

Na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Ur. l. RS, št. 94/07 – uradno prečiščeno besedilo) izdaja ravnateljica OŠ Brinje Grosuplje naslednji

Pravilnik o zavarovanju osebnih podatkov v OŠ Brinje Grosuplje

I. Splošne določbe

1. člen

(1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za zavarovanje osebnih podatkov vodenih v zbirkah osebnih podatkov v OŠ Brinje Grosuplje (v nadaljevanju zavod) z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov.

(2) Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z določbami Zakona o varstvu osebnih podatkov ter z vsebino tega pravilnika in Pravil o zavarovanju osebnih podatkov v OŠ Brinje Grosuplje.

(3) Za posamezna zakonsko urejena ravnanja v zvezi z zbiranjem, obdelavo, shranjevanjem in posredovanjem osebnih podatkov, ki niso urejena s tem pravilnikom, se neposredno uporabljajo določbe Zakona o varstvu osebnih podatkov in zakonov, ki urejajo posamezno pravno urejeno področje, na katerega se določen osebni podatek nanaša.

2. člen

Izrazi uporabljeni v tem pravilniku imajo naslednji pomen:

1. ZVOP-1: Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/2007 - uradno in prečiščeno besedilo);

2. Osebni podatek: katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;

3. Posameznik: 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;

4. Zbirka osebnih podatkov: 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;

5. Obdelava osebnih podatkov: 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);

6. Upravljavec osebnih podatkov: 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;

7. Občutljivi osebni podatki: podatki o rasmem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;

8. Uporabnik osebnih podatkov: fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;

9. Nosilec podatkov: vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilingi, naprave za prenos podatkov ipd.).

3. člen

Zavarovanje osebnih podatkov obsega organizacijske, tehnične, logično-tehnične in pravne postopke in ukrepe, s katerimi se:

- varujejo prostori ter strojna in programska (sistemska in aplikativna) oprema, na kateri so zapisani in s katero se obdelujejo osebni podatki,
- onemogoča dostop in vpogled v osebne podatke nepooblaščenim osebam,
- zagotavlja varnost posredovanja in prenosa osebnih podatkov,
- omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil ter
- zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov.

4. člen

(1) Opis zbirk osebnih podatkov, katerih upravljavec je OŠ Brinje Grosuplje (v nadaljevanju zavod), se vodi v katalogu zbirk osebnih podatkov (v nadaljevanju katalog), slednji pa se vodi v skladu z določbami 26. člena ZVOP-1.

(2) Podatki iz 1., 2., 4., 5., 6., 9., 10., 12. in 13. točke katalogov se posredujejo državnemu organu pristojnemu za vodenje registra zbirk osebnih podatkov (v nadaljevanju pristojni organ).

(3) Katalog se za vsako zbirko osebnih podatkov zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov, v istem roku pa se podatki iz kataloga posredujejo tudi pristojnemu organu. Dopolnjuje se ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki, spremembe pa se v roku 8 dni posredujejo tudi pristojnemu organu.

(4) Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled vanj pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

5. člen

(1) Ravnatelj za varstvo posamezne zbirke osebnih podatkov pisno pooblasti osebe, ki so odgovorne za zbiranje, vodenje, uporabo, hranjenje in posredovanje osebnih podatkov iz zaupane zbirke (v nadaljevanju pooblaščen oseb). Pooblastilo se vpiše v evidenco pooblaščenih oseb (obrazec 1).

(2) Za zagotavljanje varstva osebnih podatkov s strani delavcev zavoda mora, v skladu s 3. odstavkom 27. člena tega pravilnika, vsak, ki lahko zaradi narave svojega dela obdeluje posamezne kategorije osebnih podatkov, podpisati izjavo, s katero se zaveže k varovanju obdelovanih osebnih podatkov.

(3) Za uresničevanje določb tega pravilnika zavod vodi sledeče evidence o ravnanju z osebnimi podatki:

- evidenco pooblaščenih oseb, iz katere je razvidno ime zbirke, delovno mesto in osebno ime pooblaščenega, vrsta osebnih podatkov, ki jih obdeluje, ter vrsta ravnanja z njimi (obrazec 1);
- evidenco posredovanja osebnih podatkov (obrazec 2);
- evidenco posegov v strojno in programsko opremo (obrazec 3);
- evidenco izdelanih kopij vsebin zbirk osebnih podatkov (obrazec 4);
- evidenca pogodbenih obdelovalcev osebnih podatkov in sklenjenih pogodb (obrazec 5);
- evidenca obdelave osebnih podatkov vsebovanih v evidenci videoposnetkov (obrazec 6).

