Ekonomska gimnazija in srednja šola Radovljica

P R A V I L N I K

o video nadzornem
in protivlomnem alarmnem sistemu ter
zaščiti računalniških podatkov šolskega IS

Radovljica, 11. december 2018

Na osnovi 24. in 25. člena Zakona o varstvu osebnih podatkov (Ur. l. št. 94/07 ZVOP-1-UPB1) je ravnateljica Ekonomske gimnazije in srednje šole Radovljica sprejela

P R A V I L N I K
o video nadzornem in protivlomnem alarmnem sistemu ter zaščiti računalniških podatkov

I. SPLOŠNA DOLOČBA

1. člen

S tem pravilnikom Ekonomska gimnazija in srednja šola Radovljica podrobneje ureja:

- način uporabe video nadzornega sistema,
- odrejanje snemanja,
- ravnanje s posnetki ter nadzor nad uporabo,
- upravljanje protivlomnega alarmnega sistema,
- način varovanja osebnih podatkov v računalniški obliki na šolskem informacijskem sistemu

v vseh objektih Ekonomske gimnazije in srednje šole Radovljica (v nadaljevanju: objekti šole).

2. člen

Video nadzor se uvede zaradi varnosti:

- dijakov,
- zaposlenih,
- obiskovalcev in
- premoženja.

Z video nadzorom se lahko nadzoruje vhod v šolo, garderoba v avli in vstop v snemalni studio.

3. člen

Zbirka osebnih podatkov po tem členu vsebuje:

- sliko,
- datum in
- čas posnetka.

II. NAMEN SISTEMOV

4. člen

Namen video nadzornega sistema v objektih šole je:

- zagotavljanje varovanja in varnosti dijakov, zaposlenih in obiskovalcev,
- zagotavljanje nadzora vstopa v šolo ali izstopa iz šole ter
- varovanje nepremičnin in opreme v objektih in okolice šole.

Video nadzorni sistem, s katerim se izvaja video nadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.

5. člen

Šola ima vgrajen video sistem za video nadzor in snemanje tudi v času, ko šola ne posluje.

6. člen

Namen protivlomnega alarmnega sistema v objektih šole je varovanje nepremičnin in opreme v objektih šole, ko ni nihče prisoten v šoli.

7. člen

Namen zaščite računalniških podatkov šolskega IS je onemogočiti nepooblaščenim osebam dostop do informacijsko-komunikacijskih naprav, na katerih se obdelujejo osebni podatki, in do njihovih zbirk. Zagotavlja varnost posredovanja in prenosa osebnih podatkov ter omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki uporabljeni, kdaj vnešeni v zbirko podatkov, kdo je bil izvajalec oz. uporabnik, in sicer za obdobje, za katero se posamezni podatki shranjujejo.

III. UPRAVLJANJE Z VIDEO NADZOROM

8. člen

Odgovorna oseba šole (v nadaljevanju ravnatelj):
a) je pristojna za:

- izdajo sklepa o video nadzoru,
- pisno obveščanje zaposlenih delavcev,
- objavo obvestila o izvajanju video nadzora in
- pridobitev mnenja sindikata šole.

b) odloča o:

- upravičenosti vpogleda in dajanju informacij o posnetkih ter
- shranjevanju posnetkov na prenosne medije.

c) določi osebo, ki je odgovorna za:

- upravljanje z video sistemom,
- pregledovanje posnetkov,
- vodenje evidence vpogledov,
- daje informacije o posnetkih,
- odloča o shranjevanju posnetkov na prenosne medije.

9. člen

O uporabi video sistema se vodi poseben dnevnik, kamor se vpisujejo:

- spremembe nastavitev,
- okvare in tehnične težave pri delovanju,
- servisni posegi.

Dnevnik vodi operater sistema.

10. člen

Video posnetki se hranijo najmanj 30 dni in največ 1 leto za vse kamere, ki so priključene na napravo za snemanje. Nato se podatki zbrišejo, če ni z zakonom določeno drugače.

Prenos posameznih dogodkov na prenosne medije lahko odobri odgovorna oseba, ko oceni, da je potrebno zagotoviti dokazno gradivo v:

- pritožbenem,
- odškodninskem,
- disciplinskem ali kazenskem postopku.

Video posnetki imajo oznako tajnosti "interno" in se hranijo skladno s predpisi, ki urejajo hrambo tajnih podatkov in hrambo osebnih podatkov.

11. člen

Če video posnetki določenega dogodka ali stanja kažejo na sum kaznivega dejanja, je treba o tem obvestiti policijo. Na pisno zahtevo policije se posnetek izroči v tiskani obliki ali na prenosnem mediju.

