

Na podlagi Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/2022 s spremembami, v nadaljevanju: **ZVOP-2**) ter ob upoštevanju 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 - Splošne uredbe o varstvu podatkov (v nadaljevanju: **GDPR**), Svet zavoda Škofijske gimnazije Vipava

sprejema naslednji

## **PRAVILNIK O SISTEMU ZAZNAVANJA GIBANJA Z VIZUALNO VERIFIKACIJO DOGODKOV**

### **(v nadaljevanju: Pravilnik)**

#### 1. člen

#### POMEN IZRAZOV

Izrazi, uporabljeni v Pravilniku, imajo sledeč pomen:

- **Upravljalec:** Škofijska gimnazija Vipava, Goriška cesta 29, 5271 Vipava, v nadaljevanju tudi: **zavod**, ki po odgovorni osebi odloča o namenu, obsegu in načinu uporabe sistema ter o obdelavi osebnih podatkov.
- **Odgovorna oseba:** ravnatelj oziroma ravnateljica zavoda, ki je pristojna za izdajo sklepa o uvedbi sistema, imenovanje pooblaščenih oseb, odločanje o vpogledih v zajete fotografije ter za zagotavljanje izvajanja tega Pravilnika.
- **Sistem:** tehnični sistem zaznavanja gibanja z vizualno verifikacijo dogodkov proizvajalca Ajax, ki ga sestavljajo Hub, ReX in senzorji MotionCam oziroma drugi kompatibilni senzorji s funkcijo zajema fotografij, ki sprožijo alarmni dogodek.
- **Senzor:** brezžična naprava za zaznavanje gibanja (Ajax MotionCam), ki ob zaznavi gibanja v varovanem območju sproži alarmni dogodek in zajame zaporedje fotografij za namen vizualne verifikacije.
- **Vizualna verifikacija dogodka:** zajem ene ali več fotografij ob sprožitvi senzorja gibanja za namen ugotavljanja dejanskega poteka alarmnega dogodka.
- **Fotografija:** posamezna slika, zajeta ob alarmnem dogodku, ki vsebuje podobo osebe, datum, čas in lokacijo dogodka.
- **Pooblaščen oseb:** oseba, ki jo odgovorna oseba pisno pooblasti za upravljanje sistema, pregled fotografij, odločanje o izvozu podatkov oziroma vodenje evidence obdelav.
- **Zunanji izvajalec:** pravna ali fizična oseba, ki po pogodbi z upravljalcem namesti, vzdržuje ali servisira sistem in pri tem lahko dostopa le do tistih podatkov in nastavitev, ki so nujno potrebni za izvedbo storitve.

#### 2. člen

#### SORAZMERNOST IZVAJANJA SISTEMA IN NAMEN TER ČAS DELOVANJA

Ta Pravilnik določa vzpostavitev, izvajanje, namen, pogoje uporabe, način varovanja dostopa, hrambo podatkov ter pravice in obveznosti pooblaščenih oseb pri uporabi sistema zaznavanja gibanja z vizualno verifikacijo dogodkov na objektu Dijaškega doma Škofijske gimnazije Vipava, Grabrijanova ulica 19, 5271 Vipava (v nadaljevanju: Dijaški dom).

V Dijaškem domu je nameščen varnostni sistem Ajax, ki ga sestavljajo centralna enota Hub, razširitvena enota ReX ter deset (10) senzorjev gibanja s funkcijo zajema fotografij ob alarmnem dogodku. Sistem ne izvaja neprekinjenega videonadzora in ne omogoča snemanja videa, temveč ob zaznavi gibanja zajame zaporedje fotografij, namenjenih preverjanju upravičenosti sproženega alarma.

Sistem se izvaja izključno za namene varovanja življenja in zdravja dijakov, zaposlenih in obiskovalcev ter varovanja premoženja Dijaškega doma, preprečevanje vandalizma, ugotavljanje okoliščin varnostnih incidentov in preverjanje upravičenosti alarmnega dogodka v času nočnega počitka.

