OSNOVNA ŠOLA
PREŽIHOVEGA VORANCA JESENICE

PRAVILNIK O VARSTVU OSEBNIH PODATKOV

Jesenice, junij 2020

Sprejet dne 1.7.2020 s strani zakonitega zastopnika upravljavca na podlagi 24., 25. in 32. člena 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 nadaljnjem besedilu: Splošna uredba o varstvu podatkov) ter 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 s spremembami, v nadaljevanju: ZVOP-1).

Verzije dokumenta, izvedene dopolnitve ter korekcije	**Avtorji**	**Verzija**	**Datum**
Predlog	Nina Pekolj, Tomaž Gorenšek	Predlog	Julij 2019
Priprava dokončne verzije		1.0	December 2019
Prevzem v iVIZ z naslednjimi dopolnitvami in korekcijami: 1. - Vpis ustanove, upravljavca, koordinatorja za varstvo podatkov, pooblaščena oseba za varstvo podatkov (t.i. DPO) - Dopolnitev veljavnih predpisov s področja varstva osebnih podatkov ter izvajanja javno veljavnih programov vzgoje in izobraževanja - Dopolnitev drugih internih aktov upravljavca - Dopolnitev -Evidence o ravnanju z osebnimi podatki (OP) v papirnati obliki v tajništvu - Dopolnitev -Seznam pooblaščenih oseb v papirnati obliki v tajništvu - Dopolnitev -Izjava pooblaščene osebe v papirnati obliki v tajništvu - Dopolnitev -Vstop zaposlenih v pisarne - Dopolnitev -Posamezne zahteve iz naslova uresničevanja pravic posameznikov upravljavec hrani v papirnati obliki v tajništvu - Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov z dne 27.9.2011	Nataša Krajnc		Junij 2020

1 Splošne določbe

1. člen

(Uvodna določba)

S tem pravilnikom se določajo tehnični in organizacijski ukrepi za zagotavljanje varstva osebnih podatkov posameznikov, ki jih upravlja oziroma obdeluje upravljavec osebnih podatkov (v nadaljevanju tudi: iVIZ).

Upravljavec **OŠ Prežihovega Voranca Jesenice** je z doslednim izvajanjem ukrepov zmožen dokazati, da obdelava poteka v skladu z veljavnimi predpisi s področja varstva osebnih podatkov in da zagotavlja zaupnost, celovitost, razpoložljivost in točnost osebnih podatkov.

2. člen

(Namen in vsebina pravilnika)

Namen pravilnika je opredeliti namen in obseg obdelave osebnih podatkov vključno z razmejitvijo vlog in odgovornostjo upravljavca, obdelovalcev in uporabnikov osebnih podatkov, pravno podlago za obdelavo, določitev tehničnih in organizacijskih ukrepov za zagotovitev varstva pri obdelavi osebnih podatkov, način izvajanja pogodbene obdelave osebnih podatkov, evidence dejavnosti obdelav osebnih podatkov, način uresničevanja pravic posameznikov, politiko ravnanja v primeru varnostnih incidentov ter letni pregled izvajanja aktivnosti varstva podatkov.

3. člen

(Zavezanci)

Določbe tega pravilnika zavezujejo upravljavca in naslednje kategorije uporabnikov:

- pooblaščene osebe za obdelavo osebnih podatkov, ki so na podlagi delovnega razmerja ali podobnih oblik dela (na primer napoteni delavci s strani drugega delodajalca, delavci, ki opravljajo delo na podlagi študentske napotnice) pod neposrednim vodstvom upravljavca,
- internega koordinatorja za varstvo podatkov,
- pooblaščeno osebo za varstvo podatkov (DPO),
- fizične in pravne osebe, ki so z upravljavcem v pogodbenem ali drugem pravnem razmerju, v katerem niso pod neposrednim vodstvom upravljavca, in pri izvajanju katerega pride do obdelav oziroma razkritja osebnih podatkov (v nadaljevanju pogodbeni obdelovalci).

Vsak zavezanec mora biti, s strani internega koordinatorja za varstvo podatkov, seznanjen z določbami tega pravilnika. Vsak zavezanec mora pred obdelavo ali razkritjem osebnih podatkov s pisno izjavo potrditi, da je seznanjen z vsebino pravilnika ali v okviru pogodbenega razmerja sprejeti določene obveznosti, ki upravljavcu zagotavljajo varstvene in nadzorstvene pravice glede varstva osebnih podatkov (**Priloga: Izjave za zaposlene / Pogodba o obdelavi osebnih podatkov**).

Vsak zaposlen pri zavezancu se mora seznaniti tudi s Kodeksom ravnanj iVIZ (Kodeks varstva podatkov in upravljanja informacijske varnosti za izvajalce vzgoje in izobraževanja).

V primeru, da pogodbena določila, ki urejajo razmerje med upravljavcem in zavezancem niso skladna z določbami tega pravilnika, se za presojo dolžnostnih vprašanj zavezancev upoštevajo določbe tega pravilnika le v kolikor je upravljavec sposoben dokazati, da je bil zavezanec seznanjen z vsebino tega pravilnika.

4. člen

(Relevantni predpisi in akti)

Kadar narava dela to zahteva, mora upravljavec zagotoviti, da so zavezanci seznanjeni tudi s drugimi relevantnimi predpisi, poslovnimi in etičnimi pravili, kodeksi ter internimi akti, ki zavezujejo upravljavca oziroma ki jih izvaja upravljavec.

Veljavni predpisi s področja varstva osebnih podatkov ter izvajanja javno veljavnih programov vzgoje in izobraževanja so:

- Splošna uredba o varstvu osebnih podatkov (GDPR),
- Zakon o varstvu osebnih podatkov,
- Zakon o informacijskem pooblaščencu,
- Zakon do informacij javnega značaja,
- Zakon o inšpekcijskem nadzoru,
- Zakon o splošnem upravnem postopku,
- Zakon o osnovni šoli,
- Pravilnik o dokumentaciji v osnovni šoli,
- Pravilnik o zbiranju in varstvu osebnih podatkov na področju osnovnošolskega izobraževanja,
- Pravilnik o načinu in pogojih dostopa do podatkov iz centralne evidence udeležencev vzgoje in izobraževanja,
- Pravilnik o nacionalnem preverjanju znanja v osnovni šoli,
- Zakon o usmerjanju otrok s posebnimi potrebami, zakon o javnih uslužbencih.

Upravljavec je pristopil tudi k splošnim poslovnim, etičnim in informacijskim pravilom, ki so zapisana v Kodeksu ravnanj iVIZ.

Področje varstva osebnih podatkov je neposredno ali posredno urejeno tudi v drugih interni aktih upravljavca in sicer (našteti):

- Pravilnik o obdelavi osebnih podatkov,
- Pravilnik o zavarovanju osebnih podatkov,
- Kodeks ravnanja javnih uslužbencev,
- Pravilnik o sistemizaciji delovnih mest,
- Pravilnik o arhiviranju,
- Pravila o subvencioniranju šolske prehrane,
- Dogovor o preprečevanju in odpravljanju posledic mobbinga v družbi,
- Pravilnik o sistemizaciji delovnih mest,
- Katalog zbirk osebnih podatkov.

V primeru, da posamezna določila predpisov ali aktov iz prejšnjih odstavkov tega člena niso skladna z določbami tega pravilnika, je zavezanec dolžan o tem obvestiti upravljavca. Upravljavec je dolžan začeti s postopkom harmonizacije predmetnega pravilnika in/ali takšnega akta. V kolikor upravljavec v treh mesecih od prejema obvestila ne prične z izvajanjem postopka harmonizacije, je zavezanec upravičen o neskladnosti obvestiti internega koordinatorja za varstvo podatkov, DPO in zastopnika upravljavca ter v primeru dodatne eno-mesečne neodzivnosti tudi urad Informacijski pooblaščenec ter nadzorni oziroma drug pristojni organ upravljavca (npr. svet zavoda, svet šole, ipd.).

