C Š O D
CENTER ŠOLSKIH
IN OBŠOLSKIH DEJAVNOSTI

# *PRAVILNIK*

## o zavarovanju osebnih podatkov

**Center šolskih in obšolskih dejavnosti**

Frankopanska ulica 9, 1000 Ljubljana

C Š O D
CENTER ŠOLSKIH
IN OBŠOLSKIH DEJAVNOSTI

Na podlagi 19. člena Statuta Centra šolskih in obšolskih dejavnosti ob upoštevanju vsebine 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 (v nadaljevanju Splošna uredba) in na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, 94/07 – UPB ) direktor sprejema naslednji

# PRAVILNIK
# o zavarovanju osebnih podatkov

## I. SPLOŠNE DOLOČBE

1. člen
(Vsebina in namen pravilnika)

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov v Centru šolskih in obšolskih dejavnosti (v nadaljevanju CŠOD) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

S tem Pravilnikom se določijo osebe, ki so odgovorne za posamezne evidence obdelav osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo posamezne osebne podatke, s katerimi upravlja upravljavec in jih obdeluje.

Ta Pravilnik določa ukrepe za zavarovanje pri zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi osebnih podatkov pri upravljavcu.

Določbe tega Pravilnika veljajo za vse vodene zbirke podatkov pri upravljavcu, ne glede na obliko, v kateri je osebni podatek izražen.

Varstvo osebnih podatkov se zagotavlja vsakemu posamezniku, ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, ali katerokoli drugo osebno okoliščino.

V zadevah, ki jih ne ureja ta Pravilnik, se neposredno uporablja zakonodaja, ki ureja varstvo osebnih podatkov.

Ta pravilnik velja za zaposlene delavce[1] v CŠOD ter vse delavce, ki v CŠOD opravljajo dela in naloge po drugih oblikah dela (študentsko delo, dijaki na praksi, podjemne pogodbe, pogodbe o začasnem delu, naročilnice, druge pogodbe).

2. člen
(Varovani osebni podatki)

Za varovane osebne podatke štejejo tisti podatki, ki predstavljajo katerokoli informacijo v zvezi z določenim ali določljivim posameznikom, ne glede na obliko, v katero so izraženi. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto posameznika.

[1] V besedilu dokumenta uporabljeni izrazi, zapisani v moški slovnični obliki, so uporabljeni kot nevtralni za ženske in moške.

V smislu določbe 1. odstavka tega člena štejejo za osebne podatke o posamezniku zlasti:

- identifikacijski podatki o posamezniku,
- podatki, ki se nanašajo na rasno poreklo in pripadnost narodu ali narodnosti,
- podatki, ki se nanašajo na družinska razmerja,
- podatki, ki se nanašajo na stanovanjske in bivalne pogoje posameznika,
- podatki o zaposlitvi,
- podatki o socialnem in ekonomskem stanju posameznika,
- podatki o izobrazbi in pridobljenih znanjih,
- slikovni (in glasovni) podatki nadzornih video sistemov,
- podatki o uporabi komunikacijskih sredstev,
- podatki o aktivnostih v prostem času,
- podatki o zdravstvenem stanju posameznika,
- podatki o ideoloških in verskih prepričanjih,
- podatki o posamezniku na področju notranjih zadev,
- podatki o navadah posameznika.

3. člen

Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logistično-tehnične postopke in ukrepe za zagotavljanje skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, zakona, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo varstvo osebnih podatkov, s katerimi se:

- varujejo prostori, strojna in sistemska programska oprema;
- varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
- zagotavlja varnost posredovanja in prenosa osebnih podatkov;
- onemogoča nepooblaščenim osebam dostop do računalniških sistemov, na katerih se obdelujejo osebni podatki in dostop do podatkovnih zbirk;
- omogoča naknadno ugotavljanje, kdaj so bili posamezni podatki vneseni v podatkovne zbirke, oziroma računalniške sisteme, kdaj in kdo je dostopal do njih in to v obdobju, za katero se posamezni podatki shranjujejo.