Sistem ni namenjen nadzoru dela zaposlenih, spremljanju vsakodnevnega gibanja dijakov ali trajnemu spremljanju dogajanja v Dijaškem domu. Uporablja se le v obsegu, ki je nujno potreben za dosego zakonitega in zapisanega namena.

Sistem deluje izključno v času nočnega počitka, skladno s hišnim redom Dijaškega doma, praviloma od 23.00 do 6.00 naslednjega dne, oziroma v drugem časovnem razponu, kadar tako zaradi organizacije dela ali izrednih okoliščin odloči odgovorna oseba in je to nujno za dosego namena.

Sistem se lahko izjemoma aktivira tudi izven časovnega razpona iz prejšnjega odstavka, v času šolskih počitnic ter vikenda ter deluje 24 ur dnevno, kadar v objektu ni prisotnih dijakov, zaposlenih ali drugih oseb, in je to potrebno za varovanje premoženja ali preprečevanje varnostnih incidentov.

Pred uvedbo sistema je bilo ugotovljeno, da namenov iz tega člena, ki jih sistem zasleduje, ni mogoče doseči z milejšimi ukrepi, saj gre za objekt, v katerem bivajo mladoletni in polnoletni dijaki, zato je potrebna hitra in zanesljiva potrditev izrednih dogodkov v času nočnega počitka.

Strogo prepovedana je namestitev senzorjev ali uporaba sistema v prostorih, kjer posamezniki utemeljeno pričakujejo visoko stopnjo zasebnosti, in sicer:

- v sobah dijakov,
- v sanitarijah, kopalnicah in garderobah,
- v prostorih za osebno higieno.

Pravna podlaga za obdelavo osebnih podatkov je zakoniti interes upravljalca iz točke (f) prvega odstavka 6. člena GDPR - namen varovanja življenja in zdravja dijakov, zaposlenih in obiskovalcev ter varovanja premoženja Dijaškega doma, preprečevanje vandalizma, ugotavljanje okoliščin varnostnih incidentov in preverjanje upravičenosti alarmnega dogodka v času nočnega počitka, pri čemer upravljalec upošteva načela zakonitosti, sorazmernosti, minimizacije podatkov, omejitve namena in omejitve hrambe ter ustrezne določbe ZVOP-2 oz. vsakokratnega zakona, ki ureja varstvo osebnih podatkov.

### 3. člen

#### OBVESTILO O IZVAJANJU NADZORA IN UPORABI SISTEMA TER HRAMBA POSNETKOV

Upravljalec mora o uporabi sistema vnaprej in na primeren način obvestiti vse strokovno osebje Dijaškega doma, dijake in dijakinje ter njihove starše oziroma zakonite zastopnike s pisnim obvestilom ter hkrati objaviti obvestilo, ki mora biti razločno, vidno in objavljeno tako, da se posameznik seznanj z njegovim izvajanjem pred vhodom Dijaškega doma in da se lahko vstopu v nadzorovano območje odpove.

Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:

- jasno pisno ali nedvoumno grafično označbo, da je območje varovano s sistemom zaznavanja gibanja z vizualno verifikacijo dogodkov;
- namen obdelave osebnih podatkov;
- naziv in kontaktne podatke upravljalca;
- kontaktne podatke (telefon ali elektronski naslov) pooblaščenih oseb za varstvo podatkov, če je imenovana;
- informacijo o pravicah posameznika po 13. členu GDPR in načinu njihovega uveljavljanja;
- pravno podlago za obdelavo osebnih podatkov;
- kategorije uporabnikov oziroma prejemnikov podatkov;
- informacijo o roku hrambe oziroma merilih za določitev roka hrambe ter posebnih vplivih obdelave ter neobičajnih nadaljnjih obdelavah.

