

Na podlagi 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 (Splošna uredba o varstvu podatkov), Zakona o varstvu osebnih podatkov (ZVOP-2) in Sklepa o ustanovitvi javnega vzgojno-izobraževalnega zavoda »Šolski center Šentjur« se sprejme

PRAVILNIK O VAROVANJU OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se ureja uresničevanje človekove pravice do varstva osebnih podatkov, obveznosti, načela, upravičenja, postopke in ukrepe, s katerimi se zagotavlja ustavna skladnost, zakonitost in upravičenost posegov v zasebnost, dostojanstvo, tajnost osebnih podatkov ter druga vprašanja obdelave in varstva osebnih podatkov, ki jih obdeluje Šolski center Šentjur (v nadaljevanju zavod).

Zaposleni delavci, ki pri svojem delu obdelujejo osebne podatke, morajo biti seznanjeni z vsebino tega pravilnika.

V zadevah, ki jih ne ureja ta pravilnik, se neposredno uporabljajo določbe Splošne uredbe o varstvu podatkov in Zakona o varstvu osebnih podatkov.

2. člen

V tem pravilniku:

»osebni podatek« pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki);

»posameznik« pomeni določeno ali določljivo fizično osebo, na katero se nanaša osebni podatek; oseba je določljiva, če jo 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, ekonomsko, kulturno ali družbeno identiteto tega posameznika;

»obdelava osebnih podatkov« pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali z 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;

»nadzorni organ« je Informacijski pooblaščenec, določen z zakonom, ki ureja Informacijskega pooblaščenca;

»javni sektor« so državni organi, samoupravne lokalne skupnosti, nosilci javnih pooblastil v delu, kjer izvršujejo javna pooblastila, javne agencije, javni skladi, javni zavodi, univerze, samostojni visokošolski zavodi, zasebni vrtci in zasebne osnovne ter srednje šole, ki izvajajo javno veljavne vzgojno-

izobraževalne programe, samoupravne narodne skupnosti, Svet romske skupnosti Republike Slovenije in druge osebe javnega prava, ustanovljene z zakonom;

»zbirka« pomeni vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili;

»posebna vrsta osebnih podatkov« pomeni osebne podatke, ki razkrivajo rasno ali etično 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 podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;

»uporabnik« pomeni fizično ali pravno osebo, javni organ ali agencijo ali drugo telo, ko so mu bili osebni podatki razkriti;

»privolitev posameznika na katerega se nanašajo osebni podatki« pomeni vsako prostovoljno izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj;

»kršitev varstva osebnih podatkov« pomeni kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje izgubo, spremembo, nepooblaščenno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kak drugače obdelani;

»tretja država« pomeni državo, ki ni članica Evropske unije ali del Evropskega gospodarskega prostora;

»nosilec podatkov« pomeni vsak dokument, na katerem je zapisan osebni podatek in vsak drug računalniški ali elektronski nosilec podatka;

»zaposleni delavec ali delavec« pomeni osebo, ki ima z zavodom sklenjeno pogodbo o zaposlitvi ali opravlja delo na podlagi podjemne ali druge pogodbe, so zaposleni na drugem zavodu in dopolnjujejo svoje delo, opravljajo študentsko delo ali delo zaradi izobraževanja oziroma so na drug način vključeni v delovni proces;

Izrazi, katerih pomen v tem pravilniku ni opredeljen, imajo pomen kot je določen v Splošni uredbi o varstvu osebnih podatkov oziroma Zakonu o varstvu osebnih podatkov.

3. člen

Obdelava osebnih podatkov je prepovedana, če se izvaja na način ali ima za posledico nedopustno diskriminacijo glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, invalidnost, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje, genske predispozicije ali katero koli drugo osebno okoliščino posameznice in posameznika.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

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

5. člen

Zavod za zagotavljanje varnosti ljudi in premoženja ter reda v njenih prostorih ali prostorih, ki jih ima v uporabi (v nadaljnjem besedilu: službeni prostori), od posameznika, ki namerava vstopiti v prostor, zahteva navedbo osebnih podatkov iz drugega odstavka tega člena.

V zbirki o vstopih in izstopih iz službenih prostorov se lahko o posamezniku obdelujejo naslednji osebni podatki: ime in priimek, obiskana oseba (razlog obiska) in času prihoda/odhoda.