II. Varovanje prostorov in računalniške opreme

6. člen

(1) Prostor, v katerih se nahajajo nosilci osebnih podatkov ter strojna in programska oprema, na kateri so shranjeni osebni podatki (v nadaljevanju varovani prostori), morajo biti varovani z organizacijskimi, fizičnimi in tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

(2) Dostop do varovanih prostorov je mogoč le v poslovnem času zavoda, izven tega časa pa samo na podlagi dovoljenja pooblaščenih oseb ali ravnatelja zavoda.

(3) Odgovorna oseba za varstvo posamezne zbirke osebnih podatkov ne sme puščati odklenjenih in nenadzorovanih varovanih prostorov, kadar se ne nahaja v prostoru, ali drugače omogočiti nepooblaščenim osebam dostop do prostorov, v katerih se nahajajo osebni podatki (npr. z izročitvijo ključa nepooblaščenim osebam). Prav tako se ne sme puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice do vpogleda vanje.

(4) Izven poslovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

(5) Ključi varovanih prostorov se hranijo tako, da nepooblaščenim osebam nimajo dostopa do njih.

(6) Kadar se nosilci osebnih podatkov nahajajo izven varovanih prostorov (npr. hodniki, skupni prostori, aktivni arhivi), morajo biti zavarovani tako, da nepooblaščenim osebam nimajo dostopa do osebnih podatkov.

(7) Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

7. člen

(1) V varovanih prostorih, v katere prihajajo zunanji obiskovalci, učenci in druge nepooblaščenim osebe, morajo biti nosilci podatkov in monitorji nameščeni tako, da te osebe nimajo vpogleda v osebne podatke.

(2) Posebno pozornost morajo osebe, ki so odgovorne za varstvo osebnih podatkov, nameniti tistim osebnim podatkom, ki se nahajajo v prostorih zbornice. Pred vstopom nepooblaščenih oseb je potrebno osebne podatke na oglasni deski v zbornici prekriti ali odstraniti, preostale osebne podatke pa ustrezno zavarovati pred nepooblaščenim dostopom. Vsak zaposleni, ki zadnji zapusti zbornico, mora zapreti vrata, tako da vstop nepooblaščenim osebam brez osebne ključa ni mogoč.

8. člen

Vzdrževanje in popravilo strojne in programske računalniške in druge opreme, s katero se obdelujejo osebni podatki, je dovoljeno samo z odobritvijo odgovorne osebe, izvajajo pa ga lahko samo pooblašчени servisi in vzdrževalci, ki imajo z zavodom sklenjeno ustrežno pogodbo, s katero so določene dolžnosti vzdrževalca ali servisa v zvezi z varstvom osebnih podatkov.

9. člen

(1) Obiskovalci zavoda, zunanji izvajalci raznih del, vzdrževalci strojne in programske opreme ter druge nepooblaščene osebe se smejo gibati v varovanih prostorih samo v prisotnosti ali z vednostjo pooblaščene osebe ali ravnatelja.

(2) Kadar zaradi narave dela ni možna prisotnost pooblaščene osebe ali ravnatelja, morajo biti nosilci osebnih podatkov zavarovani tako, da vpogled vanje ni mogoč.

(3) Zaposleni v zavodu, ki nimajo pravice vpogleda v posamezne vrste osebnih podatkov (nepooblaščeni zaposleni) se lahko izven poslovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke v skladu z določbami tega pravilnika o varovanju osebnih podatkov izven delovnega časa (4. odstavek 6. člena).

III. Varovanje sistemske in aplikativne programske računalniške opreme ter podatkov, ki se obdelujejo z računalniško opremo

10. člen

Sistemska in aplikativna programska računalniška oprema mora biti varovana tako, da omogoča dostop samo tistim zaposlenim osebam, ki so pooblaščene za vodenje, obdelavo ali vpogled v posamezne vrste osebnih podatkov, in tistim pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

11. člen

(1) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve ravnatelja, izvajajo pa jih lahko samo pooblašчени servisi ali izvajalci, ki imajo z zavodom sklenjeno ustrežno pogodbo.