5. člen

(Opredelitev pojmov)

V tem pravilniku uporabljeni pojmi imajo naslednji pomen:

1. **upravljavec** je OŠ Prežihovega Voranca Jesenice;

2. **obdelovalec** je fizična ali pravna oseba, ki obdeluje osebne podatke v imenu upravljavca;

3. **interni koordinator za varstvo podatkov** je fizična oseba pod neposrednim vodstvom upravljavca, ali zakoniti zastopnik upravljavca, ki je seznanjena z aktivnostmi upravljanja in obdelave osebnih podatkov pri upravljavcu ter skrbi za implementacijo navodil pooblaščene osebe za varstvo podatkov in operativno organizacijo ter koordinacijo varstva osebnih podatkov pri upravljavcu;

Interni koordinator za varstvo podatkov je Nataša Krajnc.

4. **pooblaščena oseba za varstvo podatkov** je fizična ali pravna oseba, ki je s strani upravljavca pooblaščena za upravljanje področja varstva podatkov in neposredno poroča zastopniku upravljavca ter sodeluje z internim koordinatorjem za varstvo podatkov.

Pooblaščena oseba za varstvo podatkov (t.i. DPO) je dr. Klemen Pohar, LL.M.

5. **osebni podatki** so katera koli informacija v zvezi z določenim ali določljivim posameznikom. 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 tega posameznika;

6. **posebna vrsta osebnih podatkov** so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, genetski in biometrični podatki, ki se obdelujejo za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;

7. **obdelava** je 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;

8. **privolitev posameznika** pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero (izjavo ali jasnim pritrdilnim dejanjem) izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj. V primeru, da je posameznik mladoleten, se kot privolitev posameznika po tem pravilniku šteje tudi privolitev njegovega zakonitega zastopnika;

8. **omejitev obdelave** je označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

9. **oblikovanje profilov** je vsaka oblika avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;

10. **psevdonimizacija** je obdelava osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;

11. **kršitev varstva osebnih podatkov** je kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

12. **nadzorni organ** je urad Informacijski pooblaščenec Republike Slovenije, Dunajska cesta 22, 1000 Ljubljana, Slovenija;

13. **sistemska programska oprema** so programi, ki jih računalnik uporablja za krmiljenje svoje opreme in za komunikacijo z okoljem (operacijski sistem) in druga programska orodja, ki jih dobimo skupaj z operacijskim sistemom in so namenjena vzdrževalcem in uporabnikom računalnika (npr. operacijski sistem Windows 10 ter internetni pregledovalec, ki je del operacijskega sistema);

14. **aplikativna programska oprema** so programi, s katerimi se izvaja obdelava podatkov (npr. eAsistent, eDelovodnik, programska oprema za eHrambo Logitus, finančno računovodski program, ipd..);

15. **zavezanci** po tem pravilniku so vsi obdelovalci (interni in pogodbeni), zastopnik upravljavca, interni koordinator za varstvo podatkov ter pooblaščena oseba za varstvo podatkov.

2 Obdelava osebnih podatkov

6. člen

(Obseg, namen in pravna podlaga)

Obseg obdelave osebnih podatkov, vključno z namenom in pravno podlago za obdelavo osebnih podatkov, je določen v posamezni evidenci dejavnosti obdelav osebnih podatkov.

Osebne podatke lahko iz posamezne evidence dejavnosti obdelav osebnih podatkov v imenu upravljavca obdelujejo le pooblaščene osebe za obdelavo osebnih podatkov pri upravljalcu, interni koordinator za varstvo podatkov, DPO in pogodbeni obdelovalci.

7. člen

(Trajanje obdelave osebnih podatkov)

Trajanje obdelave posameznih vrst osebnih podatkov je določeno v evidenci dejavnosti obdelav osebnih podatkov.

8. člen

(Posredovanje osebnih podatkov)

Za vsako posredovanje osebnih podatkov izven lokacije upravljavca mora posameznik, ki je do podatkov upravičen, predložiti pisno vlogo (lahko kot elektronsko sporočilo).

V kolikor se pravica nanaša na drugo osebo, mora prosilec izkazati pooblastilo ali pravico za razkritje osebnih podatkov oziroma mora biti k vlogi priložena podpisana zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

Pred razkritjem osebnih podatkov osebam iz prvega odstavka tega člena, je upravljavec dolžan preveriti identiteto pooblaščene osebe ter preveriti utemeljenost zahteve (npr. sklep sodišča o določitvi sodnega izvedenca). V nobenem primeru ni dovoljeno osebnih podatkov prosilcem posredovati oziroma razkrivati ustno.

Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, določenimi s tem pravilnikom, ki preprečujejo razkritje osebnih podatkov nepooblaščenim osebam.

Osebni podatki se pošiljajo naslovnikom v zaprtih kuvertah, preko varnih informacijskih povezav (HTTPS, SSL, SSH) ali s posredovanjem prilog po elektronski pošti, ki so zaščitene z gesli. Če je to mogoče, se gesla za odpiranje prilog v elektronski pošti pošljejo po drugem komunikacijskem kanalu, kot elektronska pošta.

Posebne vrste osebnih podatkov se lahko upravičenim osebam posredujejo preko elektronskih komunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom. Praviloma je posredovanje posebnih vrst osebnih podatkov po elektronski poti tudi elektronsko podpisano z naprednim elektronskim podpisom. Posebne vrste osebnih podatkov se v papirnati obliki pošiljajo po priporočeni pošti. Predlaga se, da se pošiljajo priporočeno s povratnico. Vsa prejeta dokazila o priporočenem posredovanju, prejete povratnice in drugi dokazi o tovrstnem pošiljanju se hrani skladno z roki hrambe, določenimi v veljavnem Enotnem klasifikacijskem načrtu (EKN) za VIZ.

Upravljavec ne sme posredovati originalnih dokumentov, razen v primeru pisne odredbe sodišča oziroma, če tako zahtevajo veljavni predpisi.

Hramba originalnih dokumentov v izvirni e-obliki se izvaja skladno z lastnimi notranjimi pravili, ki se pripravijo v postopku prevzema pri Arhivu RS potrjenih Vzorčnih notranjih pravil Logitus.

Vsako posredovanje osebnih podatkov izven lokacije upravljavca, na kakršnokoli pisno zahtevo, ki ne izhaja iz potrebe po obdelavi podatkov s strani tretjih oseb, ki jim je upravljavec dolžan posredovati

podatke, mora odgovorna oseba, ki je osebne podatke posredovala, zabeležiti v **evidenco o ravnanju z osebnimi podatki**.

Upravljavec vodi in hrani evidenco o ravnanju z osebnimi podatki v papirnati obliki in sicer v tajništvu šole.

Evidenca o ravnanju z osebnimi podatki mora vsebovati najmanj naslednje podatke:

- zap. št. zahteve,
- datum prejetja zahteve za posredovanje,
- upravičenec oziroma naslovnik posredovanja,
- posredovano pooblaščeni osebi (opcijsko),
- način posredovanja,
- navedba posredovanih podatkov oziroma dokumentov,
- namen posredovanja,
- kategorija osebnih podatkov (opcijsko za posebne vrste osebnih podatkov),
- pravna podlaga (opcijsko),
- podpis ali odobritev odgovorne osebe, ki je podatke posredovala,
- podpis ali odobritev odgovorne osebe za zbirko osebnih podatkov (opcijsko).

V utemeljenih primerih (tj. za izvajanje zakonskih obveznosti, nalog v javnem interesu, za zaščito življenjskih interesov ali zaradi zakonitih interesov) se lahko osebni podatki razkrijejo ali posredujejo tudi osebam, ki se izkažejo z ustrezno zakonsko podlago. Prav tako se lahko osebni podatki razkrijejo oziroma posredujejo osebam, ki izkažejo pisno zahtevo oziroma privolitev za razkritje oziroma posredovanje podatkov, dano s strani posameznika, na katerega se podatki nanašajo.

Razkritje tretjim osebam, ki prejmejo osebne podatke v okviru delovanja ali poslovanja upravljavca (npr. sistematski pregledi, nacionalno preverjanje znanja ipd.), se ne beleži.

9. člen

(Čas hrambe in brisanje osebnih podatkov)

Čas hrambe in izvedba brisanja podatkov se izvaja skladno z veljavno zakonodajo. Obdelava osebnih podatkov poteka v obsegu z namenom obdelave in za čas do izpolnitve cilja obdelave, za čas, ki je potreben za dokazljivo izvajanje dejavnosti upravljavca ali za čas, v katerem je mogoče uveljavljati odgovornost izvajalca v zvezi z njegovimi ravnanji.