4. člen

Obdelava in zavarovanje posebnih vrst osebnih podatkov, med katere sodijo podatki o rasnem ali etničnem poreklu, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo, morata biti izvajana posebno vestno in skrbno.

5. člen
(Pomen izrazov)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Osebni podatek** - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;

2. **Posameznik** - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo fizično, fiziološko,

duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa;

3. **Zbirka osebnih podatkov** - je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika;
4. **Obdelava osebnih podatkov** - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave);
5. **Upravljavec osebnih podatkov** - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave; v pravilniku se pojem upravljavec nanaša na CŠOD;
6. **Občutljivi osebni podatki** - so podatki o rasnem narodnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;
7. **Uporabnik osebnih podatkov** - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
8. **Nosilec podatkov** - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.);
9. **Poslovna skrivnost** - so podatki, ki so označeni z oznako zaupnosti v skladu z Zakonom o gospodarskih družbah.

## II. OBDELAVA OSEBNIH PODATKOV

6. člen
(Vzpostavitev zbirke osebnih podatkov)

Vsi zaposleni in zunanji sodelavci pri upravljavcu, ki pri svojem delu uporabljajo osebne podatke, ki jih obdeluje upravljavec ali podatke, ki predstavljajo poslovno oziroma poklicno skrivnost ali imajo iz kakršnihkoli razlogov možnost dostopa do teh podatkov, morajo biti seznanjeni z določili Splošne uredbe, zakonom, ki ureja varstvo osebnih podatkov, zakonodajo, ki je podlaga za obdelavo posameznih osebnih podatkov, s tem Pravilnikom in s splošnimi akti, ki opredeljujejo poslovno oziroma poklicno skrivnost.

Posamezno zbirko osebnih podatkov na posameznem delovnem področju družbe vzpostavi pooblaščena oseba za določeno zbirko osebnih podatkov (v nadaljevanju: pooblaščena oseba zbirke), ki jo določi direktor.

7. člen
(Obdelava osebnih podatkov)

V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno zakonsko podlago po določbah zakona, ki ureja varstvo osebnih podatkov in Splošne uredbe.

Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače.

Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu določbami 13. in 14. člena Splošne uredbe.

Pooblaščene osebe zbirke ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke (v nadaljevanju: pooblaščeni obdelovalci), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami zakona, ki ureja varstvo osebnih podatkov ter z vsebino tega Pravilnika.

8. člen
(Evidenca dejavnosti obdelav osebnih podatkov – zbirke osebnih podatkov)

CŠOD, skladno s 30. členom Splošne uredbe, vodi evidenco dejavnosti obdelave osebnih podatkov (Obrazec je priloga tega Pravilnika). Evidenca dejavnosti obdelav osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Evidenco dejavnosti obdelav osebnih podatkov CŠOD vodi za osebne podatke, katerih upravljavec je, prav tako tudi za osebne podatke katere obdeluje kot pogodbeni obdelovalec.

Zaposleni, ki obdelujejo osebne podatke, morejo biti seznanjeni z evidenco dejavnosti obdelav osebnih podatkov, vpogled v evidenco dejavnosti obdelav osebnih podatkov pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

CŠOD vodi ažuren seznam (Obrazec je priloga tega Pravilnika), iz katerega je za vsako evidenco dejavnosti obdelav osebnih podatkov jasno razvidno, katera oseba je pooblaščena za posamezno evidenco obdelav osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno evidenco obdelav osebnih podatkov. V seznam se vpisujejo sledeči podatki: naziv evidence obdelav osebnih podatkov, osebno ime in delovno mesto osebe, ki je pooblaščena za evidenco dejavnosti obdelav osebnih podatkov ter osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov.

## III. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV DRUGIM UPORABNIKOM

9. člen
(Sprejem osebnih podatkov, pregledovanje pošte)

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora po zaključenem postopku evidentiranja izročiti poštno pošiljko z osebnimi podatki posamezniku, ali službi, na katero je ta pošiljka naslovljena na način, ki onemogoča vpogled v osebne podatke nepooblaščenim osebam.

