov. V primeru pa, ko ima upravljavec osebnih podatkov podlago za obdelavo osebnih podatkov v zakonu, privolitev posameznika ni potrebna.
Ukrep:	Zagotovitev ustrezne pravne podlage za obdelavo osebnih podatkov. Sprejetje internega akta – Pravilnik o izvajanju videonadzora.

	Omejitev namena obdelave osebnih podatkov. Omejitev hrambe osebnih podatkov. Pridobitev pozitivnega mnenja sindikata k uvedbi ukrepa.
--	--

Vrsta tveganja:	Zbrani podatki niso točni.
Verjetnost:	<u>Majhna</u> – osebni podatki se obdelujejo in zbirajo preko snemalne naprave, ki omogoča video snemanje.
Resnost:	<u>Majhna</u> , ker se osebni podatki obdelujejo preko naprave, ki omogoča video snemanje.
Stopnja tveganja:	<u>Nizka</u> .
Ukrep:	Po potrebi se ažurirajo podatki, pri čemer se netočni podatki nadomestijo s točnimi, in sicer po postopku, ki zagotavlja sledljivost spremembe podatkov.

Vrsta tveganja:	Uničenje ali izguba podatkov (računalniški mediji).
Verjetnost:	<u>Majhna</u> , ker so podatki v obliki listin shranjeni v ustreznih ognjevarnih omarah, v zaklenjenem prostoru; podatki na računalnikih so varovani z varnostnimi kopijami, zaščiteni z dostopnimi močnimi gesli.
Resnost:	<u>Visoka</u> , ker izguba osebnih podatkov lahko povzroči škodo posamezniku.
Stopnja tveganja:	<u>Srednja</u> .
Ukrep:	Dokumente oz. listine, ki nastanejo na podlagi uvedenega ukrepa se shranjuje v zaklenjenih, ognjevarnih omarah, predalih, podatke na računalniških in elektronskih medijih se zavaruje z dostopno kodo.

Vrsta tveganja:	Obdelava osebnih podatkov izven namena obdelave.
Verjetnost:	<u>Majhna</u> , saj so vse osebe, ki sodelujejo v procesu obdelave podatkov ustrezno poučene o pomembnosti varstva osebnih podatkov; tveganje pa kljub temu obstaja.
Resnost:	<u>Visoka</u> , saj nenamenska obdelava osebnih podatkov lahko povzroči škodo za posameznika.
Stopnja tveganja:	<u>Srednja</u> .
Ukrep:	Uvede se sledljivost obdelave podatkov, izobraževanje oseb, ki sodelujejo v postopku obdelave podatkov, uvede se omejitev dostopa do osebnih podatkov, seznanitev vseh z internim aktom – Pravilnikom o izvajanju videonadzora.

Vrsta tveganja:	Obdelava osebnih podatkov po poteku roka, ki je določen v internem aktu.
Verjetnost:	<u>Srednja</u> - vse osebe, ki sodelujejo v procesu obdelave podatkov so poučene o pomembnosti varstva osebnih podatkov; tveganje pa kljub temu obstaja.
Resnost:	<u>Visoka</u> , saj nenamenska obdelava osebnih podatkov lahko povzroči škodo za posameznika.
Stopnja tveganja:	<u>Srednja</u> .
Ukrep:	Dosledno se spoštujejo roki hrambe osebnih podatkov, dosledno se osebni podatki, ki so hranjeni na nosilcih podatkov uničujejo, skladno z določili Pravilnika o izvajanju videonadzora.

Vrsta tveganja:	Pošiljanje posnetkov po elektronski pošti.
------------------------	---

Verjetnost:	<u>Majhna</u> - vse osebe, ki sodelujejo v procesu obdelave podatkov so poučene o tem, kdo je upravičen, da posnetke pregleduje oz. obdeluje.
Resnost:	<u>Visoka</u> , saj seznanitev nepooblaščenih oseb lahko privede do škode posameznika.
Stopnja tveganja:	<u>Majhna</u> .
Ukrep:	Dosledno se spoštuje Pravilnik o izvajanju videonadzora, dana jasna navodila, da se posnetki ne posredujejo po elektronski pošti.