Izjemoma se lahko obdobje hrambe osebnih podatkov podaljša v primerih kot so:

- tekoči postopki pristojnih organov Republike Slovenije ali organov drugih držav članic EU, če obstaja verjetnost, da bo upravljavec potreboval zapise osebnih podatkov, da dokaže skladnost svojega ravnanja z veljavnimi predpisi ali
- tekoče pravdne ali druge podobne (na primer arbitražne, mediacijske, konciliacijske) zadeve, pri katerih obstaja verjetnost, da bo upravljavec potreboval zapise osebnih podatkov.

Brisanje osebnih podatkov v informacijskih sistemih, ki predstavljajo metapodatke ali elemente za priklic gradiva iz dolgoročne e-hrambe, se ne izvaja pred izbrisom gradiva, ki je povezano s temi metapodatki. Vse aktivnosti z dokumentarnim in arhivskim gradivom v eHrambi Logitus upravljavec izvede skladno z določbami prevzetih vzorčnih notranjih pravil Logitus. Dokumentarno gradivo in z njim povezane osebne podatke je upravljavec dolžan hraniti najmanj do najkrajšega roka hrambe, ki je opredeljen v veljavnem enotnem klasifikacijskem načrtu (EKN) za VIZ. Arhivsko vzorčno in arhivsko gradivo ter z njim povezane podatke (tudi osebne podatke) pa je upravljavec dolžan hraniti do dokumentirane izvedbe postopkov odbiranja, izločanja ter izročanja gradiva pristojnim arhivom skladno z njihove strani prejetimi navodili za odbiranje in strokovno tehničnimi navodili.

Vzorčna notranja pravila in tudi notranja pravila skladno z določbami ZVDAGA opredeljujejo ravnanje samo z digitalno obliko zapisa dokumentov. Navodila pristojnih arhivov pa se nanašajo na vse vrste zapisov gradiva.

Pred uničenjem podatkov in dokumentov je DPO, v sodelovanju s skrbnikom e-hrambe pri upravljavcu, dolžan vsakokrat preveriti obveznosti varovanja dokumentov in v njih vsebovanih podatkov tudi v veljavnih navodilih za odbiranje ter strokovno tehničnih navodilih, ki jih upravljavcu izda pristojni arhiv.

Uničevanje osebnih podatkov na nosilcih zapisa, ne glede na obliko, se mora izvajati tekoče in ažurno in jo izvajajo vse odgovorne osebe pri upravljavcu. Praviloma se aktivnosti uničevanje izvajajo obdobno in sicer ob primernih časovnih mejnikih: ob zaključku šolskega ali koledarskega leta, po predaji gradiva pristojnim arhivom, ob zaključku finančno računovodskega obdobja, ipd..

Fizični papirnati nosilci osebnih podatkov se uničijo kot zaupni odpad tako, da se križno razrežejo, sežgejo ali se uničijo na drug način, ki zagotavlja primerljivo stopnjo neobnovljivosti podatkov. Elektronski, optični, magnetni ali drugi nosilci, na katerih so osebni podatki trajno in neizbrisno zapisani, se izbrišejo tako, da se uničijo nosilci podatkov, ki morajo z uničenjem postati neuporabni in neobnovljivi. Osebni podatki na elektronskih, optičnih, magnetnih oziroma drugih nosilcih, na katerih podatki niso trajno in neizbrisno zapisani, se uničijo z izbrisom podatkov iz teh nosilcev. Če upravljavec razpolaga z ustreznimi sredstvi, se ti podatki iz nosilcev izbrišejo z varnim nepovratnim elektronskim izbrisom. Osebni podatki v eHrambi Logitus se izbrišejo skladno z določbami prevzetih vzorčnih notranjih pravil Logitus. Izbris osebnih podatkov se v vsakem primeru dokumentira na primeren način (na primer z zapisnikom, uradnim zaznamkom, avtomatično v informacijskem sistemu ipd.).

3 Ukrepi za varno obdelavo osebnih podatkov

10. člen

(Obveznost in odgovornost za izvajanje ukrepov)

Izvajanje organizacijskih ukrepov so dolžni zagotoviti vsi zavezanci po tem pravilniku.

Pooblaščene osebe za obdelavo osebnih podatkov, interni koordinator za varstvo podatkov in pooblaščena oseba za varstvo podatkov v zvezi s postopki obdelave prevzemajo tudi odgovornost v okviru lastnih zadolžitev in podeljenih pooblastil.

Ukrepe za zakonito in varno obdelavo osebnih podatkov, ki jih je dolžan izvajati obdelovalec, se določijo s pogodbo z obdelovalcem.

Izvajalec, zaposleni in pooblaščene osebe pri izvajalcu so dolžni izvajati ukrepe za zagotavljanje varstva osebnih podatkov, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta Pravilnik.

11. člen

(Obvezni ukrepi za varno obdelavo OP)

Upravljavec za preprečevanje nepooblaščenega dostopa, razkritja ali posredovanja osebnih podatkov ali drugo obliko zlorabe osebnih podatkov izvaja naslednje ukrepe:

- Organizacijski ukrepi:
  - dosledno vodenje evidenc dejavnosti obdelave osebnih podatkov ter oznaka posebnih vrst osebnih podatkov na evidenci, ki takšne podatke vsebuje,
  - dosledno vodenje seznama (internih in zunanjih) pooblaščenih oseb za obdelavo osebnih podatkov, izjav o varstvu osebnih podatkov in informiranje ter usposabljanje pooblaščenih oseb za obdelavo osebnih podatkov,
  - sklepanje pogodb o obdelavi osebnih podatkov z zunanjimi pogodbenimi obdelovalci osebnih podatkov, ter po potrebi vnos določb o varstvu osebnih podatkov v pogodbe o zaposlitvi in druge pogodbe z delavci, ki so pod neposrednim vodstvom upravljavca,
  - ozaveščanje vseh (internih in zunanjih) oseb, ki so jim dodeljena pooblastila za obdelavo osebnih podatkov, o relevantnih določilih tega pravilnika, ter o njihovih obveznostih in odgovornostih v zvezi z varstvom osebnih podatkov,
  - imenovanje internega koordinatorja za varstvo podatkov in pooblaščene osebe za varstvo podatkov (DPO),
  - zagotavljanja izobraževanja internemu koordinatorju za varstvo podatkov,
  - izvajanje rednih obdobnih (predvidoma letnih, lahko pa tudi pogostejših) pregledov nad ravnanjem oz. obdelavo osebnih podatkov,

    - predhodna izvedba ocene učinka v zvezi z varstvom podatkov (DPIA) v primerih izvedbe obsežnih obdelav, uvedbe novih sistemov, ki niso v uporabi pri reprezentativnem vzorcu (10%) istovrstnih iViZ ali implementacije nove tehnologije, ki bi lahko predstavljala tveganje za varstvo osebnih podatkov.
- Tehnični ukrepi:
    - zagotavljanje lastnih uporabniškim imen in drugih osebnih poverilnic za prijavo v informacijske sisteme, kjer se vrši obdelava osebnih podatkov,
    - zagotavljanje nadgradnje sistemske in antivirusne programske opreme na vseh računalnikih in strežnikih pri upravljavcu, kjer se izvaja obdelava osebnih podatkov,
    - uveljavljanje načela brezpogojen menjava gesel v VIZ informacijskih sistemih najmanj enkrat na 6 mesecev z dolžino vsaj 6 alfanumeričnih znakov,
    - preprečevanje možnosti skupinske prijave v VIZ informacijske sisteme,
    - uporaba osebnih kvalificiranih digitalnih potrdil za elektronsko podpisovanje ter dostopa do eHrambe Logitus
    - sprotno ažuriranje pooblastil odgovornih oseb v informacijskih sistemih skladno z dejanskim stanjem in organizacijskimi spremembami.