Šteje se, da je posamezni dijak oz. dijakinja oz. njegovi starši ali zakoniti zastopniki z objavo obvestila v Dijaškem domu ter pisnim obvestilom odgovorne osebe v Dijaškem domu obveščeni o uporabi sistema ter o bistveni in nujni obdelavi osebnih podatkov.

Fotografije, zajete ob alarmnem dogodku, se hranijo največ tri (3) mesece oziroma do sistemskih omejitev hrambe, razen če so potrebne za uveljavljanje ali izvajanje pravnih postopkov oziroma za vodenje disciplinskega, odškodninskega, prekrškovnega ali kazenskega postopka. V takem primeru se posamezna fotografija ali njen izvoz hrani do pravnomočnega zaključka postopka oziroma do izteka rokov, ki jih določajo veljavni predpisi. Upravljalca zagotavlja, da se po preteku obdobja hrambe podatki ne uporabljajo več.

#### 4. člen

##### TEHNIČNE ZAHTEVE IN LOKACIJE NAMESTITVE SISTEMA

Sistem namesti in tehnično vzdržuje pooblaščen zunanji izvajalec oziroma druga strokovno usposobljena oseba, ki jo določi upravljalca. Oseba, ki izvaja montažo ali servis sistema, mora biti seznanjena z določbami tega Pravilnika, z varnostnimi zahtevami sistema ter z obveznostjo zaupnosti.

Sistem temelji na brezžični komunikaciji med napravami. Hub in ReX sta nameščena na hodniku oziroma v skupnih prostorih objekta, kjer je zaradi tehničnih zahtev sistema potrebno zagotoviti ustrezno radijsko pokritost in stabilno komunikacijo z vsemi nameščenimi senzorji. Sama lokacija Hub-a ali ReX-a ne pomeni, da imajo nepooblaščenih oseb dostop do fotografij ali nastavitvev sistema.

Natančne lokacije posameznih senzorjev z vizualno verifikacijo so določene v Prilogi 1 tega Pravilnika. Senzorji so nameščeni tako, da zajemajo le vhode v skupne prostore in hodnike in samo v obsegu, ki je sorazmeren in nujno potreben za doseg namena sistema.

Pooblaščen oseba zunanjega izvajalca lahko dostopa od nastavitvev sistema ali do posameznih fotografij samo v obsegu, ki je nujno potreben za odpravo tehničnih napak, servis ali nadgradnjo in le na podlagi predhodne odobritve odgovorne osebe, kadar to zahteva narava takšnega posega.

#### 5. člen

##### VAROVANJE DOSTOPA DO SISTEMA

Sistem je tehnično zavarovan (z vstopnimi gesli) in organizacijsko fizično zavarovan pred dostopom nepooblaščenih oseb. Dostop do nastavitvev sistema, dogodkov in zajetih fotografij je mogoč izključno preko avtenticiranih uporabniških računov v namenski aplikaciji oziroma programski opremi proizvajalca na posebnem računalniku v zavarovanem prostoru.

Fizični dostop do naprav Hub ali ReX ne omogoča sam po sebi vpogleda v zajete fotografije, izvoza podatkov ali spremembe uporabniških pravic. Upravljalca zagotovi, da je upravljanje sistema omejeno na najmanjši potreben krog oseb in da so dostopne pravice dodeljene po načelu najmanjšega obsega pravic. Računalnik, s katerega pooblaščenice osebe dostopajo do sistema, mora biti zaščiten z geslom, zaklepom zaslona, biometrično zaščito oziroma drugimi primerljivimi ukrepi. Računalnik tudi beleži posamezne vpise uporabnikov (datum, ura, uporabnik).

Sistem ne omogoča beleženja posameznih vpogledov v fotografije. Sledljivost dostopa se zagotavlja z uporabo individualnih uporabniških računov pooblaščenih oseb ter z beleženjem sistemskih dogodkov.

Pooblaščenice osebe morajo zagotoviti, da nepooblaščenim osebam ni omogočen neposreden vpogled v aplikacijo ali v zajete fotografije.