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštne pošiljke in pošiljke, ki na drug način prispejo v CŠOD - prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku CŠOD in na ovojnici ni naveden CŠOD.

10.člen
(posredovanje osebnih podatkov zunanjim uporabnikom)

Osebni podatki se posredujejo samo tistim zunanjim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo. Osebni podatki se po uradni dolžnosti posredujejo samo tistim uporabnikom, ki imajo ustrezno zakonsko podlago.

Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne vloge mora uporabnik jasno navesti določbo zakona, ki ga pooblašča za pridobitev osebnih podatkov, ali pa mora k vlogi priložiti pisno zahtevo oziroma privolitev posameznika, na katerega se podatki nanašajo. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme pooblaščena oseba zbirke ali pooblaščeni obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

Upravljavec mora uporabniku ali drugemu upravljavcu, če zakon ne določa drugače, zahtevane osebne podatke posredovati najpozneje v 30-ih dneh od dne prejema popolne zahteve, ali pa ga v tem roku pisno obvestiti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

Posebne vrste osebnih podatkov (občutljivi osebni podatki) se pošiljajo naslovnikom v zaprtih ovojnicah priporočeno s povratnico ali z vročilnico.

Osebni podatki se pošiljajo priporočeno.

Obdelava posebne vrste osebnih podatkov mora biti posebej označena in zavarovana.

Posredovanje posebne vrste osebnih podatkov iz drugega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna vloga mora biti po vsebini enaka pisni vlogi iz drugega odstavka.

Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

Zaupne in osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim preprečujejo prilaščanje ali uničenje osebnih podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Posebne vrste osebne podatke je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

Originalni dokument, ki vsebuje osebne podatke, se lahko posreduje uporabniku samo na podlagi pisne odredbe sodišča. Posredovani originalni dokument mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

11.člen
(Evidenca posredovanj)

Vsako posredovanje osebnih podatkov iz prejšnjega člena se beleži v evidenco posredovanj, ki vsebuje navedbo naslednjih podatkov:

- komu se osebni podatki posredujejo, oziroma navedba, da je bilo posredovanje opravljeno po uradni dolžnosti,
- kateri podatki se posredujejo,
- kdaj so bili posredovani,
- na kakšni podlagi so bili posredovani,
- kdo je posredoval osebne podatke,
- oseba, ki so ji bili posredovani osebni podatki,
- oblika posredovanih osebnih podatkov.

Evidenco posredovanj (Obrazec je priloga tega Pravilnika) iz prvega odstavka tega člena zapiše odgovorna oseba ali pooblaščeni obdelovalec, ki je osebne podatke posredoval uporabniku.

V primeru pridobivanja in posredovanja osebnih podatkov med organi javne uprave, je potrebno upoštevati tudi določbe uredbe, ki ureja upravno poslovanje.

12.člen
(Posredovanje osebnih podatkov znotraj podjetja)

Dokumenti, ki vsebujejo osebne podatke zaposlenega, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo v skladu z 9. členom tega Pravilnika.

Osebni podatki zaposlenih in ostalih oseb se lahko posredujejo znotraj družbe tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.

Oseba iz drugega odstavka prejšnjega člena mora zapisati vsako posredovanje občutljivih osebnih podatkov znotraj družbe v skladu s prejšnjim členom.

13.člen
(Pregledovanje, prepisovanje in kopiranje osebnih podatkov s strani strank oziroma upravičencev)

Pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, je potrebno preveriti identiteto stranke oziroma vsakega drugega, ki verjetno izkaže, da ima od pregledovanja, prepisovanja in preslikovanja pravno korist (v nadaljevanju: upravičenec) z vpogledom v njegovo osebno izkaznico ali drug dokument, ki nedvoumno izkazuje njegovo istovetnost.