3.1 Evidence dejavnosti obdelav osebnih podatkov

12. člen

(Katalog evidenc dejavnosti obdelav osebnih podatkov)

Upravljavec vodi Katalog evidenc dejavnosti obdelav osebnih podatkov, ki vsebuje vse evidence dejavnosti obdelav osebnih podatkov upravljavca (v nadaljnjem besedilu: evidence OP). Zavezanec je lahko seznanjen s tistimi evidencami OP, ki so zanj relevantne.

Vsaka evidenca OP vsebuje vse naslednje informacije:

- o upravljavcu in pooblaščeni osebi za varstvo podatkov (DPO),
- namen obdelave,
- opis kategorij posameznikov, na katere se nanašajo osebni podatki,
- vrste osebnih podatkov in, kadar je to primerno, oznako, da gre za posebno vrsto osebnih podatkov,
- uporabnike ali kategorije uporabnikov, ki so jim ali jim bodo lahko razkriti osebni podatki,
- informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo,
- roke hrambe oziroma izbrisa različnih vrst podatkov,
- splošen opis varovanja osebnih podatkov in
- pravno podlago za obdelavo osebnih podatkov (neobvezno).

Upravljavec vodi in hrani evidence OP v papirnati obliki, ki se hrani tajništvu šole.

3.2 Pooblaščene osebe za obdelavo osebnih podatkov

13. člen

(Pooblaščene osebe za obdelavo osebnih podatkov)

Pooblaščene osebe za obdelavo osebnih podatkov so odgovorne za zakonito obdelavo ter varstvo in zavarovanje osebnih podatkov iz posameznih evidenc OP. Obveza varovanja osebnih podatkov, s katerimi se pooblaščena oseba seznani pri svojem delu, traja tudi po prenehanju delovnega razmerja pri upravljavcu, in sicer časovno neomejeno.

Pooblaščene osebe, ki pri svojem delu ali v imenu upravljavca obdelujejo osebne podatke iz posamezne evidence OP, lahko osebne podatke obdelujejo le pod pogojem, da imajo za obdelavo osebnih podatkov iz posamezne evidence ustrezno pisno pooblastilo.

Po tem pravilniku se kot ustrezno pooblastilo šteje vpis v **seznam pooblaščenih oseb**, ki ga potrdi zastopnik iVIZ. V seznamu pooblaščenih oseb se vodijo najmanj podatki:

- sistemizirano delovno mesto (v primeru podelitve skupinskih pooblastil) ali ime in priimek posamezne pooblaščene osebe za obdelavo osebnih podatkov,
- datum podelitve pooblastila ali vpisa v seznam in podpis odgovorne osebe,
- datum preklica pooblastila ali revizijska sled izbrisa s seznama in podpis odgovorne osebe,
- navedba evidenc OP, za katere so pooblaščeni zaposleni na določenem sistemiziranem delovnem mestu ali posamezna oseba,
- raven dostopa do osebnih podatkov znotraj posameznega informacijskega sistema, kadar je to relevantno (opcijsko),
- izjava o varovanju osebnih podatkov kot priloga k evidenci.

Pisno pooblastilo se lahko izda za posamezno ali več evidenc dejavnosti obdelav osebnih podatkov. Pisno pooblastilo mora biti podpisano s strani zakonitega zastopnika upravljavca, urejanje pooblastil pa praviloma ureja interni koordinator za varstvo podatkov.

Upravljavec vodi in hrani Seznam pooblaščenih oseb v papirnati obliki, ki se hrani v tajništvu šole.

Pogoj za veljavnost pooblastila je s strani pooblaščene osebe podpisana **Izjava za zaposlene**. Izjavo poda pooblaščena oseba v papirnati obliki in se hrani v tajništvu šole.

Pisno pooblastilo iVIZ pooblaščeni osebi oziroma sistemiziranim delovnim mestom velja do preklica. Po tem pravilniku se šteje, da je pisno pooblastilo preklicano z dnem dokumentiranega izbrisa iz **Seznama pooblaščenih oseb** in posredovanja ustreznega obvestila ali ob odpovedi delovnega razmerja. Obvestilo za sistemizirano delovno mesto se lahko objavi tudi na interni oglasni deski. **V primeru vpisa sistemiziranih delovnih mest v Seznam pooblaščenih oseb, posameznim zaposlenim na tem delovnem mestu, ni potrebno podeljevati dodatnih pooblastil kot je to določeno v izjavi Pooblastilo ustanove zaposlenemu, ki je del Izjav za zaposlene**

Z dnem preklica pooblastila mora upravljavec zagotoviti, da ne bo prišlo do nadaljnjega razkrivanja osebnih podatkov oziroma njihove obdelave, če je mogoče, tudi na način, da se osebi, ki ji je bilo preklicano pooblastilo, onemogoči dostop do osebnih podatkov (na primer z nastavitvami uporabniških računov, s kontrolo pristopa, z izročitvijo fizičnih dokumentov ipd.). Upravljavec mora zagotoviti sledljivost glede datuma izdaje in preklica posameznega pooblastila.

14. člen

(Dostop do informacijskih rešitev)

Pooblaščena oseba za obdelavo osebnih podatkov, ki pri svojem delu potrebuje dostop do informacijskih rešitev, v katerih so vsebovani osebni podatki, mora imeti v pooblastilu opredeljeno tudi raven dostopa do osebnih podatkov.

Obseg pooblastila je lahko omejen ali neomejen ter se loči (vsaj) na:

- testni uporabnik – uporabnik z dostopom do testnega okolja,
- uporabnik – običajen uporabnik,
- administrator – administrator v posamezni rešitvi.

Pooblaščena oseba za obdelavo osebnih podatkov mora z ustreznimi ukrepi skrbno varovati zaupnost ter ne sme nikoli posredovati ali razkriti svojega uporabniškega imena in gesla, certifikata (digitalno potrdilo) ali podatkov o dvofaktorski avtentikaciji za katerikoli dostop drugi osebi, niti ne nadrejeni osebi ali sodelavcu/-ki.

Razkritje iz prejšnje točke se šteje za varnostni incident, ki ga je treba obravnavati skladno s tem pravilnikom. Razkritje iz prejšnje točke predstavlja tudi kršitev določb tega pravilnika, glede na okoliščine lahko tudi hujšo ali namerno kršitev določb pravilnika.

Tehnološka sredstva za prijavo v informacijski sistem morajo ustrezati Politiki gesel, določeni v Prilogi G (Pravila uporabe IT poglavji 7 in 8) vzorčnih notranjih pravil Logitus. Podrobna pooblastila in oprema se pooblaščenim osebam podeli ter vodi skladno s Prilogo F (Prošnja za vzpostavitev ali dopolnitev pooblastil ter podelitev opreme, Prošnja za ukinitev pooblastil ter vračilo opreme), Prilogama G (Pravila in etika uporabe IT) ter Katalogom pooblastil, ki si vsi del vzorčnih notranjih pravil Logitus oziroma po njih pripravljenih lastnih notranjih pravil upravljavca.

15. člen

(Kršitve določb tega pravilnika)

Interni koordinator za varstvo podatkov obvesti zavezance, da lahko ravnanje, ki ni skladno s tem pravilnikom, povzroči negativne posledice, kot so izguba zaupanja uporabnikov storitev ali dobaviteljev upravljavca, pravdne, inšpekcijske ali prekrškovne postopke, finančne izgube in poslabšanje ugleda upravljavca. Zoper osebe, ki ravnajo v neskladju s tem pravilnikom, se lahko sprožijo ustrezni pravni postopki.

Hujše ali namerne kršitve določb tega pravilnika ali področne zakonodaje, prekoračitev ali zloraba pooblastil za obdelavo osebnih podatkov predstavlja kršitev delovnih obveznosti.

3.3 Interni koordinator za varstvo podatkov

16. člen

(Imenovanje internega koordinatorja za varstvo podatkov)

Upravljavec določi in imenuje internega koordinatorja za varstvo podatkov, ki upravljavcu pomaga pri izvrševanju tega pravilnika, predvsem v smislu izvajanja operativne organizacije in koordinacije varstva osebnih podatkov pri upravljavcu, ter sodeluje z DPO, tako da ga obvešča o vseh relevantnih informacijah in skrbi za implementacijo njegovih navodil ter priporočil. Interni koordinator za varstvo podatkov mora biti zaposlen pri upravljavcu in je lahko hkrati tudi DPO.

