Na podlagi člena 24 in 32 Splošne 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 v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 163/22; v nadaljevanju: ZVOP-2) izdaja ravnateljica Osnovne šole Vincenzo e Diego de Castro Piran naslednji

PRAVILNIK

O POSTOPKIH IN UKREPIH ZA VARNOST OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

Vsebina in namen pravilnika

1. člen

1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za varnost osebnih podatkov v Osnovni šoli Vincenzo e Diego de Castro Piran (v nadaljevanju: šola) z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava osebnih podatkov.

2) Zaposleni v šoli in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s Splošno uredbo, s področno zakonodajo, ki ureja posamezno področje njihovega dela, ter z vsebino tega pravilnika.

3) V pravilniku uporabljeni izrazi ravnatelj, delavec, zaposleni, obdelovalec in drugi izrazi, zapisani v moški spolni slovnični obliki, so uporabljeni kot nevtralni za moške in ženske.

Pomen izrazov

2. člen

1) V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. **Osebni podatek** pomeni katerokoli informacijo v zvezi z določenim ali določljivim posameznikom, na katerega se nanašajo osebni podatki; 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, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.
2. **Zbirka osebnih podatkov** pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi.
3. **Obdelava osebnih podatkov** pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.
4. **Obdelovalec osebnih podatkov** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca zbirk osebnih podatkov.

5. **Upravljavec osebnih podatkov** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice.
6. **Posebne vrste osebnih podatkov** so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.
7. **Uporabnik osebnih podatkov** pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Zaposleni v šoli se ne štejejo za uporabnike.
8. **Nosilec podatkov** so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno s 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 poslovni skrivnosti.

2) Drugi izrazi uporabljeni v tem pravilniku imajo enak pomen, kot ga določa ZVOP-2 v 5. členu in Splošna uredba v členu 4.

II. OBDELAVA OSEBNIH PODATKOV

Vzpostavitev zbirke osebnih podatkov

3. člen

Posamezno zbirko osebnih podatkov na posameznem delovnem področju šole vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba), ki jo določi ravnatelj šole.

Obdelava osebnih podatkov

4. člen

1) V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno pravno podlago v skladu s Splošno uredbo, Zakonom o osnovni šoli in ZVOP-2.

2) 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.

3) Posebne vrste osebnih podatkov morajo biti pri obdelavi posebej označene in varovane tako, da se nepooblaščenim osebam onemogoči dostop do njih.

4) O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu s členoma 13 Splošne uredbe, kadar se podatki zbirajo od posameznika in v skladu s členom 14 Splošne uredbe, kadar se osebni podatki pridobivajo iz drugih virov.

5) Odgovorne osebe ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke (npr. tajništvo, računovodstvo, itd.), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami Splošne uredbe ter z vsebino tega pravilnika.

Evidentiranje dokumentov

5. člen

Za evidentiranje zadev, dosjejev in dokumentov, ki vsebujejo osebne podatke, se smiselno uporabljajo določbe predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom.

Postopanje šole, ko posameznik uveljavlja svoje pravice na področju varstva osebnih podatkov

6. člen

1) Zahteve, ki jih uveljavljajo posamezniki, na katere se nanašajo osebni podatki na podlagi členov 15 do 22 Splošne uredbe (pravica do dostopa, popravka, izbrisa, omejitve obdelave, do prenosljivosti osebnih podatkov in do ugovora; v nadaljevanju: pravice posameznikov), šola obravnava v skladu s členom 12 Splošne uredbe, 15. in 17. členom ZVOP-2. Za vprašanja postopka, se smiselno uporablja zakon, ki ureja splošni upravni postopek.

2) V roku iz člena 12(3) Splošne uredbe (brez nepotrebnega odlašanja in najkasneje v enem mesecu po prejemu zahteve, izjemoma v podaljšanem roku do dva dodatna meseca, če je to potrebno zaradi kompleksnosti in števila zahtev), šola posameznika seznani z odločitvijo in, če je to predmet zahteve, z osebnimi podatki, ki se nanašajo nanj. Če posameznik to zahteva, ga lahko z osebnimi podatki seznani tudi ustno.