Osebni podatki iz prejšnjega odstavka se lahko hranijo največ dve leti od konca koledarskega leta po vnosu osebnih podatkov v zbirko, nato se izbrišejo ali na drug način uničijo, če drug zakon ne določa drugače.

Evidenco vstopov in izstopov vodi oseba, ki jo pooblasti direktor.

Dostop v varovane prostore je mogoč in dopusten le v delovnem času, izven tega časa pa samo na podlagi dovoljenja direktorja.

6. člen

Varovani prostori so zlasti, ne pa izključno: pisarna direktorja in ravnatelja, tajništvo in prostori računovodstva.

Dokumentacija, ki vsebuje zbirke osebnih podatkov, se hrani tako, da je onemogočen dostop nepooblaščenim osebam. Izven delovnega časa morajo biti klasični nosilci osebnih podatkov (npr. listine, kartoteke, register, seznam, itd) shranjeni v zaklenjenih omarah v varovanih prostorih. Računalniki ali druga strojna oprema, na kateri se obdelujejo osebni podatki, mora biti izven delovnega časa izklopljena in fizično in/ali programsko zaklenjena.

7. člen

V varovane prostore nezaposlene osebe ali delavci brez ustreznih pooblastil ne smejo vstopati brez spremstva ali prisotnosti delavca z ustreznimi pooblastili (za obdelavo osebnih podatkov, ki se nahajajo v varovanem prostoru). Delavec mora vestno in skrbno nadzorovati prostor in ga ob zapustitvi zakleniti. Ključi se ne smejo puščati v ključavnici v vratih. Delavci so dolžni vestno hraniti ključe zaklenjenih varovanih prostorov.

Delavec, ki pri svojem delu obdeluje osebne podatke, ne sme med delovnim časom puščati nosilcev podatkov na vidnem mestu ali jih kako drugače izpostavljati nevarnosti vpogleda nepooblaščenim osebam.

V prostorih, kjer se zadržujejo obiskovalci, morajo biti nosilci osebnih podatkov in računalniški prikazovalniki nameščeni tako, da nepooblaščenim osebam nimajo možnosti dostopa oziroma vpogleda vanje.

8. člen

Tehnično-vzdrževalno osebje in čistilke se lahko zunaj delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

9. člen

Obdelovanje osebnih podatkov je dovoljeno le v prostorih zavoda, izven prostorov zavoda pa samo na podlagi dovoljenja direktorja.

Nosilcev osebnih podatkov brez dovoljenja ni dovoljeno iznašati izven prostorov zavoda, če za to ni ustrezne podlage v zakonskih ali notranjih predpisih oziroma pogodbenih razmerjih. Za iznos prenosnih računalnikov, mobilnih telefonov in drugih prenosnih informacijsko-komunikacijskih naprav in sredstev se za ustrezno podlago v notranjih predpisih šteje dokumentacija o predaji opreme v uporabo.

10. člen

S štampiljkami, žigom, papirjem z logotipom zavoda in drugimi pripomočki, s katerimi bi bilo mogoče ponarediti dokumente, se mora ravnati enako kot z osebnimi podatki.

11. člen

Dostop do računalniške programske opreme mora biti varovan na način, da dovoljuje dostop samo določenim vnaprej pooblaščenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

12. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi izrecne odobritve direktorja, izvajajo pa ga lahko samo pooblaščenih uslužbenci zavoda, pravne ali fizične osebe, ki imajo z zavodom sklenjeno ustrezno pogodbo. Izvajalci morajo spremembe in dopolnitve systemske in aplikativne programske opreme ustrezno dokumentirati.

13. člen

Delavec, pooblaščen za obdelavo osebnih podatkov na računalniku, mora skrbeti, da se pri servisiranju, popravilu, spreminjanju ali dopolnjevanju systemske ali aplikativne programske opreme ob morebitnem kopiranju osebnih podatkov po prenehanju potrebe po kopiji, kopija uniči.