IV. UPRAVLJANJE S PROTIVLOMNIM ALARMNIM SISTEMOM

12. člen

Upravičenci, katerim so dodeljeni generalni ključi vrat za vstop v šolo, morajo obvezno dobiti posebno šifro za vklapljanje in izklapljanje alarmnega sistema.

13. člen

Šifro za vključitev in izključitev protivlomnega alarmnega sistema določi ravnatelj vsakemu upravičencu posebej.

S šiframi protivlomnega alarmnega sistema upravičencev je lahko seznanjen samo hišnik šole, razen s šifro, ki jo uporablja ravnatelj. Ta je znana samo ravnatelju.

Za tajnost šifre protivlomnega alarmnega sistema odgovarja vsak osebno.

Vsaka zloraba šifre protivlomnega alarmnega sistema in zaupanih ključev se smatra kot hujša kršitev delovne obveznosti.

14. člen

Protivlomni alarmni sistem ob vstopu v objekt izklopi zaposleni, ki prvi vstopi v objekt, in vklopi zaposleni, ki zadnji zapusti objekt.

V. OBVEŠČANJE O VIDEO NADZORU in PROTIVLOMNEMU SISTEMU

15. člen

Šola mora o video nadzoru obvestiti vse zaposlene in dijake ter objaviti obvestilo, ki mora biti vidno in tako objavljeno, da se posameznik seznani z njegovim izvajanjem najkasneje, ko se nad njim prične izvajati video nadzor.

Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:
1. da se izvaja video nadzor (in protivlomni alarmni sistem),
2. naziv osebe šole, ki ga izvaja,
3. telefonska številka za pridobitev informacij, kje in koliko časa se shranjujejo posnetki iz video nadzornega sistema.

Šteje se, da je z obvestilom iz drugega odstavka tega člena posameznik obveščen o obdelavi osebnih podatkov po 19. členu Zakona o varstvu osebnih podatkov (Ur. l. št. 94/07 ZVOP-1-UPB1).

V. TEHNIČNE ZAHTEVE VIDEO NADZORNEGA IN PROTIVLOMNEGA ALARMNEGA SISTEMA

16. člen

Sistem za video nadzor namesti in tehnično vzdržuje pooblaščeni izvajalec.

17. člen

Mesto namestitve kamere ter njena funkcija sta določena z načrtom varovanja. S kamero se nadzira:
- vhod v šolo in parkirišče,
- avla in prostor z garderobnimi omaricami,
- vhod v telovadnico (avla) in
- vhod v video učilnico.

18. člen

Kamer ni dovoljeno nameščati zlasti v:
- garderobah za preoblačenje,
- dvigalih,
- sanitarnih prostorih dijakov in osebja šole,
- učilnicah ter
- kabinetih.

19. člen

Naprava za snemanje mora imeti naslednje funkcije:
– da je dostop do nastavitev možen samo s posebnim vstopnim geslom.

20. člen

Video nadzorni sistem se nahaja v arhivu in mora biti nameščen tako, da druge osebe nimajo vpogleda v prikazovalnike posnetkov.

21. člen

Video sistem je lahko v času, ko ni nihče prisoten v šoli, povezan s pooblaščenim zunanjim pogodbenim izvajalcem, ki mora imeti licenco za izvajanje tehničnega varovanja in vzdrževanja.

Posnetke videonadzornega sistema pregleduje ravnateljica in od nje pooblaščena oseba.

22. člen

Senzorji protivlomnega alarmnega sistema so nameščeni po načrtu tako, da je zagotovljeno varovanje kritičnih mest, za katere je ocenjeno, da bi lahko prišlo da nasilnega vstopa.

23. člen

Protivlomni alarmni sistem mora biti vezan na pooblaščenega pogodbenega izvajalca, ki mora imeti licenco za izvajanje tehničnega varovanja in vzdrževanja.

VI. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

24. člen

Prostori, kjer se nahajajo računalniški podatki oz. šolski strežniki, ki so glavni nosilci varovanih osebnih podatkov, morajo biti varovani z organizacijskimi ter fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop v te prostore je mogoč in dopusten le v delovnem času in samo za zaposlene.

Vsi računalniki ali druga strojna oprema, na kateri se obdelujejo ali hranijo osebni podatki, morajo biti izven delovnega časa izklopljeni in fizično ali programsko zaklenjeni, da je dostop do osebnih podatkov hranjenih na diskih računalnika nepooblaščenim osebam onemogočen.

Delavec, ki dela v tako varovanih prostorih, mora vestno in skrbno nadzorovati prostor in ob zapustitvi prostora zakleniti prostor.

Zaposleni delavci in čistilke se lahko gibljejo v varovanih prostorih izven delovnega časa in brez prisotnosti odgovornega vzdrževalca le, če so nosilci podatkov shranjeni v zaklenjenih omarah na način, ki ga določa ta pravilnik za čas izven delovnega časa.