17. člen

(Naloge internega koordinatorja)

Interni koordinator za varstvo podatkov ima pri upravljavcu vsaj naslednje naloge:

1. Interno skrbništvo nad Kodeksom ravnanj iVIZ in s tem povezano skrbjo za ustrezno obveščenost zaposlenih, drugih delavcev in pogodbenih obdelovalcev v zvezi z varstvom podatkov, vključujoč skladnost s Kodeksom ravnanj iVIZ, internimi akti upravljavca ter veljavnimi predpisi na ravni EU in nacionalni ravni;
2. operativna organizacija in koordinacija vseh aktivnosti v zvezi z varstvom podatkov ter morebitnimi zahtevki;
3. Skrb za ažurnost evidenc iz Kodeksa ravnanj iVIZ;
4. Sodelovanje z vodstvom iVIZ in DPO ter sodelovanje pri sestankih o varovanju podatkov;
5. Poročanje DPO-ju glede dejanskega stanja v iVIZ, v primerih, ko mora biti obveščen DPO ali urad Informacijski pooblaščenec (v nadaljevanju nadzorni organ);
6. Skrb za implementacijo navodil in priporočil DPO ter nadzornega organa;
7. Skrb za posredovanje pogodb o obdelavi podatkov vsem pogodbenim obdelovalcem upravljavca;
8. Sodelovanje z nadzornim organom kot kontaktna točka, kadar ni kontaktna točka DPO;
9. Določitev plana in termina izvedbe internih presoj s področja varstva podatkov, ki vključujejo:
    - pripravo in ažuriranje seznama pogodbenih obdelovalcev podatkov pri upravljavcu
    - preveritev ali pripravo aktualne ocene tveganj s področja varstva podatkov
    - preveritev seznama podpisnikov izjav (interni zaposleni) s področja varstva podatkov pri upravljavcu
    - preveritev ustreznosti upravljavčevih katalogov evidenc obdelav
    - preveritev ustreznosti Kodeksa ravnanj in njegovih prilog za upravljavca ter posredovanje pripomb in predlogov dopolnitev DPO ter Logitus d.o.o.
10. Sodelovanje pri izvedbi letnih pregledov s področja varstva podatkov;
11. Sprotno obveščanje pooblaščene osebe za varstvo podatkov o incidentih s področja varstva podatkov pri upravljavcu;
12. Kreiranje in upravljanje zahtevkov s področja varstva podatkov za upravljavca na portalu Service Desk Logitus.

3.4 Pooblaščena oseba za varstvo podatkov (DPO)

18. člen

(Imenovanje DPO)

Upravljavec določi in imenuje pooblaščeno osebo za varstvo podatkov, ki upravljavcu na neodvisen način pomaga pri upravljanju področja varstva podatkov in zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe o varstvu podatkov ter določbami zakona, ki ureja varstvo osebnih podatkov in drugih predpisov, ki urejajo obdelavo in varstvo osebnih podatkov pri opravljanju dejavnosti vzgoje in izobraževanja.

19. člen

(Naloge DPO)

Pooblaščena oseba za varstvo podatkov ima vsaj naslednje naloge:

- sodelovanje z internim koordinatorjem za varstvo podatkov ter izvedba nalog, za katere je DPO zaprošen s strani internega koordinatorja za varstvo podatkov oziroma zastopnika ali drugih odgovornih oseb upravljavca;
- svetovanje internemu koordinatorju za varstvo podatkov ter po potrebi tudi zaposlenim, ki izvajajo obdelavo, o njihovih obveznostih v skladu s Splošno Uredbo o varstvu podatkov in drugimi določbami prava Unije ali nacionalne zakonodaje iz področja varstva osebnih podatkov;
- spremljanje skladnosti Kodeksa ravnanj iVIZ in ravnanja upravljavca s Splošno Uredbo o varstvu podatkov, drugimi določbami prava Unije ali nacionalne zakonodaje s področja varstva osebnih podatkov in politikami upravljavca v zvezi z varstvom osebnih podatkov, vključno s predlogi porazdelitve nalog,
- obveščanje, ozaveščanje in usposabljanje internega koordinatorja za varstvo podatkov ter osebja, vključenega v dejanja obdelave, ter s tem povezanimi internimi presojami s področja varstva podatkov;
- svetovanje pri izvajanju politike varnostnih incidentov;
- svetovanje vodstvu pri izvajanju ocene učinka tveganja in spremljanje njenega izvajanja;
- sodelovanje z nadzornim organom (urad Informacijski pooblaščenec RS);
- delovanje kot kontaktna točka za nadzorni organ, še posebej pri kompleksnih vsebinskih vprašanjih v zvezi z obdelavo osebnih podatkov pri izvajalcu, vključno s predhodnim posvetovanjem v primerih, ko je iz ocene učinka razvidno, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja, in, kjer je ustrezno, posvetovanje glede drugih zadev;
- izvajanje aktivnosti, potrebnih za ustrezno komunikacijo s posamezniki, na katere se nanašajo osebni podatki in ki s pooblaščeno osebo za varstvo podatkov stopijo v stik glede vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic na podlagi Splošne uredbe o varstvu podatkov in drugih veljavnih predpisov s področja varstva osebnih podatkov;
- sodelovanje pri izvedbi internih pregledov, tudi v zvezi zakonitostjo izvajanja dejavnosti obdelave osebnih podatkov,
- druge naloge, za izvedbo katerih se v posameznem primeru dogovorita pooblaščena oseba za varstvo podatkov in upravljavec.

Kadar je na funkcijo pooblaščene osebe za varstvo podatkov imenovana zunanja oseba, se podrobnosti glede njenih nalog, njihovega izvajanja ter plačila zanje uredijo v pogodbi s to osebo.

Pooblaščena oseba za varstvo podatkov lahko po lastni presoji, upoštevajoč zahtevnost in pomembnost nalog, znanje in usposobljenost internega koordinatorja za varstvo podatkov ter morebitne druge relevantne okoliščine, delegira posamezne naloge, ki jih opravlja skladno s tem pravilnikom, internemu koordinatorju za varstvo podatkov. Interni koordinator za varstvo podatkov se mora ravnati po navodilih pooblaščene osebe za varstvo podatkov, v okviru svojega znanja in usposobljenosti izvesti delegirane naloge in po potrebi poročati pooblaščeni osebi za varstvo podatkov. V primeru, da interni koordinator sam nima ustreznega znanja in usposobljenosti za izvedbo posamezne naloge, lahko pooblaščena oseba za varstvo podatkov določi, da nalogo izvede skupaj z internim koordinatorjem za varstvo podatkov.

Interni koordinator se mora tudi v takem primeru ravnati po navodilih ter sodelovati s pooblaščeno osebo za varstvo podatkov.

20. člen

(Obveščanje DPO)

Katerakoli zaposlena oseba pri upravljavcu ali druga oseba pod neposrednim vodstvom upravljavca, še slasti pooblaščena oseba za obdelavo osebnih podatkov, ali pogodbeni obdelovalec mora, ko izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov ipd.) ali vdora v zbirko osebnih podatkov, o tem takoj obvestiti internega koordinatorja. Kadar oseba meni, da obvestitev navedene osebe bi bila učinkovita, oziroma če je zadeva nujna, interni koordinator za varstvo podatkov pa ni razpoložljiv, o zlorabi osebnih podatkov neposredno obvesti pooblaščeno osebo za varstvo podatkov.

Interni koordinator opravi prvo analizo stanja in po lastni presoji v nadaljnje korake vključi tudi pooblaščeno osebo za varstvo podatkov. Slednji mora biti obveščen takoj, vsaj v vseh primerih, o katerih je potrebno v roku 72 ur obvestiti urad Informacijski pooblaščenec.

V kolikor katerakoli druga oseba izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščeno uničenje, spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov ipd.) ali vdora v zbirko osebnih podatkov, mora o tem takoj obvestiti pooblaščeno osebo za varstvo podatkov na kontakt, ki je objavljen na spletni strani upravljavca.