Podatki, pridobljeni ob alarmnih dogodkih, se varujejo z namenom ugotovitve dejstev varnostnega incidenta in so dostopni izključno pooblaščenim osebam ter pristojnim organom, kadar za to obstaja ustrezna pravna podlaga.

#### 6. člen

##### POOBLAŠČENE OSEBE TER DNEVNIK OZ. EVIDENCA OBDELAVE

Odgovorna oseba s posebnim sklepom imenuje pooblaščenice osebe za upravljanje sistema, pregled fotografij, odločanje o izvozu fotografij ter vodenje evidence obdelave. Pooblaščenice osebe so dolžne ravnati z vsemi podatki zaupno in jih uporabljati izključno za namene, določene s tem Pravilnikom.

Upravljalca vodi dnevnik oziroma evidenco obdelave, iz katere je mogoče ugotoviti katera oseba je v sistem vpogledovala ter kdaj je vpogled opravljen oz. je razvidna uporaba sistema, ali je bil narejen izvoz fotografij, komu so bili podatki posredovani, na kateri pravni podlagi in s kakšnim namenom. V evidenco se vpisujejo tudi spremembe nastavitve sistema, okvare, tehnične težave in servisni posegi. Dnevnik oziroma evidenca obdelave se hrani skladno z določbami 76. člena ZVOP-2 dve leti po koncu leta, ko je fotografija nastala oz. v skladu z zakonskimi zahtevami.

Sledljivost ogleda, uporabe ali posredovanja je zagotovljena z vpisovanjem. Izvoz ali posredovanje fotografij na drug medij oziroma pristojnemu organu lahko odobri odgovorna oseba, kadar oceni, da je to potrebno za zavarovanje dokazov v internem postopku ali v postopkih pred pristojnimi organi in za to obstaja ustrezna pravna podlaga. To dejanje se vpiše v evidenco.

#### 7. člen

##### DELOVANJE IN HRAMBA

Sistem deluje senzorično. Ob zaznavi gibanja se sproži alarmni dogodek, pri katerem senzor zajame zaporedje fotografij v nadzorovanem območju. Število zajetih fotografij se določi v nastavitvah sistema, pri čemer se v Dijaškem domu praviloma uporablja nastavitvev treh (3) fotografij na alarmni dogodek.

Sistem ne omogoča neprekinjenega snemanja videa, zvočnega snemanja ali stalnega spremljanja prostora v živo.

Fotografije, zajete ob alarmnem dogodku, se prenašajo v virtualno shrambo Ajax Cloud, od koder so preko aplikacije dostopne pooblaščenim uporabnikom sistema. Proizvajalec v podporni dokumentaciji navaja, da se fotografije iz MotionCam detektorjev prenašajo v virtualno shrambo na Ajax Cloud strežniku, ki gostuje na infrastrukturi Amazon Web Services, in da so fotografije v tej shrambi zaščitene z AES-256 šifriranjem. Prav tako proizvajalec navaja, da se v aplikacijah Ajax fotografije hranijo do sistemskih omejitev hrambe (do 500 dogodkov, ki jih zabeleži sistem). Zaradi tehničnih značilnosti

sistema se podatki shranjujejo v omejenem obsegu in se samodejno brišejo oziroma prepisujejo po načelu krožnega zapisa (FIFO), ko je dosežena zmogljivost sistema.

Sistem ne omogoča individualnega brisanja posameznih zapisov v evidenci dogodkov. Fotografije se samodejno izbrišejo po preteku roka hrambe zaradi tehničnih omejitev sistema.

Upravljalca redno spremlja splošne pogoje in obvestila proizvajalca, ki se nanašajo na zasebnost in varnost obdelave.