25. člen

Delavec, ki pri svojem delu uporablja osebne podatke ali jih kakorkoli obdeluje, ne sme med delovnim časom puščati nosilcev osebnih podatkov na pisalnih mizah ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam.

Nosilcev osebnih podatkov delavci EGSŠ Radovljica ne smejo odnašati izven šole brez izrecnega dovoljenja ravnatelja. Posredovanje osebnih podatkov pooblaščenim eksternim institucijam in drugim, ki izkažejo zakonsko podlago za pridobitev osebnih podatkov, dovoli ravnatelj.

26. člen

Vzdrževanje in popravilo strojne računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z vednostjo in odobritvijo pooblaščene osebe, izvajajo pa ga lahko samo šolski vzdrževalec učne tehnologije ter pooblaščeni servisi in njihovi vzdrževalci ob spremstvu oz. nadzoru šolskega vzdrževalca. Zunanji izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

Vzdrževalec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

V času servisiranja računalnika in programske opreme mora biti vzdrževalec ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki.

V primeru izkazane potrebe po popravilu računalnika, na čigar disku se nahajajo šolski podatki, izven EGSŠ Radovljica in brez kontrole pooblaščenega vzdrževalca se morajo podatki iz diska računalnika izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč, se mora popravilo obvezno opraviti v poslovnih prostorih EGSŠ Radovljica v prisotnosti pooblaščenega vzdrževalca.

27. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se dnevno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi in da se ugotovi vzrok pojava virusa.

Vsi podatki in programska oprema, ki so namenjeni uporabi na šolskih računalnikih in celotnem IS zavoda ter prispejo na medijih za prenos računalniških podatkov ali prek telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

28. člen

Dostop do podatkov prek aplikativne programske opreme mora biti varovan s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Vsa gesla in postopki, ki se uporabljajo za dostop ali za administriranje v mreži osebnih računalnikov, administriranje z elektronsko pošto in administriranje prek aplikativnih programov in so lahko v tiskani ali računalniški obliki, se lahko hranijo le v varovanih prostorih, kjer je vstop nezaposlenim prepovedan.

29. člen

Za potrebe restavriranja osebnih podatkov oziroma računalniškega sistema po okvarah ali izgubi podatkov iz drugih razlogov mora vzdrževalec, ki vodi zbirke osebnih podatkov, redno izdelovati kopije vsebine zbirk osebnih podatkov, ki jih vodi.

Računalniške kopije vsebin zbirk osebnih podatkov na USB ključih, zunanjih diskih ali drugih medijih se hranijo v zavarovanih prostorih, zaščitenih proti ognju, poplavam in elektromagnetnim motnjam ter so v predpisanih klimatskih razmerah.

30. člen

Vsebina zbirke osebnih podatkov, ki se prenašajo po komunikacijskih kanalih, po elektronski pošti ali fizično na računalniških medijih izven zavoda, se mora zaščititi z ustreznimi standardnimi kriptografskimi metodami.

31. člen

Osebni podatki se lahko vodijo v zbirki celotnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo. Po prenehanju potrebe po vodenju osebnih podatkov, se podatki zbrišejo oziroma uničijo nosilci podatkov.

Brisanje osebnih podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča restavriranje brisanih podatkov.

Uničevanje osebnih podatkov na nosilcih iz predhodnega odstavka se mora izvajati tekoče in ažurno.

VII. KONČNA DOLOČBA

32. člen

Ta pravilnik prične veljati naslednji dan po objavi na oglasni deski šole in v e-zbornici., uporabljati pa se začne takoj po objavi.

Datum: 11. december 2018 žig Ravnateljica:

Številka: Ksenija Lipovšček, univ. dipl. soc.

Priloge:

- obvestilo za vrata in obvestilo zaposlenih (1),
- seznam lokacij kamer video nadzornega sistema (2),
- seznam oseb, ki lahko odklepajo šolo in upravljajo z alarmnim sistemom (3),
- seznam oseb, ki so pooblaščene za administriranje v mreži računalnikov (4),
- seznam oseb, ki imajo kodo od ognjevarne omare v arhivu (5),
- zapis posveta s sindikatom (6),
- sklep o uvedbi videonadzora (7),
- Imenovanje pooblaščene osebe za videonadzor: (8 /1-3)
    - za upravljanje videonadzornega sistema,
    - za pregledovanje posnetkov videonadzornega sistema
    - za vodenje evidence videonadzornega sistema**.**

Opomba:

1. *Načrt varovanja mora izdelati izvajalec sistemov.*
2. *Priloži se samo zapis (ne soglasje) s posveta s sindikatom.*