(2) Izvajalci morajo posege v programsko opremo iz prejšnjega odstavka beležiti v evidenci posegov v strojno in programsko opremo (obrazec 3), ki se vodi v tajništvu.

(3) Delavec, pooblaščen za zbiranje in obdelavo osebnih podatkov, mora pred popravilanjem, spreminjanjem ali dopolnjevanjem sistemske ali aplikativne programske opreme poskrbeti za izdelavo varnostnih kopij (back up), ki jih po prenehanju potrebe uniči po določenih tega

pravilnika. Izdelavo kopij mora evidentirati v evidenci izdelanih kopij zbirk osebnih podatkov (obrazec 4), kopije pa se hranijo v skladu s 17. členom tega pravilnika.

(4) Pooblaščen delavec mora biti med posegom ves čas prisoten in zagotoviti, da ne pride do nedovoljenega ravnanja z osebnimi podatki.

(5) V primeru, da se izkaže potreba po posegu v strojno opremo, ki se mora opraviti izven zavoda in brez prisotnosti pooblaščen osebe za varstvo osebnih podatkov shranjenih na tej strojni opremi, je potrebno narediti kopijo teh podatkov, le-to shraniti v skladu s 17. členom tega pravilnika, na strojni opremi pa osebne podatke izbrisati na način, ki onemogoča restavrancijo.

12. člen

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

13. člen

(1) Sistemska in aplikativna programska oprema, vsebina diskov mrežnega strežnika in lokalnih delovnih postaj z osebnimi podatki se lahko stalno in sprotno preverja glede na prisotnost računalniških virusov.

(2) Ob pojavu računalniškega virusa mora oseba, pooblaščen za varstvo posamezne zbirke osebnih podatkov, nemudoma obvestiti vzdrževalca opreme, ta pa sočasno z odstranitvijo virusa in ustrezno zaščito ter namestitvijo protivirusnih programov poskuša ugotoviti vzrok pojava virusa v računalniškem informacijskem sistemu.

(3) Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu, in prispejo v zavod z mediji za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti pred namestitvijo ali uporabo preverjeni glede prisotnosti računalniških virusov.

14. člen

(1) Zaposleni ne smejo inštalirati programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

(2) Prav tako ne smejo odnašati programske ali strojne opreme iz zavoda brez odobritve ravnatelja in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

15. člen

(1) Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, ki mora omogočati tudi

možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov ali kdaj so bili osebni podatki uporabljeni ali drugače obdelovani ter kdo je to storil.

(2) Na podlagi režima zavoda za dodeljevanje gesel mora biti osebam, ki lahko zaradi narave svojega dela obdelujejo osebne podatke, dodeljeno geslo za dostop do osebnih podatkov vodenih v računalniku. Oseba mora skrbno varovati dodeljeno geslo in ga po potrebi tudi spremeniti, da onemogoči nepooblaščenno obdelavo osebnih podatkov.

16. člen

(1) Gesla, ki se uporabljajo za administriranje programov, v katerih se hranijo zbirke osebnih podatkov, se hranijo v zapečatenih ovojnica v ognjevarni in protivlomno zaščiteni omari v pisarni pomočnika ravnatelja in se jih varuje pred dostopom nepooblaščenih oseb. Na ovojnici se označi, do katere zbirke osebnih podatkov je možno dostopati s shranjenim geslom. Po potrebi se geslom doda tudi opis postopkov za dostop do podatkov zaščiteneh z njimi.

(2) Do shranjenih gesel ima dostop samo ravnatelj, ki jih lahko uporabi le v nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira na ovojnici, na katero se zabeleži, kdo je odprl ovojnico, datum in uro uporabe in podpis.

(3) Po vsaki takšni uporabi se določi novo geslo, ovojnico pa se na novo zapečati.

17. člen

(1) Za potrebe restavriranja računalniškega sistema ob okvari in ob drugih izjemnih situacijah mora delavec, ki je pooblaščen za vodenje posamezne zbirke osebnih podatkov, skrbeti za redno izdelavo kopij vsebine strežnika in lokalnih postaj (back up).