3) Odločitev o pravicah posameznika mora vsebovati razloge in informacijo o pravici do pritožbe pri nadzornem organu v roku 15 dni od seznanitve z odločitvijo. Odločitev ima lahko obliko uradnega zaznamka, ki se pošlje posamezniku na način, ki omogoča seznanitev z odločitvijo in dokazovanje njenega prejema.

Posredovanje osebnih podatkov uporabnikom

7. člen

1) Na zahtevo uporabnika, šola posreduje osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam, če je za posredovanje podana pravna podlaga v skladu s 6. členom ZVOP-2 na podlagi zahteve iz prvega odstavka 41. člena ZVOP-2.

2) Če se zahteva za posredovanje nanaša na posebne vrste osebnih podatkov, mora oseba pri šoli, ki odloča o posredovanju, pred posredovanjem podatkov preveriti, če so za posredovanje izpolnjeni tudi pogoji iz člena 9 (2) Splošne uredbe.

3) Zahteva za posredovanje osebnih podatkov mora vsebovati naslednje podatke, ki jih opredeljuje prvi odstavek 41. člena ZVOP-2:

1. podatke o vlagatelju zahteve (za fizično osebo: osebno ime, naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika posameznika, posameznika, ki samostojno opravlja dejavnost, ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis vlagatelja oziroma pooblaščene osebe;
2. pravno podlago za pridobitev zahtevanih osebnih podatkov;
3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve;
4. predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo;
5. vrste osebnih podatkov, ki naj se mu posredujejo;
6. obliko in način pridobitve zahtevanih osebnih podatkov.

4) O zahtevi za posredovanje osebnih podatkov šola odloča v skladu z 41. členom ZVOP-2 in s smiselno uporabo zakona, ki ureja splošni upravni postopek.

5) Posredovanje osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva pisno ali ustno. V pisni vlogi mora uporabnik jasno navesti pravno podlago za pridobitev osebnih podatkov. Če uporabnik zahteva posredovanje osebnih podatkov ustno, odgovorna oseba pri šoli, ki sprejme takšno vlogo, o tem napravi zapisnik, ki ga morata podpisati vlagatelj in oseba, ki je zapisnik pripravila.

6) Če je vloga uporabnika za posredovanje nerazumljiva ali nepopolna, ga šola pozove na dopolnitev v roku 5 dni od prejema vloge, v kateri mu postavi rok za dopolnitev.

7) Šola o zahtevi za posredovanje odloči najpozneje v 15 dneh od prejema popolne zahteve ali pa vlagatelja v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredovala. Šola in vlagatelj zahteve za posredovanje se lahko v istem roku tudi dogovorita za podaljšanje tega roka.

8) Ko se zahteva nanaša na posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig, če šola zahtevo za posredovanje osebnih podatkov delno ali v celoti zavrne, se vlagatelja obvesti o pravici do pritožbe pri Informacijskem pooblaščencu.

9) Kadar se zahteva za posredovanje osebnih podatkov nanaša na podatke, ki niso iz uradnih evidenc ali javnih knjig, se vlagatelja obvesti o pravici sodnega varstva, ki se uveljavlja pred sodiščem s splošno pristojnostjo v skladu z zakonom, ki ureja nepravdni postopek.

Način posredovanja osebnih podatkov

8. člen

1) Osebni podatki,, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v skladu z določbami predpisov, ki urejajo upravno poslovanje z dokumentarnim gradivom, oziroma 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. V kolikor se posredujejo osebni podatki v papirnem izpisu, je treba osebne podatke posredovati s priporočeno poštno pošiljko in oznako "zaupno" oziroma po kurirju v zaprti ovojnici z oznako "zaupno".