21. člen

(Strokovna usposobljenost DPO)

Pooblaščena oseba za varstvo podatkov mora imeti ustrezno strokovno znanje za opravljanje nalog in obveznosti. V ta namen upravljavec kot osebo, pooblaščeno za varstvo podatkov, imenuje internega zaposlenega ali zunanjo osebo za varstvo podatkov, s katero sklene pogodbo o opravljanju storitve pooblaščene osebe za varstvo podatkov. V primeru, ko je na funkcijo pooblaščene osebe za varstvo podatkov imenovana interna oseba upravljavca, ta oseba pri upravljavcu ne sme imeti možnosti opredelitve namenov oziroma storitev obdelave osebnih podatkov, kar pomeni, da pooblaščena oseba za varstvo podatkov ne sme biti oseba upravljavca z vodstvenimi pooblastili.

V primeru, kadar je kot pooblaščena oseba za varstvo podatkov imenovana interna oseba upravljavca, ji je upravljavec dolžan zagotoviti redno strokovno usposabljanje in izobraževanje s področja varstva osebnih podatkov. Interna pooblaščena oseba za varstvo podatkov se mora udeležiti izobraževanja ali usposabljanja s področja varstva osebnih podatkov najmanj enkrat v obdobju dveh zaporednih koledarskih let. Udeležba izobraževanja oziroma usposabljanja ni potrebna, če pooblaščena oseba za varstvo podatkov izkazuje ohranjanje strokovne usposobljenosti s strokovnim oziroma znanstvenim publiciranjem na področju varstva osebnih podatkov. Kadar je na funkcijo pooblaščene osebe za varstvo podatkov imenovana zunanja oseba, se lahko ohranjanje njene strokovne usposobljenosti alternativno zagotavlja tudi s pridobivanjem izkušenj pri opravljanju te funkcije pri večjem številu istovrstnih oseb.

3.5 Pogodbena obdelava osebnih podatkov

22. člen

(Obdelovalci)

Posamezna opravila v zvezi z obdelavo osebnih podatkov v imenu upravljavca lahko opravlja obdelovalec osebnih podatkov (obdelovalec), ki je registriran za opravljanje takšne dejavnosti in zagotavlja postopke in ukrepe za zavarovanje in varstvo osebnih podatkov, ki so potrebni za varstvo podatkov pred naključnim ali nezakonitim uničenjem ali naključno izgubo, spreminjanjem, nepooblaščenim posredovanjem ali dostopom ali katerim koli drugim nezakonitim načinom obdelave.

Pogodbeno obdelavo osebnih podatkov pri obdelovalcu ureja pogodba ali drug pravni akt, kadar tako določajo veljavni predpisi s področja varstva osebnih podatkov. Pogodba o obdelavi osebnih podatkov

mora biti pripravljen skladno s prilogo Kodeksa ravnanj (**Pogodba o obdelavi osebnih podatkov**) ali mora samostojno ali skupaj s splošnimi pogoji in politikami zasebnosti (v primeru uporabe standardiziranih predlog pogodb posredovanih s strani ponudnikov IT storitev) vsebovati najmanj informacije:

- vsebina in trajanje obdelave osebnih podatkov,
- opis narave in namena obdelave,
- vrsta ali opis obdelovanih osebnih podatkov,
- kategorije posameznikov, na katere se nanašajo osebni podatki (opcijsko po potrebi),
- najmanj naslednje pravice in obveznosti upravljavca in obdelovalca: dolžnost poročanja obdelovalca, pravica do nadzora s strani upravljavca, tehnični in organizacijski varnostni ukrepi, način izbrisa ali vrnitve osebnih podatkov in morebitnih kopij le-teh ob prenehanju pogodbenega razmerja ter roki za vračilo, notifikacijska (obvestilna) dolžnost pred vključitvijo novega obdelovalca s strani obdelovalca (»podobdelovalec«) ter pogoji za podobdelovalca, obvezno ravnanje obdelovalca v primeru spora z upravljavcem, obvezno ravnanje v primeru prenehanja obdelovalca,
- vsa druga obvezna določila skladno s Splošno uredbo o varstvu podatkov.

Pogodba ali drug pravni akt po določbah tega člena mora biti sestavljena pisno v fizični (papirnati) ali elektronski obliki.

Pooblaščena pravna ali fizična oseba, ki opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti sprejet primerljiv način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

Upravljavec vodi evidenco sklenjenih pogodb z obdelovalci skladno s prilogo Kodeksa ravnanj (**Seznam pooblaščenih oseb)**, ki ga potrdi zastopnik iVIZ. V seznamu pooblaščenih oseb se vodijo najmanj podatki:

- naziv pogodbenega obdelovalca,
- kratek opis obdelave,
- številka pogodbe o obdelavi in datum sklenitve.

3.6 Interne presoje skladnosti dejavnosti obdelav osebnih podatkov z veljavnimi predpisi

23. člen

(Presoje skladnosti)

Upravljavec mora redno izvajati interne presoje skladnosti izvajanja dejavnosti obdelave osebnih podatkov z veljavnimi predpisi. Presoje skladnosti se izvajajo najmanj enkrat letno.

Letne, redne presoje se izvajajo v sodelovanju z družbo Logitus sočasno s pregledom dejanskega izvajanja notranjih pravil in uporabe eHrambe Logitus. Interne presoje se dokumentira skladno z določili in prilogami tega Kodeksa ravnanj (**Pregled varstva podatkov** in **Vprašalnik s povzetkom za oceno tveganj varstva podatkov)**.

Interni koordinator varstva podatkov ali DPO lahko vodstvu iVIZ iz utemeljenih razlogov predlagata tudi izvedbo izredne presoje. Predlog za izvedbo izredne presoje mora biti obrazložen. Za izvedbo (oziroma odsotnost izvedbe) rednih in izrednih presoj je odgovoren zakoniti zastopnik upravljavca.

3.7 Predhodna izvedba DPIA

24. člen

(Ocena učinka v zvezi z varstvom osebnih podatkov)

Upravljavec je dolžan izvesti oceno učinka le v pogojih, določenih v Kodeksu ravnanj iVIZ.

4 Tehnični ukrepi za varno obdelavo osebnih podatkov

25. člen

(Prostori in nosilci osebnih podatkov)

Nosilci osebnih podatkov so vsak računalniški ali elektronski nosilec podatkov, vsak dokument (v papirnati ali elektronski obliki), na katerem je zapisan osebni podatek, in strojna ter programska oprema. Varovani morajo biti z organizacijskimi ukrepi, določenimi s tem pravilnikom in Prilogama G Kodeksa ravnanj, ki nepooblaščenim osebam onemogočajo dostop do osebnih podatkov.

Nepooblaščene osebe ne smejo vstopati v prostore kjer se nahajajo osebni podatki brez spremstva ali prisotnosti pooblaščenega zaposlenega delavca. Delavec, ki dela v teh prostorih, mora vestno in skrbno nadzorovati prostor, vstope in izstope iz prostora ter ob zapustitvi prostor zakleniti. V kolikor so pri upravljavcu nameščena druga tehnična sredstva za preprečevanje oziroma odkrivanje nepooblaščenih vstopov v prostore (na primer alarmni sistem, video nadzorni sistem), je treba ta sredstva dosledno uporabljati.

Delavec, ki pri delu obdeluje osebne podatke, nosilcev osebnih podatkov ne sme puščati nenadzorovanih ali jih kako drugače izpostavljati nevarnosti vpogleda vanje nepooblaščenim osebam oziroma nepooblaščenim delavcem.

V prostorih, v katere imajo vstop uporabnimi storitev oziroma osebe, ki niso zaposlene pri upravljavcu oziroma niso pooblaščene za obdelavo osebnih podatkov, morajo biti nosilci podatkov in računalniški prikazovalniki nameščeni v času obdelave ali dela na njih tako, da je uporabnikom storitev in drugim nepooblaščenim osebam onemogočen vpogled oz. dostop do osebnih podatkov. Nastavljeni morajo biti tudi ohranjevalniki zaslona za čas neaktivnosti delavca na računalniški opremi.

Poslovni partnerji in drugi obiskovalci se smejo gibati v prostorih upravljavca le ob prisotnosti delavca, ki mora skrbeti za to, da je dostop ali vpogled v nosilce podatkov nepooblaščenim osebam onemogočen. Prostori upravljavca se morajo redno zaklepati, s čimer se nepooblaščenim osebam prepreči nenapovedan oziroma nedovoljen vstop.