Delavec, pooblaščen za obdelavo osebnih podatkov na računalniku, mora biti ves čas servisiranja računalnika in programske opreme prisoten in mora nadzirati, da ni nedopustnega ravnanja z osebnimi podatki. Ob izkazani potrebi po popravilu računalnika, na katerega disku so osebni podatki, zunaj zavoda in brez nadzora pooblaščenega zaposlenega, se morajo podatki z diska računalnika izbrisati tako, da je onemogočena obnova. Če tak izbris ni mogoč, se mora popravilo opraviti v poslovnih prostorih zavoda v prisotnosti pooblaščenega delavca.

14. člen

Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se sprotno preverja z antivirusnimi programi na prisotnost računalniških virusov.

Ob pojavu računalniškega virusa je potrebno storiti vse, da se s pomočjo strokovnjakov virus odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem sistemu.

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

15. člen

Zavod za obdelovanje podatkov uporablja le sistemsko in aplikativno programsko opremo, ki jo odobri direktor.

Delavci ne smejo nepooblaščenoma namestiti nobene programske opreme na računalnike ali na druge informacijsko-komunikacijske naprave.

Delavci ne smejo nepooblaščenoma odnašati programske opreme zavoda, prav tako te opreme ne smejo nepooblaščenoma posredovati tretjim osebam.

16. člen

Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel in pooblastil uporabnikom.

Direktor določi režim dodeljevanja, hranjenja in spreminjanja gesel oziroma določijo ustrezno osebo, ki po pooblastilu opravlja dodeljevanje, hranjenje in spreminjanje gesel.

17. člen

Za potrebe obnove osebnih podatkov v primeru izrednih dogodkov je potrebno redno izdelovati ustrezne kopije.

18. člen

Zavod vodi dnevnik obdelave, kadar gre za redno in sistematično spremljanje posameznikov, ali kadar je z oceno učinka, ki je določena z naslednjim členom Pravilnika, ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave, ali če tako določa zakon, o naslednjih dejanjih obdelave osebnih podatkov: 1. zbiranje; 2. spreminjanje; 3. vpogled; 4. razkritje, vključno s prenosi; 5. izbris; 6. druga dejanja obdelave, ki jih določa zakon.

Dnevnik obdelave iz prejšnjega odstavka mora za dejanja obdelave iz prejšnjega odstavka vsebovati vrsto dejanja obdelave, datum in čas obdelave, identifikacijo osebe, ki je izvedla dejanje obdelave, ter identifikacijo uporabnikov osebnih podatkov, da je mogoče naknadno ugotoviti točno identiteto teh oseb. Dodatne vsebine dnevnika obdelave lahko določi zavod ob upoštevanju ocene učinka.

Dnevnik obdelave se uporablja le za izkazovanje zakonitosti obdelave ter izvajanje notranjega nadzora, izvajanje nadzorov ali drugih zakonsko določenih preverjanj s strani nadzornega organa ali drugih pristojnih organov, zagotavljanje celovitosti in varnosti osebnih podatkov ter za odpravljanje napak v delovanju informacijskega sistema ali obdelavi podatkov.

Vsebina dnevnika obdelave se hrani dve leti od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave, če drug zakon ne določa drugače. Kadar je z oceno učinka ali analizo upoštevni tveganj ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati s podaljšanjem roka hrambe, se sme dnevnik obdelave hraniti največ pet let od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave.

Z zasnovo programske opreme se zagotavlja možnost naknadnega ugotavljanja kdo in kdaj je obdeloval posamezne osebne podatke tudi za primere, ko ni potrebno voditi dnevnika obdelave iz gornjih odstavkov tega člena.

19. člen

Kadar je možno, da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov, zavod pred obdelavo opravi oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov.

20. člen

Delavci, ki so zadolženi za sprejem in evidenco pošte, morajo izročiti poštno pošiljko z osebnimi podatki neposredno posamezniku ali službi, na katero je ta pošiljka naslovljena.

Delavci, ki so zadolženi za sprejem in evidenco pošte, odpirajo in pregledujejo vse poštno pošiljke in pošiljke, ki na drug način prispejo v zavod - prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavci, ki so zadolženi za sprejem in evidenco pošte, ne odpirajo tistih pošiljk, ki so naslovljene na drugo podjetje in so pomotoma dostavljene ter pošiljk, ki so označene kot osebni podatki ali za katere iz označbe na ovojnici izhaja, da se nanašajo na natečaj ali razpis.