(2) Kopije se hranijo na zunanjih diskah ali drugih ustreznih nosilcih, ki so shranjeni v zaklenjenih ognjevarnih omarah.

IV. Storitve, ki jih opravljajo zunanje pravne ali fizične osebe

18. člen

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (v nadaljevanju pogodbeni obdelovalec), se sklone pisna pogodba skladno z 11. členom Zakonom o varstvu osebnih podatkov. V pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

(2) Omenjeno velja tudi za zunanje izvajalce, ki vzdržujejo strojno in programsko opremo ali ki izdelujejo in instalirajo novo strojno ali programsko opremo.

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

(4) Izvajalec, ki bi izven naročnikovih prostorov za zavod opravljal storitve, pri katerih se uporablja osebne podatke oziroma ima dostop do njih, mora zagotoviti vsaj enako strog način varovanja osebnih podatkov, kot ga predvideva ta pravilnik. Obveznosti izvajalca se podrobneje opredeli v pogodbi, s katero se stranki dogovorita za izvajanje takih storitev.

(5) Evidenca pogodbenih obdelovalce osebnih podatkov in sklenjenih pogodb se vodi v tajništvu (obrazec 5).

V. Sprejem in posredovanje osebnih podatkov

19. člen

(1) Delavec v tajništvu, ki je zadolžen za sprejem in evidenco pošte, sprejema, odpira in pregleduje vse poštno pošiljke in pošiljke, ki na drug način prispejo v zavod, razen pošiljk iz tretjega in četrtega odstavka tega člena.

(2) Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljene v zavod. Taka pošiljka se neodprta vrne pošti.

(3) Delavec, ki je zadolžen za sprejem in evidenco pošte, evidentira, vendar pa ne odpira pošiljk z osebnimi podatki ali pošiljk, za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis in so opremljeni z označbo, da jih ni dovoljeno odpirati. Takšna pošiljka se izroči direktno posamezniku, na katerega je naslovljena ali ki je pooblaščen za obdelavo njene vsebine.

(4) Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk naslovljenih neposredno na delavca zavoda, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter tistih pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov zavoda.

20. člen

(1) Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

(2) Občutljivi osebni podatki se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico.

(3) Osebni podatki se pošiljajo priporočeno.

(4) Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi z običajno lučjo vidna njena vsebina. Prav tako mora ovojnica zagotoviti, da njenega odprtja in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja.

21. člen

(1) Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

(2) Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in z elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

22. člen

(1) Osebni podatki se posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

(2) Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora biti vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

(3) Vsako posredovanje osebnih podatkov se beleži v evidenci posredovanja osebnih podatkov (obrazec 2), iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

(4) Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča ali drugega pristojnega organa na osnovi zakonite pravne podlage, iz katere bi bilo razvidno, da se mora priložiti originalni dokument. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo, v spis pa priložiti odredbo, na podlagi katere je bil originalni dokument posredovan.

(5) Vsi podatki, z izjemo tistih iz prejšnjega odstavka, se posredujejo na kopiji dokumenta.

VI. Brisanje podatkov

23. člen

(1) Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo. Izjema je videoposnetek incidenta, ki se hrani do konca postopka, vodenega zaradi incidenta, nato pa se uniči v skladu s pravilnikom.

(2) Rok za uničenje ali izbris iz zbirke osebnih podatkov so razvidni iz 7. točke kataloga zbirke osebnih podatkov.

24. člen

(1) Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela izbranih podatkov.

(2) Podatki na klasičnih medijih (listine, kartoteke, register, seznam ...) se uničijo na način, ki onemogoča čitanje vseh ali dela uničenih podatkov. Praviloma je potrebno listinske nosilce z osebnimi podatki razrezati z napravo za razrez dokumentov, ki je nameščena v tajništvu zavoda.

(3) Na enak način se uničuje pomožno gradivo za izdelavo dokumentov z osebnimi podatki, kot so osnutki, matrice, skice, poskusni oziroma neuspešni izpis, ipd. Uničenje tega gradiva se mora izvajati ažurno.