2) Osebne podatke je dovoljeno posredovati z informacijskimi, komunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje ali uničenje podatkov ter neupravičeno seznanjanje z njihovo vsebino. Posredovanje osebnih podatkov po elektronski pošti je treba zavarovati z geslom.

3) Posebne vrste osebnih podatkov je dovoljeno posredovati preko komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

4) 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.

Evidenca posredovanj

9. člen

1) Vsako posredovanje osebnih podatkov iz prejšnjega člena se zaznamuje z navedbo naslednjih podatkov:

- kateri osebni podatki so bili posredovani,
- osebno ime/firma in naslov/sedež osebe, ki so ji bili posredovani osebni podatki,
- datum in ura posredovanja osebnih podatkov,
- pravna podlaga, na kateri so bili posredovani osebni podatki ter
- za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, so bili podatki posredovani.

2) Zaznamek iz prejšnjega odstavka je v pisni ali elektronski obliki kot del podatkov zadeve, o kateri se vodi postopek. Oblika uradnega zaznamka je odvisna od nosilca podatkov, ki vsebuje posredovani osebni podatek (spis, informacijski sistem za podporo pisarniškemu poslovanju).

3) Če osebni podatek, ki se posreduje, ni del podatkov zadeve, o kateri se vodi postopek, se zaznamek iz prvega odstavka tega člena v obliki iz prejšnjega odstavka evidentira neposredno v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek.

4) Za zaznamek iz prvega odstavka tega člena je odgovorna oseba, ki je osebne podatke posredovala uporabniku.

Dostop znotraj šole

10. člen

1) Osebni podatki zaposlenih v šoli in ostalih oseb se lahko posredujejo znotraj šole tudi tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.

2) Katerakoli oseba, ki ukrepa pod vodstvom šole in ima dostop do osebnih podatkov, osebnih podatkov ne sme obdelati brez navodil šole, razen če to od nje zahteva zakon.

Pregledovanje, prepisovanje in kopiranje osebnih podatkov spisov

11. člen

1) Ne glede na določbe 6. člena tega pravilnika, se za pregledovanje zadev, ki po zakonu, ki ureja splošni upravni postopek sodijo med upravne zadeve ali druge javnopravne stvari (v nadaljevanju: pregledovanje, prepisovanje in kopiranje spisov), uporabljajo določbe predpisov, ki urejajo splošni upravni postopek in upravno poslovanje z dokumentarnim gradivom.

2) Pred pregledovanjem, prepisovanjem in kopiranjem spisov, je treba 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, potni list, vozniško dovoljenje ali drug dokument, ki nedvoumno izkazuje njegovo istovetnost.

3) Pri vsakem posameznem pregledovanju, prepisovanju in kopiranju dokumentov po tem členu, ki vsebujejo osebne podatke, se naredi uradni zaznamek, ki se vloži v spis. Iz uradnega zaznamka, ki ga mora podpisati tudi stranka oziroma upravičenec, mora biti razvidna številka spisa, datum in ura pregleda, vrsta dokumenta, katerega kopija se je posredovala upravičencu, osebno ime stranke oziroma upravičenca, njegov naslov, številka in vrsta dokumenta, iz katerega je ugotovljena identiteta ter namen, zaradi katerega je bilo opravljeno pregledovanje, prepisovanje oziroma kopiranje dokumenta.

4) Stranko oziroma upravičenca je pred pregledovanjem, prepisovanjem in kopiranjem spisa, ki vsebujejo osebne podatke, treba opozoriti na dolžnost varovanja takšnih podatkov. Opozorilo mora biti sestavni del uradnega zaznamka iz prejšnjega odstavka.

Kopiranje in tiskanje osebnih podatkov s strani zaposlenih

12. člen

Delavci šole, 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 zaposlenih, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah.

Hramba osebnih podatkov

13. člen

1) Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe, kot je razviden iz evidence dejavnosti obdelave za posamezno zbirko osebnih podatkov.