Delavci, ki so zadolženi za sprejem in evidenco pošte, ne smejo odpirati pošiljk, naslovljenih na zaposlenega, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku ter pošiljk, na katerih je najprej navedeno osebno ime zaposlenega brez označbe njegovega uradnega položaja in šele nato naslov zavoda.

21. člen

Osebnne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo prilaščanje in uničevanje podatkov ter neupravičeno seznanjanje z njihovo vsebino.

Osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica 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.

Prenos osebnih podatkov po elektronski pošti mora biti zavarovan z gesli za identifikacijo.

III. ZAKONITOST OBDELAVE OSEBNIH PODATKOV

22. člen

Obdelava osebnih podatkov je zakonita le in kolikor je izpolnjen vsaj eden od naslednjih pogojev:

- (a) posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
- (b) obdelava je potrebna za izvajanje pogodbe, katere pogodbeni stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe;
- (c) obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za zavod;
- (d) obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe;
- (e) obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene zavodu;
- (f) obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva zavod, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki.

Obdelava osebnih podatkov je zaradi izvajanja zakonske obveznosti, javnega interesa ali izvajanja javne oblasti v primerih iz točk c) in e) prvega odstavka zakonita le, če obdelavo osebnih podatkov, vrste osebnih podatkov, ki naj se obdelujejo, kategorije posameznikov, na katere se ti osebni podatki nanašajo, namen njihove obdelave in rok hrambe osebnih podatkov ali rok za redni pregled potrebe po hrambi določa zakon.

V skladu s prvim odstavkom tega člena se lahko obdelujejo osebni podatki posameznika, ki je dal privolitev za obdelavo svojih osebnih podatkov za enega ali več določenih namenov, če tako možnost določa zakon, sicer pa na podlagi privolitve, če ne gre za izvrševanje zakonskih pristojnosti, nalog ali oblastnih obveznosti.

Za izvrševanje točke e) prvega odstavka tega člena se lahko izjemoma obdelujejo tisti osebni podatki, ki so nujno potrebni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo.

23. člen

Osebni podatki se obdelujejo zakonito in pošteno in morajo biti točni in ažurni, pri obdelavi pa mora zavod upoštevati načelo sorazmernosti, po katerem morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene za katere se zbirajo in nadalje obdelujejo.

24. člen

Zavod za vsako zbirko podatkov vzpostavi evidenco dejavnosti obdelave osebnih podatkov, ki vsebuje: podatke o upravljavcu osebnih podatkov, podatke o pooblaščenih osebah za varstvo osebnih podatkov, naziv zbirke, namen obdelave osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki v zbirki, vrste osebnih podatkov v zbirki, kategorije uporabnikov osebnih podatkov, ki so jim bili ali jim bodo razkriti osebni podatki, informacije o prenosih osebnih podatkov v tretjo državo ali mednarodno organizacijo, rok hrambe, splošen opis zavarovanja osebnih podatkov in pravna podlaga za obdelavo osebnih podatkov.

Evidenca dejavnosti obdelave se za vsako zbirko osebnih podatkov zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov. Evidenca dejavnosti osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

Zavod za zbirke podatkov vzpostavi seznam evidenc dejavnosti obdelave.

25. člen

Kadar zavod obdeluje osebne podatke na podlagi soglasja, mora pisno soglasje vsebovati:

- jasno opredeljeno voljo za izdajo soglasja,
- navedbo podatkov, ki se zbirajo,
- opredeljen namen zbiranja podatkov,
- zagotovilo, da se bodo podatki uporabljali le za namen, za katerega so zbrani,
- čas shranjevanja podatkov,
- pravice posameznika,
- datum podpisa izjave in
- podpis osebe.

Posameznik na katerega se nanašajo osebni podatki, lahko kadarkoli prekliče soglasje za obdelavo osebnih podatkov. Preklic soglasja ne vpliva na zakonitost obdelave na podlagi soglasja pred njenim preklicem.