#### 8. člen

Posamezniki, na katere se nanašajo osebni podatki, lahko pri upravljalcu uveljavljajo pravico do dostopa do osebnih podatkov, pravico do omejitve obdelave, pravico do ugovora, pravico do izbrisa, kadar so za to izpolnjeni pogoji, ter druge pravice, določene z GDPR in ZVOP-2. Upravljalca o zahtevi odloči v zakonskem roku in ob upoštevanju omejitev, ki izhajajo iz varstva pravic drugih oseb, varovanja dokazov ali drugih zakonitih razlogov.

Če posameznik meni, da se njegovi osebni podatki obdelujejo v nasprotju s predpisi, ima pravico vložiti pritožbo pri Informacijskem pooblaščenca Republike Slovenije.

#### 9. člen

#### KONČNE DOLOČBE

Ta Pravilnik začne veljati prvi dan po objavi na oglasni deski Dijaškega doma.

Za vprašanja obdelave in varovanja osebnih podatkov, ki v tem Pravilniku niso posebej urejena, se neposredno uporabljajo določbe GDPR, ZVOP-2 ter drugi veljavni predpisi s področja varstva osebnih podatkov in informacijske varnosti.

#### Priloge:

PRILOGA 1 – SEZNAM SENZORJEV Z VIZUALNO VERIFIKACIJO V DIJAŠKEM DOMU

PRILOGA 2 – SKLEP O UVEDBI SISTEMA ZAZNAVANJA GIBANJA Z VIZUALNO VERIFIKACIJO DOGODKOV

PRILOGA 3 – VZOREC EVIDENCE OBDELAVE

PRILOGA 4 – VZOREC SKLEPA O IMENOVANJU POOBlašČENIH OSEB

PRILOGA 5 – OBVESTILO O IZVAJANJU SISTEMA

PRILOGA 6 – OCENA UČINKOV V ZVEZI Z VARSTVOM OSEBNIH PODATKOV (DPIA)

Vipava, 15. 4. 2026

SVET ZAVODA ŠKOFIJSKE GIMNAZIJE VIPAVA





## PRILOGA 1: SEZNAM SENZORJEV V DIJAŠKEM DOMU

(1) Na naslovu Dijaškega doma ŠGV so nameščeni naslednji senzori:

- *vhod na recepciji (en senzor – oznaka 1)*
- *stranski vhod v skupnih prostorih (en senzor – oznaka 2)*
- *vhod pri kapeli (en senzor – oznaka 10)*
- *na hodniku v prvem nadstropju dekliške stavbe (en senzor – oznaka 1-6)*
- *na hodniku drugega nadstropja dekliške stavbe (en senzor – oznaka 2-4)*
- *na hodniku tretjega nadstropja dekliške stavbe (en senzor – oznaka 3-5)*
- *na hodniku mansarde dekliške stavbe (en senzor – oznaka 4-3)*
- *na hodniku prvega nadstropja fantovske stavbe (en senzor – oznaka 1-7)*
- *na hodniku drugega nadstropja fantovske stavbe (en senzor – oznaka 2-8)*
- *na hodniku mansarde fantovske stavbe (en senzor – oznaka 3-9)*

## PRILOGA 2: SKLEP O UVEDBI SISTEMA ZAZNAVANJA GIBANJA Z VIZUALNO VERIFIKACIJO DOGODKOV

Zavod Škofijska gimnazija Vipava  
Goriška cesta 29  
5271 Vipava

Na podlagi 76. člena Zakona o varstvu osebnih podatkov (ZVOP-2) in Pravilnika o sistemu zaznavanja gibanja z vizualno verifikacijo dogodkov ravnatelj izda naslednji:

**SKLEP O UVEDBI SISTEMA ZAZNAVANJA GIBANJA Z VIZUALNO VERIFIKACIJO DOGODKOV V  
DIJAŠKEM DOMU ŠKOFIJSKE GIMNAZIJE VIPAVA**

Z dnem \_\_\_\_\_ se v Dijaškem domu Škofijske gimnazije Vipava, Grabrijanova ulica 19, 5271 Vipava, uvede sistem zaznavanja gibanja z vizualno verifikacijo dogodkov na naslednjih lokacijah:

1. **Vhod recepcija:** en senzor (oznaka 1)
2. **Stranski vhod skupni prostori:** en senzor (oznaka 2)
3. **Vhod pri kapeli:** en senzor (oznaka 10)
4. **Hodnik 1. nadstropja dekliške stavbe:** en senzor (oznaka 1-6)
5. **Hodnik 2. nadstropja dekliške stavbe:** en senzor (oznaka 2-4)
6. **Hodnik 3. nadstropja dekliške stavbe:** en senzor (oznaka 3-5)
7. **Hodnik mansarde dekliške stavbe:** en senzor (oznaka 4-3)
8. **Hodnik 1. nadstropja fantovske stavbe:** en senzor (oznaka 1-7)
9. **Hodnik 2. nadstropja fantovske stavbe:** en senzor (oznaka 2-8)
10. **Hodnik mansarde fantovske stavbe:** en senzor (oznaka 3-9)

**OBRAZLOŽITEV:**

Sistem se uvaja izključno za varovanje življenja in zdravja dijakov, zaposlenih in obiskovalcev ter za varovanje premoženja Dijaškega doma in preprečevanje vandalizma v času nočnega počitka zaradi v preteklosti zaznanih varnostnih incidentov. Sistem ni namenjen nadzoru zaposlenih ali dijakov, temveč izključno hitri in zanesljivi potrditvi varnostnega incidenta. Senzorji so nameščeni le v skupnih prostorih in na hodnikih; v sobe, sanitarije in druge prostore, kjer se pričakuje visoka stopnja zasebnosti, niso nameščeni. Fotografije se zajamejo le ob sprožitvi alarmnega dogodka in se hranijo največ tri (3) mesece, razen v primeru, ko so potrebne za izvedbo postopkov pred pristojnimi organi ali za zavarovanje dokazov oz. do roka, ki jih določajo veljavni predpisi. Upravljelec nima vzpostavljenih neobičajnih nadaljnjih obdelav ali prenosov v tretje države. Informacije in dostop: Več informacij je na voljo na tel. št. 05 365 50 00, na e-naslovu [info@sgv.si](mailto:info@sgv.si) ali na spletni strani [www.sgv.si](http://www.sgv.si). Osebnne podatke v evidenci lahko obdelujeta le ravnatelj ter s posebnim sklepom pooblaščen oseba skladno s Pravilnikom o sistemu zaznavanja gibanja z vizualno verifikacijo dogodkov.

Melita Košir,  
ravnateljica SGV



## PRILOGA 3: VZOREC OBRAZCEV

Upravljaec dnevnika oz. evidence obdelave vodi skladno s smernicami Informacijskega pooblaščenca. Vsi obrazci so dostopni na:

[https://www.ip-rs.si/fileadmin/user\\_upload/Pdf/obrazci/novi\\_obrazci/EVIDENCA\\_UPORABE\\_VIDEONADZORNEGA\\_SISTEMA.pdf](https://www.ip-rs.si/fileadmin/user_upload/Pdf/obrazci/novi_obrazci/EVIDENCA_UPORABE_VIDEONADZORNEGA_SISTEMA.pdf)

Upravljaec vodi evidenco obdelave oziroma dnevnik vpogledov, ki vsebuje najmanj naslednje podatke:

Datum in čas	Pooblaščenca oseba	Dogodek/lokacija	Dejanje	Namen/pravna podlaga	Opombe

V evidenco se vpisujejo vpogledi v fotografije, izvozi, posredovanja pristojnim organom, spremembe nastavitve sistema, okvare in servisni posegi.

Evidenca se lahko vodi tudi v elektronski obliki v datoteki, ki se nahaja na računalniku za dostop.