2) Po preteku roka hrambe 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.

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

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

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

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

7) Pri prenosu nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, na mesto uničenja, je treba zagotoviti ustrezno varnost tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.

8) Prenos nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo imenuje ravnatelj šole.

9) Komisijo iz prejšnjega odstavka sestavljajo delavci šole, en član komisije je odgovorna oseba.

10) O uničenju iz osmega odstavka tega člena komisija sestavi ustrezen zapisnik.

Evidenca dejavnosti obdelave

14. člen

1) Opis zbirke osebnih podatkov, katerih upravljavec je šola, se vodi v evidenci dejavnosti obdelave za posamezne zbirke osebnih podatkov (opisu zbirk osebnih podatkov), ki se vodi v skladu z določbami člena 30 Splošne uredbe.

2) Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni z evidencami dejavnosti obdelave za posamezne zbirke osebnih podatkov, vpogled v evidence pa je treba omogočiti tudi vsakomur, ki to zahteva in ki vpogled izkaže z ustrezno pravno podlago.

3) Šola je dolžna voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko

zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo naslednji podatki:

1. naziv zbirke osebnih podatkov,
2. osebno ime in delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov,
3. osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov,
4. kadar obstajajo, skupnega upravljavca, predstavnika upravljavca,
5. namen ali namene obdelave in pravno ali pravne podlage,
6. opis kategorij posameznikov, na katere se nanašajo osebni podatki,
7. vrste osebnih podatkov,
8. kadar je ustrezno, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, vključno z navedbo te tretje države ali mednarodne organizacije, v primeru prenosov iz drugega pododstavka člena 49(1) Splošne uredbe pa tudi dokumentacijo o ustreznih zaščitnih ukrepih,
9. rok hrambe,
10. splošni opis tehničnih in organizacijskih varnostnih ukrepov.

III. UPORABA ELEKTRONSKE POŠTE, RAČUNALNIKOV IN INTERNETA

Elektronska pošta in uporaba druge programske opreme na računalniku

15. člen

1) Elektronska pošta in računalnik se uporabljata v službene namene.

2) 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.

3) Oseba, zadolžena za delovanje računalniškega informacijskega sistema, lahko na posebej utemeljeno pisno zahtevo ravnatelja, v prisotnosti komisije iz četrtega 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.

4) Vpogled v vsebino elektronske pošte zaposlenega opravi tričlanska komisija, ki jo vsakokrat imenuje ravnatelj. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik.

5) 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 ravnatelja opravi nadzor količine uporabe elektronske pošte, a zgolj z vidika obsega priponk, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebine elektronske pošte.

6) 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 elektronski pošti.

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

Internet

16. člen

1) Internet se uporablja v službene namene.

2) 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.

3) Ravnatelj lahko s posebno odredbo odredi blokado določenih spletnih strani.

4) Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema, na podlagi pisne odredbe ravnatelja.

5) O blokadi se obvesti vse zaposlene po elektronski pošti.

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

Varovanje prostorov

17. člen

1) Prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo osebne podatke, tajne podatke in druge varovane podatke, strojna in programska oprema (v nadaljevanju: varovani prostori), morajo biti varovani z organizacijskimi in/ali tehničnimi ukrepi iz tega pravilnika, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

2) Dostop do varovanih prostorov je mogoč le v rednem delovnem času, izven njega pa samo na podlagi dovoljenja ravnatelja.

3) V varovani prostor lahko vstopa le zaposleni, ki ima dodeljen ključ za konkretni varovani prostor, v prostore, kjer se nahaja strojna in programska oprema, pa zgolj tisti, ki so po pooblastilu ravnatelja pristojni za nadzor in vzdrževanje opreme, in ravnatelj.

4) Varovani prostori ne smejo ostajati nenadzorovani oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo. Ključi se ne smejo puščati v ključavnici v vratih.

5) V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni. Ključe hrani zaposleni, ki nadzoruje posamezen varovani prostor, na zavarovanem mestu v varovanem prostoru.

6) Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo na hodnikih in v drugih skupnih prostorih, morajo biti stalno zaklenjeni. Ključe hrani zaposleni, ki nadzoruje posamezno omaro, mizo in drugo pohištvo, na zavarovanem mestu v varovanem prostoru, ki ga nadzoruje.

7) Osebe, ki niso zaposlene v šoli (npr. vzdrževalci prostorov, strojne in programske opreme, starši in drugi obiskovalci itd.) se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

8) Posebne vrste osebnih podatkov se ne smejo hraniti izven varovanih prostorov.

Varovanje nosilcev podatkov, ki vsebujejo osebne podatke

18. člen

1) Zaposleni ne smejo puščati nosilcev podatkov, ki vsebujejo osebne podatke, na vidnem mestu (npr. na mizah) v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

2) Nosilci podatkov, ki vsebujejo posebne vrste osebnih podatkov, se ne smejo hraniti izven varovanih prostorov.

3) Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni odnašajo izven prostorov šole samo z dovoljenjem ravnatelja.

4) Nosilcev podatkov, ki vsebujejo posebne vrste osebnih podatkov, zaposleni ne smejo odnašati izven prostorov šole, razen izjemoma z dovoljenjem ravnatelja, če je to nujno potrebno za reševanje zadeve, ki vsebuje te posebne vrste osebnih podatkov.

5) V prostorih, ki so namenjeni poslovanju s starši otrok ali strankami, morajo biti nosilci podatkov, ki vsebujejo osebne podatke, in računalniški prikazovalniki nameščeni tako, da starši otrok ali stranke nimajo vpogleda vanje.

Varovanje strojne in programske opreme

19. člen

1) Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in vzdrževalci, ki imajo s šolo sklenjeno ustrezno pogodbo. Ob predaji opreme v servis morata oseba, ki predaja opremo, in oseba, ki jo sprejema v popravilo, izpolniti primopredajni zapisnik.

2) Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim, ki jih določi oseba, zadolžena za delovanje računalniškega informacijskega sistema, v soglasju z ravnateljem, ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

3) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije ter posamezniki, ki imajo s šolo sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

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

5) Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se vsakodnevno preveri z vidika prisotnosti računalniških virusov. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu šole.

6) Vsi podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo v šolo na medijih za prenos računalniških podatkov ali preko komunikacijskih kanalov, morajo biti pred uporabo preverjeni z vidika prisotnosti računalniških virusov.

7) Zaposleni ne smejo namestiti programske opreme brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema. Prav tako ne smejo odnašati programske opreme iz prostorov šole brez odobritve ravnatelja in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

8) Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vnešeni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil glede na tveganja.

9) Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi režim dodeljevanja, hranjenja in spreminjanja gesel.

V. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

Pogodbena obdelava

20. člen

1) Z vsakim obdelovalcem osebnih podatkov šola sklene pisno pogodbo v skladu s členom 28 Splošne uredbe.

2) Pogodba iz prejšnjega odstavka mora obvezno vsebovati tudi postopke in ukrepe za zagotovitev varnosti osebnih podatkov.

3) Prejšnji odstavek velja tudi za obdelovalce osebnih podatkov, ki vzdržujejo obstoječo strojno in programsko opremo ter izdelujejo in nameščajo novo strojno ali programsko opremo.

4) Obdelovalci osebnih podatkov lahko opravljajo storitve obdelave osebnih podatkov samo v okviru pooblastil iz pogodbe iz prvega odstavka tega člena in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

5) Obdelovalci osebnih podatkov, ki za šolo opravljajo pogodbeno dogovorjene storitve izven prostorov šole, morajo imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

6) Vodi se seznam pogodbenih obdelovalcev, ki vsebuje: naziv in sedež pravne osebe, ime in priimek oseb, ki izvajajo zunanje storitve ter kontaktne podatke teh oseb (naslov elektronske pošte in telefonska številka). Seznam se hrani v tajništvu in pri ravnatelju. Seznam se po potrebi ažurira.