Pri vsakem posameznem pregledovanju, prepisovanju in kopiranju dokumentov po tem členu, ki vsebujejo osebne podatke, se zapiše uradni zaznamek, ki se vloži v spis. Iz uradnega zaznamka, ki ga mora podpisati tudi upravičenec, mora biti razviden datum in ura pregleda, vrsta dokumenta, katerega kopija se je posredovala upravičencu, osebno ime upravičenca, njegov naslov, številka in vrsta dokumenta, iz katerega je ugotovljena identiteta ter namen, zaradi katerega je bil opravljen pregled, prepis oziroma kopiranje dokumenta.

Upravičenca je pred pregledom, prepisovanjem in kopiranjem dokumentov, ki vsebujejo osebne podatke, potrebno opozoriti na dolžnost varovanja takšnih podatkov. Opozorilo mora biti sestavni del uradnega zaznamka iz prejšnjega odstavka.

14.člen

(Kopiranje in tiskanje osebnih podatkov s strani zaposlenih)

Osebe, ki pri izvajanju svojih delovnih nalog kopirajo, na drug tehnični način razmnožujejo ali tiskajo dokumente, ki vsebujejo osebne podatke, na napravah, ki jih uporablja večje število oseb, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah.

## IV. VAROVANJE PROSTOROV, NOSILCEV PODATKOV, STROJNE IN PROGRAMSKE OPREME

15.člen

(Varovanje prostorov)

Prostori, v katerih se nahajajo nosilci z osebnimi podatkov, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja direktorja, namestnika direktorja ali vodje enote.

Ključi varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključi se ne puščajo v ključavnici v vratih od zunanje strani.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Izven delovnega časa morajo biti prostori ali omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

Delavci ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

16.člen

(varovanje nosilcev s podatki)

Nosilci z osebnimi podatki, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

V prostorih, ki so namenjeni poslovanju s strankami, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni tako, da stranke nimajo vpogleda vanje.

Prepovedano je odnašanje nosilcev osebnih podatkov izven prostorov upravljavca brez predhodnega dovoljenja pooblaščenega delavca.

17.člen

S štampiljkami, papirjem z glavo CŠOD in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, je potrebno ravnati, kot z zaupnimi podatki.

18.člen

Komunikacijski kanali med zavarovanimi prostori, ki so prostorsko oddaljeni, morajo biti zavarovani pred nepooblaščenim pristopom. Vse povezave so opisane v načrtu komunikacijskih mrež, ki je sestavni del tega

pravilnika in je shranjen v zaprti ovojnici v trezorju, dostopen direktorju, namestniku direktorja in pooblaščeni osebi, zadolženi za delovanje računalniškega informacijskega sistema.

19.člen

Osebne podatke, ki se prenašajo po komunikacijskih kanalih, ali fizično na magnetnih medijih in so v času prenosa izven objektov upravljavca, je potrebno napraviti nečitljive z ustreznimi standardiziranimi kriptografskimi metodami.

20.člen
(vzdrževanje in popravila)

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo s CŠOD sklenjeno ustrezno pogodbo za varovanje osebnih podatkov.

21.člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v zavarovanih prostorih samo z vednostjo pooblaščene osebe. Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

## V. VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

22.člen
(dostop do programske opreme)

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

23.člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščene osebe, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo s CŠOD sklenjeno ustrezno pogodbo za varovanje osebnih podatkov. Upravljavci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

24.člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila, kot za ostale podatke iz tega pravilnika.

25.člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja glede na prisotnost računalniških virusov. Ob pojavu računalniškega virusa se tega čimprej odpravi s

pomočjo ustrezne strokovne službe CŠOD, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu CŠOD.

Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v CŠOD na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred uporabo preverjeni glede prisotnosti računalniških virusov.

26.člen

Delavci ne smejo inštalirati programske opreme brez vednosti pooblaščene osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz Centra šolskih in obšolskih dejavnosti brez odobritve direktorja in vednosti pooblaščene osebe, zadolžene za delovanje računalniškega informacijskega sistema.

27.člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

Direktor sprejme politiko dodeljevanja, hranjenja in spreminjanja gesel.