Vrsta tveganja:	Sodelovanje s pogodbenimi obdelovalci osebnih podatkov.
Verjetnost:	<u>Majhna</u> - v primeru obdelave osebnih podatkov s strani obdelovalca je vedno predhodno sklenjena Pogodba o obdelavi osebnih podatkov, na podlagi katere se določijo pravice in obveznosti pogodbenega obdelovalca.
Resnost:	<u>Majhna</u> , saj upravljavec osebnih podatkov samostojno obdeluje osebne podatke.
Stopnja tveganja:	<u>Majhna</u> .
Ukrep:	V primeru prenosa obdelave osebnih podatkov iz upravljavca na obdelovalca je potrebno skleniti ustrezno Pogodbo o obdelavi osebnih podatkov.

3. UKREPI ZA OMEJITEV TVEGANJA (ukrepi za obravnavanje tveganj, vključno z zaščitnimi ukrepi, varnostni ukrepi ter mehanizmi za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti)

VRSTE UKREPOV	OBRAZLOŽITEV
Ukrepi, ki prispevajo k varstvu pravic posameznika	Posameznik ima naslednje pravice: • informiranje posameznika o obdelavi podatkov; • pravica do seznanitve in prenosljivosti podatkov; • pravica do popravka in izbrisa podatkov; • pravica do ugovora in omejitve obdelave; • odnosi s (pogodbenimi) obdelovalci; • varovalke glede prenosa podatkov v tretje države; • predhodno posvetovanje.
Ocena potrebnosti in sorazmernosti dejanj obdelave glede na njihov namen	Ukrepi, ki prispevajo k upoštevanju nujnosti in sorazmernosti: • določeni, izrecni in zakoniti nameni obdelave; • zakonitost obdelave; • obdelava je ustrezna, relevantna in omejena na to, kar je potrebno za namene, za katere se obdelujejo podatki; • upoštevana je omejitev shranjevanja – roki hrambe. Določi se minimalni zadostni nabor osebnih podatkov, s katerim se lahko doseže namen obdelave: • če določeni osebni podatki niso potrebni, potem naj se jih ne zbira; • če so osebni podatki potrebni, potem uporabiti manj občutljive/posebne od bolj občutljivih, ne zbirati več enoličnih identifikatorjev, če to ni nujno potrebno.

	Nabor osebnih podatkov se skrči na minimum. Na sorazmernost se pazi v vseh fazah – tudi npr. pri: • oblikovanju iskalnikov (kakšni so možni iskalni kriteriji, kaj se izpiše pri rezultatih iskanja); • uporabniških pravicah (ali določen uporabnik res potrebuje dostop do določenih podatkov - nivojski dostop) – več podatkov pomeni večje zahteve za sledljivost. Dostop do osebnih podatkov: • vnaprej določeni osebi, minimalen nabor podatkov, sledljivost.
Preveritev pravne podlage	Upravljavec osebnih podatkov mora venomer zagotavljati ustrezno pravno podlago za obdelavo osebnih podatkov. Ustrezna pravna podlaga je podana v kolikor je izpolnjen eden izmen taksativno naštetih pogojev: (a) posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov; (b) obdelava je potrebna za izvajanje pogodbe, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe; (c) obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca; (d) obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe; (e) obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu; (f) obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.«
Preveritev pogodbene obdelave	Če bo določena opravila nad osebnimi podatki izvajal pogodbeni obdelovalec je potrebno upoštevati zahteve iz Zakona o varstvu osebnih podatkov in Evropske Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov – pisna pogodba in konkretizirani postopki za zavarovanje osebnih podatkov pri pogodbenem partnerju. Pogodbeni obdelovalec obdeluje osebne podatke v imenu in na račun upravljavca osebnih podatkov. Obdelava pomeni kakršnokoli ravnanje z osebnimi podatki – tudi samo shranjevanje, pošiljanje ali uničenje podatkov se šteje za obdelavo osebnih podatkov. Na pogodbeno obdelavo je potrebno gledati skozi oči posameznika – ali bi lahko prišlo do zlorabe osebnih podatkov pri pogodbenem obdelovalcu. Pogodbenega obdelovalca ima upravljavec pravico in dolžnost nadzorovati.