Tehnično-vzdrževalni delavci in čistilke se lahko gibljejo v poslovnih prostorih izven delovnega časa in brez prisotnosti pooblaščenega delavca le, če so nosilci osebnih podatkov shranjeni v zaklenjenih omarah ali arhivu (npr. ognjevarni sef oziroma omare), tehnično-vzdrževalni delavci in čistilke pa nimajo ključev teh omar ali arhivov oziroma so osebni podatki shranjeni na za njih nedostopnih elektronskih medijih.

Delavci, ki zaznajo nepooblaščen vstop v prostore upravljavca, nepooblaščen dostop do omar, medijev, programov ali opreme, na kateri se nahajajo osebni podatki, ali sum takega ravnanja, morajo o tem nemudoma obvestiti internega koordinatorja za varstvo podatkov. Slednji, po potrebi s posvetovanjem z zakonitim zastopnikom upravljavca ali pooblaščeno osebo za varstvo podatkov, presodi (predvsem upoštevajoč namen nepooblaščenega vstopa ali dostopa), kakšna so potrebna nadaljnja ravnanja (na primer ozaveščanje delavcev, izboljšanje sistema varovanja, disciplinski postopki, obvestitev pristojnih organov) ter po potrebi poda priporočilo zakonitemu zastopniku upravljavca.

26. člen

(Vstop zaposlenih v pisarne)

Za dostop do pisarne je potrebno imeti ključe pisarne. Ključe dodeli ravnatelj šole. Dvojnike ključev pisarne je delavcem prepovedano izdelovati, razen v kolikor to ni izrecno naročeno delavcu s strani ravnatelja.

Ključev se ne sme puščati v ključavnici v vratih z zunanje ali notranje strani. Glavna vhodna vrata ob neprisotnosti vsaj enega delavca se sproti zaklepajo.

Ključa/dostopne kartice ali vstopne alarmne kode delavec ne sme posojati, dajati ali razkrivati drugim osebam, niti v kolikor so to drugi delavci. V primeru izgube ali kraje mora delavec nemudoma obvestiti

zastopnika upravljavca oziroma drugo osebo, ki ji je pri upravljavcu dodeljeno skrbništvo nad ključi, dostopnimi karticami oziroma alarmnimi kodami.

27. člen

(Ukrepi za varovanje sistemske in aplikativne računalniške opreme)

Dostop do računalniške programske opreme, kjer so shranjeni osebni podatki, mora biti varovan na način, ki omogoča dostop samo pooblaščenim delavcem.

Računalniki, na katerih se obdelujejo osebni podatki, morajo biti ustrezno zaščiteni s sodobno antivirusno zaščito, imeti nameščen ohranjevalnik zaslona in nastavljeno omogočanje avtomatičnih popravkov operacijskega sistema.

Delavci oziroma pooblaščene osebe za obdelavo osebnih podatkov morajo upoštevati vsa interna navodila (Politike G) v zvezi z računalniško opremo in temu primerno računalnike tudi uporabljati.

Informatik upravljavca skrbi, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja strojne, sistemske ali aplikativne programske opreme z osebnimi podatki ob morebitnem kopiranju, po prenehanju potrebe po kopiji, kopija brez nepotrebnega odlašanja uniči.

Informatik upravljavca mora biti v času servisiranja računalnika ali programske opreme, ki vsebuje osebne podatke, ves čas prisotna in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki, zlasti v primeru, če se v računalniku nahajajo osebni podatki posebne vrste.

Shranjevanje osebnih podatkov na računalnike, ki niso namenjeni opravljanju dela pri upravljavcu, ni dovoljeno. Enako velja glede shranjevanja osebnih podatkov na medije.

Delavec, ki osebne podatke shranjuje na tak računalnik oziroma medij, je, v kolikor bi prišlo do razkritja ali nepooblaščene obdelave osebnih podatkov zaradi takega ravnanja, tudi civilno in kazensko odgovoren.

Dostop do osebnih podatkov mora biti vedno zavarovan vsaj z geslom za prijavo v računalnik.

Namenska, osebna gesla se redno spreminjajo, zlasti pa ob vsakem sumu, da je prišlo do zlorabe gesla. Novo geslo ne sme biti enako ali podobno prejšnjemu.

Gesel za dostop do osebnih podatkov se ne sme shranjevati na papirju ali na način, da je dostop do gesel omogočen nepooblaščenim osebam. V primeru zlorabe gesla ali suma zlorabe gesla, je potrebno geslo nemudoma spremeniti ter o zlorabi gesla ali sumu zlorabe gesla obvestiti internega koordinatorja za varstvo podatkov, osebo, ki je odgovorna za dodeljevanje gesel, ali zakonitega zastopnika upravljavca.

Delavec, ki ima dostop do katerekoli informacijske rešitve ali evidence, mora pri delu z osebnimi in zaupnimi podatki ravnati še posebej skrbno, da se ne razkrijejo osebni podatki nepooblaščeni osebi ali razkrijejo zaupni podatki, ki se štejejo za poslovno skrivnost upravljavca ali njegovih pogodbenih partnerjev.

Delavec ne sme nikoli posredovati ali razkriti svojega uporabniškega imena, gesla ali certifikata (digitalno potrdilo) za katerikoli dostop nepooblaščeni osebi, temveč mora zaupnost teh podatkov varovati z najvišjo skrbnostjo.

Razkritje uporabniškega imena, gesla ali certifikata drugi osebi pomeni zelo resne kršitve varstva osebnih podatkov, ki se varujejo v skladu s tem pravilnikom, ter hudo kršitev delovnega razmerja in lahko predstavlja razlog za odpoved pogodbe o zaposlitvi ter odškodninske zahteve, ob ugotovitvi suma namena zlorabe pa tudi naznanitev pristojnim organom.

5 Politika varnostnih incidentov

28. člen

(Zloraba osebnih podatkov)

Za zlorabo osebnih podatkov se šteje vsaka uporaba oziroma obdelava osebnih podatkov v namene, ki ni v skladu z namenom upravljanja podatkov, s Splošno uredbo o varstvu podatkov, z zakonom ali s pogodbo zaposlene osebe, delavca oziroma pogodbenega partnerja z upravljavcem osebnih podatkov, na podlagi katere se podatki obdelujejo, ali namenom, določenem v evidenci dejavnosti obdelav osebnih podatkov.

Kot zloraba se šteje tudi kršitev varstva osebnih podatkov, to je kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani

Za poskus zlorabe šteje poskus uporabe osebnih podatkov v nedovoljene namene. Zastopnik upravljavca mora zoper tistega, ki je zlorabil osebne podatke ali je nepooblaščeno vdrl v zbirko osebnih podatkov, ustrezno ukrepati.

Za zlorabo osebnih podatkov se šteje, primeroma:

- nepooblaščen vpogled v osebne podatke,
- nepooblaščeno odkrivanje oziroma razkrivanje osebnih podatkov,
- nepooblaščeno uničenje,
- nepooblaščeno spreminjanje,
- poškodovanje zbirke,
- vdor v zbirko osebnih podatkov,
- prilaščanje osebnih podatkov.

29. člen

(Ukrepanje ob ugotovitvi zlorabe osebnih podatkov)

Kdorkoli, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov, mora izvesti postopke skladno s 20. členom tega pravilnika.

Vsi zaposleni oziroma drugi delavci in pogodbeni obdelovalci morajo slediti navodilom internega koordinatorja za varstvo podatkov ali DPO-ja z namenom, da se čimprej zaustavi nadaljnja zloraba osebnih podatkov oziroma njene škodljive posledice ter zavaruje dokaze.

Vdor ali kakršenkoli drug informacijski varnostni incident je interni koordinator ali pooblaščena oseba za varstvo podatkov dolžan dokumentirati skladno z določili vzorčnih notranjih pravil (**Priloga F, Identifikacija varnostnega incidenta**), katerega minimalna zahtevana vsebina je podatek o vsebini kršitve varstva osebnih podatkov, dejstva v zvezi s kršitvijo, njeni učinki in sprejeti popravni ukrepi. Vzorec **poročila** je dostopen v samopomoči na portalu Service Desk Logitus (http://servicedesk.logitus.com).