28.člen
(gesla in njihova uporaba)

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska oz. nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnicah v trezorju in se jih varuje kot »uradna tajnost-strogo zaupno« pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

29.člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki tam nahajajo. Za izdelavo kopij je odgovoren vzdrževalec računalniškega informacijskega sistema. Če se podatki nahajajo na lokalnih delovnih postajah, je za rezervne kopije zadolžen uporabnik, oziroma vzdrževalec računalniškega informacijskega sistema, če je to tako dogovorjeno. Dinamiko predpiše direktor CŠOD.

Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

30.Člen

(Elektronska pošta in uporaba druge programske opreme na računalniku)

Elektronska pošta in računalnik se uporabljata v službene namene.

Ne glede na prejšnji odstavek se elektronska pošta in ostala programska oprema na računalniku lahko uporabljata v omejenem obsegu in razumnih mejah tudi v zasebne namene. Vsebina elektronske pošte v zasebne namene ne sme biti neprimerna ali žaljiva.

Oseba, zadolžena za delovanje računalniškega informacijskega sistema, lahko na posebej utemeljeno pisno zahtevo delodajalca, v prisotnosti komisije iz 4. odstavka tega člena, v izrednih primerih (nenadna odpoved delavca, smrt delavca, ali drug izreden dogodek) vpogleda v elektronsko pošto le, če je to nujno potrebno za vodenje delovnega procesa.

Vpogled v vsebino e-pošte zaposlenega opravi dvočlanska komisija, ki jo vsakokrat imenuje delodajalec. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik.

Če se pojavi utemeljen sum, da zaposleni ne spoštujejo omejitev iz drugega odstavka tega člena, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo delodajalca opravi nadzor količine uporabe elektronske pošte, a zgolj z vidika obsega priponk, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebine elektronske pošte.

O namenu uporabe elektronske pošte in ostale programske opreme iz prvega in drugega odstavka tega člena ter možnosti nadzora iz tretjega in četrtega odstavka tega člena mora biti zaposleni pisno obveščen. Kot zadostno obvestilo se šteje obvestilo vsem zaposlenim po e-pošti.

Vpogled v telefonske prometne podatke priključkov, katerih lastnik je CŠOD, lahko CŠOD zahteva od operaterjev telekomunikacijskih storitev ali vzdrževalca hišne centrale le takrat, kadar pride med družbo in zaposlenim do kakršnegakoli spora glede višine stroškov porabe konkretnega telefonskega priključka.

31.člen
(Internet)

Internet se uporablja v službene namene.

Ne glede na prejšnji odstavek se internet lahko uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene. Internetne strani, ki se pregledujejo v zasebne namene, ne smejo vsebovati neprimerne ali žaljive vsebine.

Direktor lahko s posebnim sklepom odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede pooblaščena oseba, zadolžena za delovanje računalniškega informacijskega sistema. O blokadi se obvesti vse zaposlene po elektronski pošti.

## VI. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

32.člen
(Pogodbena obdelava)

Upravljavec lahko zaupa posamezna opravila v zvezi z obdelavo osebnih podatkov zunanji pravni ali fizični osebi (pogodbeni obdelovalec), pri tem pa si mora upravljavec prizadevati, da pogodbeni obdelovalec zagotavlja zadostna jamstva o tem, da bo izvajal ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil obdelave s Splošno uredbo, zakonom, ki ureja področje varstva osebnih podatkov in tem Pravilnikom.

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (pogodbeni obdelovalec), se sklene pisna pogodba. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

Pogodbeni obdelovalci (zunanje pravne ali fizične osebe) smejo opravljati samo storitve obdelave osebnih podatkov v okviru naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pogodbeni obdelovalci, ki za CŠOD opravljajo dogovorjene storitve izven prostorov upravljavca, morajo imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta Pravilnik.

CŠOD vodi seznam pogodbenih obdelovalcev (Obrazec je priloga tega Pravilnika).