**PRILOGA 4: VZOREC SKLEPA O IMENOVANJU POOBLAŠČENIH OSEB**

Na podlagi 76. člena Zakona o varstvu osebnih podatkov (Ur. list RS, št. 163/22 ZVOP-2) ter Pravilnika o sistemu zaznavanja gibanja z vizualno verifikacijo dogodkov imenujem

[VSTAVITI IME IN PRIIMEK OSEBE TER NAZIV],

kot pooblaščen osebo za upravljanje sistema, pregled fotografij in vodenje evidence obdelave skladno s Pravilnikom.

V Vipavi, [VSTAVITI DATUM]



Melita Košir,  
ravnateljica ŠGV

## PRILOGA 5: VZOREC OBVESTILA O IZVAJANJU SISTEMA

**OBMOČJE JE VAROVANO S SISTEMOM ZAZNAVANJA GIBANJA Z VIZUALNO VERIFIKACIJO DOGODKOV**

- Upravljaivec sistema: Zavod Škofijska gimnazija Vipava, Goriška cesta 29, 5271 Vipava.
- Kontaktni podatki: tel: 05 365 50 00, e-naslov: info@sgv.si
- Pooblaščenca oseba za varstvo podatkov (DPO): [dpo@datainfo.si](mailto:dpo@datainfo.si)
- Namen obdelave fotografij: Sistem se izvaja izključno za namene varovanja življenja in zdravja dijakov, zaposlenih in obiskovalcev ter varovanja premoženja Dijaškega doma, preprečevanje vandalizma, ugotavljanje okoliščin varnostnih incidentov in preverjanje upravičenosti alarmnega dogodka v času nočnega počitka ter v času šolskih počitnic ter vikenda ter deluje 24 ur dnevno, kadar v objektu ni prisotnih dijakov, zaposlenih ali drugih oseb, in je to potrebno za varovanje premoženja ali preprečevanje varnostnih incidentov.
- Opis sistema: V skupnih prostorih in na hodnikih so nameščeni senzorji gibanja, ki ob sprožitvi alarmnega dogodka zajamejo fotografije za preverjanje upravičenosti alarma. Sistem ne izvaja stalnega snemanja videa in ne omogoča zvočnega snemanja.
- Pravna podlaga je zakoniti interes, kot ga določa točka (f) prvega odstavka 6. člena Splošne uredbe o varstvu podatkov (GDPR) - namen varovanja življenja in zdravja dijakov, zaposlenih in obiskovalcev ter varovanja premoženja Dijaškega doma, preprečevanje vandalizma, ugotavljanje okoliščin varnostnih incidentov in preverjanje upravičenosti alarmnega dogodka v času nočnega počitka.
- Uporabniki podatkov: Pooblaščenca osebe Upravljalca, zunanji vzdrževalec sistema (le v okviru vzdrževanja opreme) ali drugi pristojni organi na podlagi zakonske zahteve.
- Informacije o posebnih vplivih obdelave: obdelava ne vključuje posebnih vplivov, ki bi prekomerno posegali v zasebnost posameznikov izven določenih namenov.

- Rok hrambe: največ tri (3) mesece oziroma do sistemskih omejitev hrambe, razen v primeru, ko je hramba potrebna zaradi postopka ali zavarovanja dokazov vendar najdlje v roku, ki ga določajo veljavni predpisi
  
- Neobičajne nadaljnje obdelave:
  - Prenos v tretje države: Se ne izvaja.
  - Spremljanje v živo: Se ne izvaja.
  - Zvočna intervencija: Se ne izvaja.
  - Prenos na mobilne naprave: Se ne izvaja (onemogočeno).
  