(4) Prepovedano je odmetavati odpadne nosilce podatkov z osebnimi podatki v koše za smeti.

(5) Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi med prenosom.

(6) Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna komisija, ki o uničenju sestavi tudi ustrezen zapisnik. Navedeno ne velja za uničenje pomožnega gradiva, kot izhaja iz 3. odstavka tega člena, ki ga mora na ustrezen način in sprti uničiti oseba, ki je izdelala pomožno gradivo.

(7) Gradivo, na katerem so osebni podatki in nastane pri pedagoškem delu (testi, naloge ...), se vrne učencem po predpisih.

VII. Ukrepanje ob sumu nepooblaščenega dostopa, zlorabe ali vdora v zbirke osebnih podatkov

25. člen

(1) Zaposleni so dolžni z največjo skrbnostjo poskrbeti, da ne pride do zlorabe ali seznanitve nepooblaščenih oseb z osebnimi podatki. V ta namen morajo skrbeti za spoštovanje pravil, določenih s tem pravilnikom.

(2) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem zaupnih podatkov, o zlonamerni ali nepooblaščen uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti ravnatelja, ki mora ustrezno ukrepati. Sami pa morajo nemudoma ukreniti vse, kar je v njihovi moči, da bi takšno aktivnost preprečili.

(3) Kadar ima poskus ali zloraba osebnih podatkov znake kaznivega dejanja, se o tem obvesti pristojne organe.

VIII. Odgovornost za izvajanje ukrepov zavarovanja osebnih podatkov

26. člen

(1) Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so v zavodu odgovorni ravnatelj, pooblaščen osebe za varstvo posamezne zbirke osebnih podatkov in vsi zaposleni, ki v okviru del in nalog na delovnem mestu, za katerega so sklenili delovno razmerje, zbirajo in obdelujejo osebne podatke, imajo dostop do njih ali se z njimi na katerikoli način seznanijo.

(2) Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja ravnatelj.

27. člen

(1) Kdor 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.

(2) Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

(3) Pred nastopom dela na delovnem mestu, na katerem se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov in seznanja s posledicami kršitev. S podpisom izjave posameznik potrjuje, da je seznanjen z določbami tega pravilnika ter določbami ZVOP-1.

(4) Obrazec izjave je priloga tega pravilnika. Izjava se hrani v personalni mapi delavca.

28. člen

(1) Delavec, ki krši določila tega pravilnika in določila drugih predpisov, ki urejajo varovanje osebnih podatkov v zavodu, je za kršitev disciplinsko odgovoren.

(2) Kadar delavec stori hujšo kršitev delovnih obveznosti v zvezi z varstvom osebnih podatkov, je to po predpisih, ki urejajo delovna razmerja, lahko podlaga za odpoved pogodbe o zaposlitvi.

(3) Med hujše kršitve se štejejo predvsem naslednja ravnanja ali opustitve:

- sporočanje osebnih podatkov nepooblaščenim osebam oziroma iznašanje takih podatkov izven zavoda;
- nepooblaščen izdelava kopij osebnih podatkov;
- opustitev nadzora nad nosilci osebnih podatkov med poslovnim časom in s tem omogočanje nepooblaščenim osebam dostop do osebnih podatkov;

- nestrokovno ali neustrezno popravilo, spreminjanje ali nameščanje programske ali strojne opreme, zaradi česar pride do izgube osebnih podatkov ali drugih napak povezanih z varstvom osebnih podatkov;
- če opusti dolžnosti in potrebno skrbnost pri svojem delu, zaradi česar pride do izgube, uničenja ali seznanitve nepooblaščenih oseb z osebnimi podatki;
- druge hujše kršitve, povezane z varstvom osebnih podatkov, zaradi katerih je zavod utrpel škodo.

(4) Pogodbeni sodelavci odgovarjajo za kršitve, povezane z varstvom osebnih podatkov, skladno s prevzetimi pogodbenimi obveznostmi in predpisi, ki urejajo varstvo osebnih podatkov.