IV. PRAVICE POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

26. člen

Kadar se osebni podatki v zvezi s posameznikom, na katerega se nanašajo osebni podatki, pridobijo od tega posameznika, zavod zadevnemu posamezniku takrat, ko pridobi osebne podatke, zagotovi vse naslednje informacije:

- (a) identiteto in kontaktne podatke zavoda in njegovega predstavnika;
- (b) kontaktne podatke pooblaščenih oseb za varstvo podatkov;
- (c) namene, za katere se osebni podatki obdelujejo, kakor tudi pravno podlago za njihovo obdelavo;
- (d) kadar obdelava temelji na zakonitih interesih, zakonite interese, za uveljavljanje katerih si prizadeva upravljavec ali tretja oseba;
- (e) uporabnike ali kategorije uporabnikov osebnih podatkov;
- (f) kadar je ustrezno, dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo.

Poleg informacij iz prvega odstavka zavod takrat, ko pridobi osebne podatke posamezniku, na katerega se ti nanašajo, zagotovi naslednje dodatne informacije, ki so potrebne za zagotovitev poštene in pregledne obdelave:

- (a) obdobje hrambe osebnih podatkov ali, kadar to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- (b) obstoj pravice, da se od upravljavca zahtevajo dostop do osebnih podatkov in popravek ali izbris osebnih podatkov ali omejitve obdelave v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora obdelavi in pravice do prenosljivosti podatkov;
- (c) kadar obdelava temelji na soglasju, obstoj pravice, da se lahko privolitev kadar koli prekliče, ne da bi to vplivalo na zakonitost obdelave podatkov, ki se je na podlagi privolitve izvajala do njenega preklica;
- (d) pravico do vložitve pritožbe pri nadzornem organu;
- (e) ali je zagotovitev osebnih podatkov statutarna ali pogodbeno obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo, in
- (f) obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov in smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

27. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov in naslednje informacije:

- (a) namene obdelave;
- (b) vrste zadevnih osebnih podatkov;
- (c) uporabnike ali kategorije uporabnika, ki so jim bili ali jim bodo razkriti osebni podatki, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;
- (d) kadar je mogoče, predvideno obdobje hrambe osebnih podatkov ali, če to ni mogoče, merila, ki se uporabijo za določitev tega obdobja;
- (e) obstoj pravice, da se zahteva popravek ali izbris osebnih podatkov ali omejitve obdelave osebnih podatkov v zvezi s posameznikom, na katerega se nanašajo osebni podatki, ali obstoj pravice do ugovora taki obdelavi;
- (f) pravico do vložitve pritožbe pri nadzornem organu;

(g) kadar osebni podatki niso zbrani pri posamezniku, na katerega se ti nanašajo, vse razpoložljive informacije v zvezi z njihovim virom;

(h) obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

Kadar se osebni podatki prenesejo v tretjo državo ali mednarodno organizacijo, ima posameznik, na katerega se nanašajo osebni podatki, pravico biti obveščen o ustreznih zaščitnih ukrepih.

28. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da zavod brez nepotrebne odlašanja popravi netočne osebne podatke v zvezi z njim. Posameznik, na katerega se nanašajo osebni podatki, ima ob upoštevanju namenov obdelave, pravico do dopolnitve nepopolnih osebnih podatkov, vključno s predložitvijo dopolnilne izjave.

Uslužbenec, ki obdeluje osebne podatke, lahko pred vnosom v zbirko osebnih podatkov preveri točnost osebnih podatkov z vpogledom v osebni dokument ali drugo ustrezno javno listino.

29. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da zavod brez nepotrebne odlašanja izbriše osebne podatke v zvezi z njim, zavod pa ima obveznost osebne podatke brez nepotrebne odlašanja izbrisati, kadar velja eden od naslednjih razlogov:

- (a) osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- (b) posameznik, na katerega se nanašajo osebni podatki, prekliče privolitev, na podlagi katere poteka obdelava, in kadar za obdelavo ne obstaja nobena druga pravna podlaga;
- (c) posameznik, na katerega se nanašajo osebni podatki, obdelavi ugovarja (za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi);
- (d) osebni podatki so bili obdelani nezakonito;
- (e) osebne podatke je treba izbrisati za izpolnitev pravne obveznosti v skladu s pravom Unije ali pravom države članice.

Kadar zavod objavi osebne podatke in je v skladu s prvim odstavkom osebne podatke obvezana izbrisati, ob upoštevanju razpoložljive tehnologije in stroškov izvajanja sprejme razumne ukrepe, vključno s tehničnimi, da upravljavce, ki obdelujejo osebne podatke, obvesti, da posameznik, na katerega se nanašajo osebni podatki, od njih zahteva, naj izbrišejo morebitne povezave do teh osebnih podatkov ali njihove kopije.