- Informacije o obstoju in uveljavljanju pravic: posamezniki lahko svoje pravice (dostop, popravek ali izbris osebnih podatkov ali omejitev obdelave ter pravico do ugovora in prenosljivosti podatkov) skladno s 13. členom GDPR uveljavljajo pri upravljalcu na zgoraj navedenih kontaktih oziroma vložijo pritožbo pri Informacijskem pooblaščenču. Več informacij o pravicah je na voljo na spletnem naslovu: <https://sgv.si/politika-varstva-osebni-podatkov/>
  
- Informacija o pravici do vložitve pritožbe pri nadzornem organu: Pritožbo lahko podate Informacijskemu pooblaščenču (naslov: Dunajska 22, 1000 Ljubljana, e-naslov: gp.ip@ip-rs.si telefon: 012309730, spletna stran: [www.ip-rs.si](http://www.ip-rs.si)).

**PRILOGA 6: OCENA UČINKOV V ZVEZI Z VARSTVOM OSEBNIH PODATKOV (DPIA)****OCENA UČINKOV V ZVEZI Z VARSTVOM OSEBNIH PODATKOV (DPIA)****1. Opis obdelave**

V Dijaškem domu je nameščen sistem Ajax, ki ob zaznavi gibanja v skupnih prostorih in na hodnikih v času nočnega počitka zajame zaporedje fotografij za preverjanje alarmnega dogodka. Sistem ne omogoča neprekinjenega videonadzora, snemanja zvoka ali trajnega spremljanja prostora.

**2. Namen obdelave**

Namen obdelave je varovanje oseb in premoženja, preprečevanje vandalizma, hitro preverjanje resničnosti alarmnega dogodka ter zavarovanje dokazov ob morebitnem varnostnem incidentu.

**3. Kategorije podatkov in posameznikov**

Obdelujejo se fotografije oseb, ki se znajdejo v zaznavnem območju sensorja ob alarmnem dogodku, ter metapodatki o času in lokaciji dogodka. Posamezniki so dijaki in dijakinje, zaposleni, obiskovalci in druge osebe, ki se v času delovanja sistema zakonito ali nezakonito nahajajo v varovanem območju.

**4. Presoja nujnosti in sorazmernosti**

Sistem je omejen na skupne prostore in deluje le v času nočnega počitka. Ne posega v sobe, sanitarije ali druge posebej varovane zasebne prostore. V primerjavi s klasičnim videonadzorom gre za manj invaziven ukrep, saj se zajemajo le fotografije ob alarmu in ne neprekinjen video zapis.

**5. Tveganja za pravice in svoboščine posameznikov**

- možnost nepooblaščenega dostopa do zajetih fotografij;
- tveganje prekomernega vpogleda v osebne podatke brez utemeljenega razloga;
- tveganje, povezano s hrambo v oblaku in morebitnim čezmejnim prenosom podatkov;
- tveganje, da bi posameznik ob neustreznem obveščanju ne bil vnaprej seznanjen z obdelavo.

**6. Ukrepi za zmanjšanje tveganj**

- omejevanje sistema na skupne prostore in nočni čas;
- uporaba avtentificiranih uporabniških računov in omejitev dostopnih pravic;
- uporaba zaščiteneh naprav za dostop do aplikacije;
- vodenje evidence vpogledov, izvozov in servisnih posegov;
- objava jasnega obvestila in internih informacij o delovanju sistema;
- samodejno brisanje fotografij po poteku roka hrambe;
- redno spremljanje informacij proizvajalca glede varnosti, zasebnosti in prenosa podatkov.

**7. Ocena preostalega tveganja**

Po izvedbi navedenih organizacijskih in tehničnih ukrepov upravljalec ocenjuje, da je preostalo tveganje za pravice in svoboščine posameznikov nizko do srednje in sorazmerno z zasledovanim legitimnim ciljem varovanja oseb in premoženja in ne povzroča velikega tveganja za pravice in svoboščine posameznikov.

**8. Sklep**

Na podlagi te ocene upravljalec ugotavlja, da je uporaba sistema ob upoštevanju tega Pravilnika dopustna in skladna z načeli varstva osebnih podatkov, pod pogojem rednega pregleda delovanja



sistema, osveževanja DPIA, preverjanja nastavitev hrambe in spremljanja pogojev proizvajalca glede obdelave v oblaku.