## VII. HRAMBA OSEBNIH PODATKOV

33.člen

Osebni podatek lahko upravljavec vodi v zbirki osebnih podatkov toliko časa, kolikor je potrebno, da se doseže namen, za katerega se podatki obdelujejo.

Osebni podatki se shranjujejo toliko časa, kolikor je rok hrambe, opredeljen v evidenci dejavnosti obdelave osebnih podatkov.

Po preteku roka hranjenja se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Za brisanje osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Osebni podatki v fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv (npr. rezalnik papirja).

Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

Prepovedano je odmetavati odpadne nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov (npr. v koš za smeti).

Pri prenosu nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja, je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov. O uničenju se sestavi ustrezen zapis.

Ob vsakokratnem uničenju se sestavi zapisnik. Področje arhiviranja in uničenja dokumentarnega gradiva se uredi s Pravilnikom o ravnanju z arhivskim in dokumentarnim gradivom v CŠOD.

## VIII. UKREPANJE OB SUMU (NEPOOBLAŠČENEGA DOSTOPA) KRŠITVE VARSTVA OSEBNIH PODATKOV

34.člen

Upravljavec mora zagotoviti ustrezne tehnične in organizacijske ukrepe, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

Delavci so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti direktorja, sami pa poskušajo takšno aktivnost preprečiti.

V primeru, da upravljavec ugotovi, da je v procesu obdelave osebnih podatkov prišlo do slučajnega, namernega ali drugačnega nezakonitega uničenja, spremembe, izgube, nepooblaščenega razkritja, dostopa ali druge oblike nepooblaščene obdelave, je dolžan upravljavec brez nepotrebnega odlašanja, oziroma najpozneje v 72 urah po seznanitvi s kršitvijo, o kršitvi uradno obvesti pristojni nadzorni organ (Informacijskega pooblaščenca).

Ta obveznost upravljavca ni podana, če ni izkazana verjetnost, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, na katere se kršitev nanaša.

Uradno obvestilo (Obrazec je priloga tega pravilnika) iz 3. odstavka tega člena nadzornemu organu mora vsebovati vsaj naslednje podatke:

- opis vrste kršitve varstva osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov;
- sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
- opis verjetnih posledic kršitve varstva osebnih podatkov;
- opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve.

Ob navedenih ukrepih mora upravljavec ozaveščati osebe, udeležene v postopkih obdelave podatkov o varnostnih politikah ter postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov (kot npr.: odjavljanje iz sistema po zaključku dela, uporaba programskega zaklepanja računalnika ob odsotnosti od računalnika, zaklepanje prostorov ali stalni nadzor, politika čiste in urejene delovne mize in delovnega prostora, pomen zagotavljanja sledljivosti obdelave, vsak uporabnik uporablja svoje uporabniško ime in geslo, fizično varovanje gesel, previdnost pri izbiri gesel, občasno spreminjanje gesel, varno pošiljanje podatkov po elektronskih medijih, pazljivost in skrbnost pri posredovanju podatkov po telefonu, takojšnje obveščanje o incidentu, posvetovanje s pooblaščeno osebo za varstvo osebnih podatkov, upoštevanje notranjih pravil in aktov...).

## IX. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

35.člen
(Odgovornost za izvajanje in nadzor nad izvajanjem)

Za izvajanje predpisanih postopkov in ukrepov za zavarovanje zaupnih in osebnih podatkov je odgovoren direktor, ki imenuje tudi pooblaščene osebe.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem Pravilnikom, opravlja pooblaščena oseba za varstvo osebnih podatkov (DPO).

36.člen
(Izvajanje postopkov in ukrepov)

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem opravljanja dela in nalog za CŠOD.

37.člen
(Izjava)

Pred nastopom dela pri katerem se obdelujejo osebni podatki, mora delavec podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov (Obrazec je priloga tega Pravilnika).