Gornja odstavka se ne uporabljata v primerih, določenih v Splošni uredbi o varstvu podatkov.

30. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da zavod omeji obdelavo, kadar velja en od naslednjih primerov:

- (a) posameznik, na katerega se nanašajo osebni podatki, oporeka točnosti podatkov, in sicer za obdobje, ki upravljavcu omogoča preveriti točnost osebnih podatkov;

(b) je obdelava nezakonita in posameznik, na katerega se nanašajo osebni podatki, nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitve njihove uporabe;

(c) upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;

(d) je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

Kadar je bila obdelava osebnih podatkov omejena v skladu s prvim odstavkom, se taki osebni podatki z izjemo njihovega shranjevanja obdelujejo le s privolitvijo posameznika, na katerega se ti nanašajo, ali za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov ali zaradi varstva pravic druge fizične ali pravne osebe ali zaradi pomembnega javnega interesa.

31. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico, da prejme osebne podatke v zvezi z njim, ki jih je posredoval zavodu, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga upravljavec, ki so mu bili osebni podatki zagotovljeni, pri tem oviral, kadar:

(a) obdelava temelji na privolitvi ali na pogodbi, in

(b) se obdelava izvaja z avtomatiziranimi sredstvi.

32. člen

Kadar zavod obravnava zahteve posameznika za uveljavljanje pravic iz gornjih členov in druge zahteve posameznika s področja varstva osebnih podatkov, dostopa do osebnih podatkov, njihovega pridobivanja in obdelave po tem ali drugem zakonu, posameznika seznaniti z odločitvijo in, če je to predmet zahteve, z osebnimi podatki, ki se nanašajo nanj, v roku 30 dni. Če posameznik to zahteva, ga lahko z osebnimi podatki seznaniti tudi ustno.

Odločitev mora vsebovati razloge in informacijo o pravici do pritožbe pri nadzornem organu.

Odločitev ima lahko obliko uradnega zaznamka, ki se pošlje posamezniku na način, ki omogoča seznanitev z odločitvijo in dokazovanje njenega prejema.

33. člen

Zavod (ali obdelovalec) od prejema zahteve za uveljavitev pravic ne sme izbrisati, odsvojiti ali spremeniti zahtevanih osebnih podatkov, ki so predmet postopka, dnevnikov obdelav in drugih povezanih informacij, ne glede na potek predpisanih ali interno določenih rokov hrambe, dokler o zadevi ni pravnomočno odločeno, po pravnomočnosti pa skladno s pravnomočno odločitvijo v zadevi.

34. člen

Zavod posreduje osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam, če je za posredovanje dana pravna podlaga ter na podlagi zahteve iz naslednjega odstavka,

razen če drug zakon določa drugače. Prejemnik podatkov sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se mu posredujejo, na kar se prejemnika izrecno opozori.

Če drug zakon ne določa drugače, zahteva za posredovanje osebnih podatkov vsebuje naslednje podatke:

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 pooblaščenice osebe;
2. pravno podlago za pridobitev zahtevanih osebnih podatkov;
3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za doseg 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.

Zavod vlagatelju zahteve, če drug zakon ne določa drugače, zahtevane osebne podatke posreduje najpozneje v 15. dneh od prejema popolne zahteve ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval. Če zavod ne ravna v skladu s prejšnjim odstavkom, se šteje, da je zahteva zavrnjena.

Zavod za vsako posredovanje osebnih podatkov zagotovi možnost poznejše ugotovitve, kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če drug zakon za posredovanje posameznih vrst podatkov določa drugače oziroma je to razvidno iz dnevnika obdelave.

Informacije iz prejšnjega odstavka zavod hrani dve leti, razen če drug zakon za posredovanje posameznih vrst podatkov določa drugačen rok.

35. člen

Za iznos osebnih podatkov v tretje države se neposredno uporabljajo določbe Splošne uredbe o varstvo podatkov.

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

36. člen

Zavod lahko posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa pogodbenemu obdelovalcu, ki je registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe za varovanje osebnih podatkov.

Pogodbeni obdelovalec sme opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru danih pooblastil zavodu in osebnih podatkov ne sme obdelovati za noben drug namen.