Priporočljivo je, da interni koordinator za varstvo podatkov, po potrebi ob sodelovanju pooblaščene osebe za varstvo podatkov, po vsakem odkritem incidentu zlorabe osebnih podatkov izvede analizo stanja ter identificira okoliščine, ki so omogočile ali znatno doprinesle k incidentu zlorabe osebnih podatkov. V zvezi s temi okoliščinami se opredeli tveganje njihove ponovitve ter predvidi ukrepe za zmanjšanje tega tveganja. Predvideni ukrepi morajo biti sorazmerni glede na verjetnost ponovitve incidenta, resnost njegovih posledic ter naravo osebnih podatkov (resneje je treba obravnavati incidente v zvezi s posebnimi vrstami osebnih podatkov), pri čemer se upošteva tudi razpoložljive vire upravljavca. V zvezi s predvidenimi ukrepi se določi rok in odgovorno osebo za njihovo izvedbo, ob poteku tega roka pa se dokumentira dejansko stanje ter oceni uspešnost implementacije ukrepov. Po potrebi se predlaga tudi spremembo tega pravilnika.

V primeru kršitve varnosti osebnih podatkov je zakoniti zastopnik upravljavca dolžan brez nepotrebnega odlašanja najpozneje v 72 urah po seznanitvi s kršitvijo o kršitvi obvestiti urad Informacijski

pooblaščenec RS. V ta namen interni koordinator za varstvo podatkov v sodelovanju z DPO preveri, ali poročilo vsebuje naslednjo minimalno zahtevano vsebino:

- 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 DPO ali druge kontaktne osebe, 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, če je to ustrezno.

Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, je upravljavec dolžan o tem obvestiti posameznike, čigar osebnih podatki so bili zajeti v varnostni incident. Obveznost obveščanja ni podana, če ni izkazana verjetnost, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov, na katere se kršitev nanaša.

6 Uresničevanje pravic posameznikov

30. člen

(Pravice posameznikov)

Upravljavec mora posameznikom zagotoviti vse pravice, ki jih ima slednji po veljavnih predpisih in sicer:

- pravica dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki in kadar je tako, dostop do osebnih podatkov (tj. vpogled ter njihovo prepisovanje ali kopiranje) in naslednje informacije:
  - namen obdelave,
  - vrste zadevnih osebnih podatkov,
  - uporabnike ali kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabniki v tretjih državah ali mednarodnih organizacijah,
  - predvideno obdobje hrambe osebnih podatkov,
- omogoči popravek netočnih osebnih podatkov v zvezi z njim in mu omogoči dopolnitev nepopolnih osebnih podatkov, vendar le skladno z veljavno zakonodajo in pod pogojem, da podatki niso pridobljeni iz centralnih uradnih evidenc,
- omogoči pravico do izbrisa osebnih podatkov (t. i. pravica do pozabe),
- omogoči pravico do omejitve uporabe,
- omogoči pravico do ugovora obdelave,
- omogoči pravico do prenosljivosti podatkov in mu posreduje podatke v strukturirani, splošno uporabljeni in strojno berljivi obliki ali jih neposredno posreduje drugemu upravljavcu.

Upravljavec na zahtevo posameznika slednjemu posreduje:

- izpis osebnih podatkov, ki so vsebovani v zbirki osebnih podatkov in se nanašajo nanj,
- seznam uporabnikov, katerim so bili posredovani osebni podatki, kdaj, na kakšni podlagi in za kakšen namen,
- informacije o virih, na katerih temeljijo zapisi, ki jih o posamezniku vsebuje zbirka osebnih podatkov, in o metodi obdelave,
- informacije o namenu obdelave in vrsti osebnih podatkov, ki se obdelujejo, ter vsa potrebna pojasnila v zvezi s tem.

Omejitve pravic posameznikov so dopustne izključno v primerih, ki jih določajo veljavni predpisi.

Vsebina pravic posameznikov, njihove omejitve ter način uresničevanja le-teh so navedene v **Informacijah za posameznike**, ki so javno objavljene. Upravljavec mora zagotoviti, da so vse pooblaščene osebe za obdelavo osebnih podatkov, interni koordinator za varstvo podatkov in DPO seznanjeni z Informacijami za posameznike in vsebino pravic, ki jih imajo posamezniki.

Upravljavec v okviru reševanja zahtev iz naslova uresničevanja pravic posameznikov po Splošni uredbi o varstvu podatkov vzpostavi in vodi **evidenco postopkov uresničevanja pravic posameznikov**, v katero vpisuje najmanj:

- posameznika, ki je zahtevo podal,
- vsebino zahteve ali opravilno številko, pod katero se zadeva rešuje ter
- status reševanja zadeve.

Posamezne zahteve iz naslova uresničevanja pravic posameznikov upravljavec hrani v papirnati obliki in sicer v tajništvu šole. (*Vsebina posamezne zahteve ni predmet evidence postopkov po Splošni uredbi o varstvu podatkov, pač pa se hrani in jasno evidentira v okviru skupne zadeve, v kateri so razvidne zahteve posameznikov za uresničevanje pravic po GDPR*.)

7 Zaupni podatki in poslovna skrivnost

[*Upravljavec lahko v tem poglavju podrobneje opredeli druge podatke in informacije, ki jih je treba varovati kot zaupne oziroma za katere ima vzpostavljeno politiko varovanja, ki je enaka ukrepom za varstvo in zavarovanje osebnih podatkov. Upravljavec ima lahko v ta namen ločen notranji akt ali je brez slednjega.]*

31. člen

(Varstvo zaupnih podatkov oziroma poslovne skrivnosti)

Zaposleni in druge osebe, ki so pooblaščene za dostop do podatkov upravljavca, morajo pri izvrševanju svojih funkcij oziroma delovnih obveznosti varovati zaupnost podatkov, za katere je upravljavec pisno določil, da so zaupne narave ter podatkov, za katere je mogoče v danih okoliščinah razumno sklepati, da se jih ohrani kot skrivnost. Podatke, ki so zaupne narave oziroma predstavljajo poslovno skrivnost upravljavca, morajo osebe, ki do njih dostopajo, varovati tako, da:

- jih ne razkrivajo, posredujejo ali omogočajo kakršno koli drugačno seznanitev z njimi nepooblaščenim osebam;
- uporabljajo zaupne informacije zgolj za dovoljene namene njihove uporabe ter v najmanjšem potrebnem obsegu za dosego teh namenov;
- zaupne informacije razmnožujejo le v najmanjšem obsegu, ki je potreben za izpolnitev dovoljenih namenov njihove uporabe, pri čemer morajo zagotoviti, da je zaupnost kopij varovana enako, kot zaupnost izvirnih zaupnih informacij;
- na zahtevo odgovorne osebe upravljavca nemudoma uničijo vse zaupne informacije, v vseh oblikah, na vseh nosilcih ter vključno z vsemi kopijami, za katere odgovorna oseba tako določi. Tudi po morebitnem uničenju zaupnih informacij mora oseba, ki se je z informacijami seznanila, še vedno varovati njihovo zaupnost, skladno s tem pravilnikom.

Interni koordinator za varstvo podatkov zagotovi, da se z obveznostmi varovanja zaupnih podatkov seznanijo vse osebe pod neposrednim vodstvom upravljavca, ki do takih podatkov dostopajo oziroma imajo do njih pravico dostopa, ter da se z zunanjimi osebami, ki dostopajo oziroma imajo pravico dostopa do zaupnih podatkov sklenejo ustrezni dogovori o varovanju zaupnosti informacij.

8 Prehodne in končne določbe

32. člen

(Končna določba)

Ta pravilnik začne veljati naslednji dan po podpisu zastopnika upravljavca, a ne kasneje kot **v roku 90 dni od pristopa h Kodeksu ravnanj iVIZ**.

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov, z dne 27.9.2011.

Spremembe in dopolnitve tega pravilnika se izvajajo v okviru dopolnitev Kodeksa ravnanj iVIZ. Tudi spremembe in dopolnitve pravilnika mora pred uveljavitvijo potrditi zastopnik upravljavca.

Ravnatelj : dr. Robert Kerštajn

Podpis: _____

Datum: 1.7.2020