38.člen
(Odgovornost za kršitve)

Za kršitev določil iz prejšnjega člena so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

## X. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

39.člen

Upravljavec mora posamezniku na njegovo zahtevo:

- omogočiti vpogled v dejavnosti obdelav osebnih podatkov – zbirke osebnih podatkov;
- potrditi, ali se podatki v zvezi z njim obdelujejo ali ne in mu omogočiti vpogled v osebne podatke, ki so vsebovani v evidenci obdelav osebnih podatkov in se nanašajo nanj, ter njihovo prepisovanje ali kopiranje (pravica do dostopa);
- dopolniti, popraviti, izbrisati, omejiti obdelavo osebnih podatkov, za katere posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom (pravica do popravka, do izbrisa, do omejitve obdelave),
- omogočiti ugovor v zvezi z obdelavo osebnih podatkov, ki se nanašajo nanj (pravica do ugovora)
- posredovati osebne podatke, ki jih je posameznik posredoval upravljavcu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in ima tudi pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral (pravica do prenosljivosti podatkov).

Upravljavec na zahtevo posameznika do seznanitve z osebnimi podatki zagotovi kopijo osebnih podatkov, ki se obdelujejo. Kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi, in če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače, upravljavec informacije zagotovi v elektronski obliki, ki je splošno uporabljana in je skladna s pravili posredovanja osebnih podatkov s tem Pravilnikom.

40.člen

Upravljavec osebnih podatkov mora posamezniku na njegovo zahtevo tudi:

- posredovati izpis osebnih podatkov, ki so vsebovani v evidenci obdelave osebnih podatkov in se nanašajo nanj;
- posredovati seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen;
- dati informacijo o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje evidenca obdelav osebnih podatkov, in o metodi obdelave;
- dati informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem;
- pojasniti tehnične oziroma logično-tehnične postopke odločanja, če izvaja avtomatizirano odločanje z obdelavo osebnih podatkov posameznika.

## XI. POSEBNE UREDITVE ZA ZBIRKE OSEBNIH PODATKOV VODENIH PRI UPRAVLJAVCU

41.člen
(Obdelava osebnih podatkov za katere je potrebna privolitev)

Pisno privolitev mora upravljavec pridobiti za obdelavo osebnih podatkov, katerih obdelava ni potrebna za izpolnitev zakonskih obveznosti, za izvajanje pogodbe, za zaščito življenjskih interesov, za izvajanje nalog v javnem interesu ali pri izvajanju javne oblasti ter zaradi zakonitih interesov za katere si prizadeva upravljavec.

Pisna privolitev iz predhodnega člena mora vsebovati:

- jasno opredeljeno voljo za izdajo soglasja,
- identiteto in kontaktne podatke upravljavca,
- kontaktne podatke pooblaščene osebe za varstvo osebnih podatkov,
- natančno opredeljen namen zbiranja podatkov in pravno podlago za obdelavo,
- navedbo podatkov, ki se zbirajo,
- uporabnike ali kategorije uporabnikov osebnih podatkov,
- zagotovilo, da se bodo podatki uporabljali le za namen za katerega so zbrani,
- čas shranjevanja podatkov,
- seznanitev z možnostjo preklica soglasja, ter z obstojem ostalih pravic, ki jih določa Splošna uredba,
- datum podpisa izjave in podpis osebe (če je privolitev v tiskani obliki, če je v e-obliki posameznik s klikom potrdi privolitev).

42.člen
(Videonadzor)

V primeru izvajanega videonadzora mora upravljavec osebnih podatkov o izvajanju videonadzora objaviti obvestilo. Obvestilo mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor.

Področje videonadzora je urejeno s Pravilnikom o videonadzoru v CŠOD.

## XII. KONČNE DOLOČBE

43.člen

Ta pravilnik začne veljati na dan, ko ga podpiše direktor in se objavi na spletni strani CŠOD, uporabljati pa se prične s 1.9.2018.

Številka dokumenta: 0072-0001/2018-1
V Ljubljani, 8.8.2018

Branko Kumer, MSc
Direktor

C Š O D
CENTER ŠOLSKIH
IN OBŠOLSKIH DEJAVNOSTI
LJUBLJANA, SLOVENIJA
1