	Zaposleni pri pogodbenem obdelovalcu morajo biti natančno poučeni, kaj smejo in kaj ne smejo z osebnimi podatki.
Preveritev točnosti in ažurnosti	Osební podatki morajo biti točni in ažurni. Pred vnosom osebnih podatkov v zbirko se lahko preveri točnost podatkov z vpogledom v osebni dokument. Predvideni so postopki za dopolnitev, brisanje ali popravek netočnih in neažurnih podatkov.
Posredovanje osebnih podatkov	Osební podatke se lahko posreduje uporabnikom osebnih podatkov, ki razpolagajo z ustrezno pravno podlago.
Varnost obdelave osebnih podatkov - interni akti	Osební podatki morajo biti med obdelavo ustrezno zavarovani s postopki in ukrepi, s katerimi se preprečujejo, da bi podatki bili dostopni nepooblaščenim osebam, bili uničeni, spremenjeni ali na drug način zlorabljeni. Upoštevajo se naslednji ukrepi za obvladovanje splošnih tveganj v povezavi z varnostjo podatkov: • sprejeti so interni akti o varstvu osebnih podatkov; • izvaja se ocena učinkov; • s pogodbenimi obdelovalci osebnih podatkov so sklenjene ustrezne pogodbe; • uporabljajo se ukrepi za tehnično in organizacijsko varovanje osebnih podatkov; • opredeljene so pravice uporabnikov za dostop do podatkov; • beležijo se dostopi do osebnih podatkov v zbirki; • udeležene osebe so ozaveščene z zakonodajo in sprejetimi internim akti s področja varstva osebnih podatkov; • drugo (<i>navedite</i>): _____
Določitev odgovornih oseb	Določen, dokumentiran ter ažuriran mora biti nabor odgovornih oseb za posamezno zbirko osebnih podatkov ter oseb, ki imajo pooblastila za dostop do osebnih podatkov.
Notranja sledljivost obdelave	Zagotovljena mora biti sledljivost, in sicer: • sistem mora omogočati poznejše ugotavljanje, kdaj so bili posamezni osebni podatki uporabljeni ali drugače obdelani in kdo je to storil; • zavarovanje je potrebno in dopustno prilagoditi naravi in tveganju, ki ga prinaša obdelava določenih vrst osebnih podatkov, • vodenje evidence uporabe posnetkov.
Zunanja sledljivost obdelave (posredovanje)	Za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni pravni podlagi.
Interni nadzor	Redno izvajanje internega nadzora s preverjanjem: • ali se lahko odkrijejo zlorabe osebnih podatkov;

	• ali se lahko ugotovi, ali zaposleni uporabljajo osebne podatke za legitimne in zakonite namene, ali gre za radovednost in usluge prijateljem; • varnost osebnih podatkov temelji tudi na ustrezni izobraženosti in ozaveščenosti zaposlenih – človeški faktor je pogost vzrok zlorab.
Evidenca dejavnosti obdelave	Vsako obdelavo osebnih podatkov je potrebno predvideti v internem aktu – Evidence dejavnosti obdelave, saj se na ta način zagotavlja preglednost obdelave osebnih podatkov.
Izvajanje videonadzora	Tudi pri izvajanju videonadzora je pomembna nujnost in sorazmernost, predvsem zaradi doseganja ciljev in namenov, ki bi jim naj videonadzor služil.

3. člen

Ocena učinka je pokazala, da v zvezi z obdelavo osebnih podatkov, ki jih doprinese ukrep izvajanja videonadzora, obstaja določena stopnja tveganja, vendar so ta tveganja, z uvedbo posameznih ukrepov, kot izhajajo iz ocene učinka, obvladljiva.

V posledici navedenega se ukrep izvajanja videonadzora v okolici OŠ Trzin lahko uvede.

Trzin, dne 27.03.2023

Matejka Chvatal
ravnatelj