VI. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

Obveščanje o kršitvi varnosti osebnih podatkov

21. člen

1) Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov (v nadaljevanju: varnostni incident) takoj obvestiti ravnatelja, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti. Zaposleni, ki je dogodek zaznal o varnostnem incidentu obvesti tudi pooblaščeno osebo za varstvo osebnih podatkov.

2) Odgovorna oseba pri šoli poskrbi, da se nemudoma po zaznavi kršitve preišče okoliščine varnostnega incidenta in pripravi ocena tveganja za nastanek škodljivih učinkov. V skladu z oceno tveganja se po potrebi, v skladu s členom 33 Splošne uredbe, o kršitvi varnosti obvesti Informacijskega pooblaščenca najkasneje 72 ur po zaznani kršitvi.

3) Obvestilo Informacijskemu pooblaščencu iz prejšnjega odstavka vsebuje vsaj:

1. opis vrste kršitve varnosti 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;
2. sporočilo o imenu in kontaktnih podatkih pooblaščene osebe za varstvo podatkov ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;
3. opis verjetnih posledic kršitve varnosti osebnih podatkov;
4. opis ukrepov, ki jih je šola sprejela ali katerih sprejetje se predlaga za obravnavanje kršitve varnosti osebnih podatkov, pa tudi ukrepov za ublažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

4) Če ocena tveganja pokaže, da varnostni incident predstavlja veliko tveganje za pravice in svoboščine posameznikov, šola brez nepotrebnega odlašanja sporoči posameznikom, na katere se nanašajo osebni podatki, da je prišlo do kršitve varnosti osebnih podatkov. Za posameznike, šola opiše v jasnem in preprostem jeziku, vrsto kršitve varnosti osebnih podatkov in vsaj informacije ter ukrepe iz 2., 3. in 4. točke prejšnjega odstavka.

VII. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA VARNOST OSEBNIH PODATKOV

Izvajanje postopkov in ukrepov

22. člen

1) Za izvajanje postopkov in ukrepov za varnost osebnih podatkov, določenih s tem pravilnikom, so odgovorne pooblaščene osebe, ki jih imenuje ravnatelj.

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

Odgovorne osebe in dolžno nadzorstvo

23. člen

1) Za izvajanje postopkov in ukrepov za varnost osebnih podatkov, določenih s tem pravilnikom, so odgovorne pooblaščene osebe, ki jih imenuje ravnatelj.

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

Izjava delavca

24. člen

1) Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni ali druga oseba, ki osebno opravlja delo za šolo, podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov in drugih zaupnih podatkov.

2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami zakona, izjava pa mora vsebovati tudi pouk o posledicah kršitve tega pravilnika in zakona.

3) Osebe, ki so zaposlene v šoli ob uveljavitvi tega pravilnika, morajo v roku 30 dni od uveljavitve tega pravilnika, podpisati izjavo iz prvega odstavka tega člena.

Odgovornost za kršitev

25. člen

1) Kršitev določil tega pravilnika s strani zaposlenih pomeni kršenje obveznosti iz delovnega razmerja, ostali pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

2) Odgovornost iz prejšnjega odstavka ne izključuje kazenske ali odškodninske odgovornosti.

VIII. PREHODNE IN KONČNE DOLOČBE

Začetek veljavnosti

26. člen

1) Z dnem veljavnosti tega pravilnika preneha veljati Pravilnik o postopkih in ukrepih za varnost osebnih podatkov, z dne 29.08.2008.

2) Pravilnik se objavi na oglasni deski šole in začne veljati s 13.09.2023

Številka: 007-30/2023-1

Datum: 13/9/2023

SCUOLA ELEMENTARE VINCENZO e DIEGO de CASTRO PIRANO - PIRAN OSNOVNA ŠOLA

Ravnateljica: Ambra Šlosar Karbič