IX. Posebne ureditve za zbirke osebnih podatkov vodenih v zavodu

29. člen (zbirke osebnih podatkov učencev)

(1) Določbe tega pravilnika se uporabljajo tudi za

- zbirke osebnih podatkov, ki jih zavod vodi v skladu z Zakonom o osnovni šoli, tj. za:
 - zbirko podatkov o učencih, vpisanih v osnovno šolo, in njihovih starših,
 - zbirko podatkov o napredovanju učencev, izdanih spričevalih, vzgojnih opominih in drugih listinah,
 - zbirko podatkov o učencih, ki potrebujejo pomoč oziroma svetovanje in
 - zbirko podatkov o gibalnih sposobnostih in morfoloških značilnostih učencev,
- obdelavo osebnih podatkov, ki jih zavod obdeluje zaradi izvajanja programa osnovnošolskega izobraževanja na podlagi drugih določb Zakona o osnovni šoli in drugih predpisov s področja vzgoje in izobraževanja (nacionalno preverjanje znanja, izrekanje pohval in vzgojnih ukrepov, opravičevanje odsotnosti učencev, izobraževanje na domu ...) ter za
- obdelavo osebnih podatkov otrok s posebnimi potrebami, ki so v osnovnošolsko izobraževanje vključeni na podlagi odločbe o usmeritvi, in otrok s posebnimi potrebami, ki so na podlagi odločbe o usmeritvi vključeni v poseben program vzgoje in izobraževanja.

(2) Zavod podrobnejše zavarovanje osebnih podatkov učencev iz prejšnjega odstavka uredi v skladu s Pravilnikom o zbiranju in varstvu osebnih podatkov na področju osnovnošolskega izobraževanja (Uradni list RS, št. 80/04 in 76/08) s posebnim predpisom.

30. člen (osebni podatki, pridobljeni na podlagi pisnega soglasja staršev)

(1) Za zbiranje osebnih podatkov učencev, ki nima podlage v zakonu, mora zavod pridobiti pisno soglasjem staršev. Obrazec soglasja je priloga tega pravilnika.

(2) Tako zbrane podatke zavod zavaruje pred posegi nepooblaščenih oseb v skladu z določbami tega pravilnika.

31. člen (videonadzor)

(1) Videonadzor v šoli se uvede na podlagi sklepa o uvedbi videonadzora, ki ga sprejme ravnatelj.

(2) Z vzpostavitvijo videonadzora se oblikuje evidenca osebnih podatkov, za varstvo katere ravnatelj pooblasti zaposlenega delavca zavoda. Pooblaščen osebno obdeluje osebne podatke iz omenjene evidence v skladu s pooblastilom in vsako obdelavo zabeleži v evidenci obdelave osebnih podatkov vsebovanih v evidenci videoposnetkov (obrazec 6).

X. Hramba in roki hrambe osebnih podatkov

32. člen

(1) Prostori, v katerih se hrani dokumentacija z osebnimi podatki, ter rok hranjenja osebnih podatkov se za vsako zbirko osebnih podatkov določi v katalogu zbirke osebnih podatkov.

(2) Rok hranjena osebnih podatkov, naveden v katalogu zbirke osebnih podatkov, mora biti usklajen z določbami ustreznih področnih predpisov.

XI. Prehodne in končne določbe

33. člen

Katalog zbirk osebnih podatkov in zbirke osebnih podatkov, organizacija zavarovanja ter ureditev drugih zadev določenih s tem pravilnikom se mora uskladiti z določbami tega pravilnika in z Zakonom o varstvu osebnih podatkov v roku 30 dni od dneva sprejema tega pravilnika.

34. člen

Z določbami tega pravilnika se seznanijo vsi zaposleni v zavodu najkasneje v 30 dneh po sprejemu.

35. člen

Z dnem, ko prične veljati ta pravilnik, preneha veljati Pravilnik o zavarovanju osebnih podatkov v OŠ Brinje Grosuplje z dne 26. 2. 2001.

36. člen

Ta pravilnik začne veljati in se uporabljati naslednji dan po objavi na spletni strani zavoda.

Grosuplje, dne 15. 12 . 2015

Ravnateljica

Irena Kogovšek

Priloga 1: Evidence o ravnanju z osebnimi podatki

Priloga 2: Pooblastilo za obdelavo osebnih podatkov

Priloga3: Izjava o varovanju osebnih podatkov

Priloga 4: Soglasje za zbiranje osebnih podatkov učencev OŠ Brinje Grosuplje