Medsebojne pravice in obveznosti se uredijo s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih za varovanje osebnih podatkov.

Pooblaščen osebni zavoda, ki je podpisala pogodbo o obdelavi osebnih podatkov, mora spremljati izvajanje postopkov in ukrepov za varovanje osebnih podatkov. V primeru spora med zavodom in pogodbenim obdelovalcem je dolžan pogodbeni obdelovalec osebne podatke, ki jih je pogodbeno obdeloval, na podlagi zahteve zavoda, nemudoma vrniti zavodu. Morebitne kopije teh podatkov mora takoj uničiti. V primeru prenehanja delovanja pogodbenega obdelovalca se osebni podatki in morebitne kopije teh podatkov brez nepotrebnega odlašanja vrnejo zavodu.

Pooblaščen pravna ali fizična oseba, ki za zavod opravlja dogovorjene storitve izven prostorov zavoda, mora imeti vsaj enako ustrezen način varovanja osebnih podatkov kakor ga predvideva ta pravilnik.

VI. BRISANJE PODATKOV

37. člen

Obdobje hrambe osebnih podatkov je odvisno od podlage in namena obdelave posamezne kategorije osebnih podatkov.

Po poteku roka hranjenja se osebni in drugi varovani podatki izbrišejo oz. uničijo nosilci podatkov.

38. člen

Brisanje podatkov na računalniških medijih se opravi na način, po postopku in metodi, ki onemogoča obnovo vseh ali dela brisanih podatkov.

Osebni podatki, vsebovani na klasičnih nosilcih (listine, kartoteke, registri, sezname...) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo/brišejo v prostorih zavoda. V tem primeru se uničevanje in brisanje osebnih podatkov opravi komisijsko. Komisija prisostvuje in protokolira vsak izbris in uničenje nosilcev osebnih podatkov z zapisnikom. Uničenje/brisanje nosilcev podatkov se lahko pogodbeno zaupa tudi organizaciji, ki se ukvarja z uničevanjem zaupne dokumentacije. V tem primeru uničenje in brisanje nadzoruje pooblaščen delavec, ki protokolira vsak izbris in uničenje nosilcev podatkov z zapisnikom.

Na enak način se uničuje pomožno gradivo (npr. matrice, grafikone, skice, poizkusne ali neuspešne izpise ipd.). Uničevanje pomožnega gradiva se mora izvajati tekoče in ažurno.

Ustrezno zavarovanje osebnih podatkov je potrebno zagotoviti tudi pri prenosu nosilcev osebnih podatkov na mesto uničenja.

39. člen

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

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

40. člen

Delavci so dolžni izvajati ukrepe za preprečevanje kršitve varstva osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik. Delavec, ki izve ali opazi, da je prišlo do kršitve varstva osebnih podatkov, mora takoj o tem obvestiti pooblaščenega osebo za varstvo osebnih podatkov ali direktorja.

Direktor mora zoper tistega, ki je kršil določbe varstva osebnih podatkov, ustrezno ukrepati.

41. člen

V primeru kršitve varstva osebnih podatkov zavod brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvesti pristojni nadzorni organ (Informacijski pooblaščenec), razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene pravice in svoboščine posameznikov. Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, se mu priloži navedbo razlogov za zamudo.

Obdelovalec po seznanitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja uradno obvesti zavod.

Uradno obvestilo vsebuje vsaj:

- opis vrste kršitve varstva osebnih podatkov
- sporočilo o imenu in kontaktnih podatkih pooblaščenega osebe za varstvo osebnih podatkov
- opis verjetnih posledic kršitve varstva osebnih podatkov
- opis ukrepov, ki jih zavod sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varstva osebnih podatkov, pa tudi ukrepov za blažitev morebitnih škodljivih učinkov kršitve, če je to ustrezno.

Zavod dokumentira vsako kršitev varstva osebnih podatkov.

VIII. VIDEONADZOR

42. člen

Odločitev o uvedbi videonadzora sprejme direktor. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora.

Zavod o odločitvi iz prejšnjega odstavka objavi obvestilo. Obvestilo se vidno in razločno objavi na način, ki omogoča posamezniku, da se seznaní z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove.

Obvestilo iz prejšnjega odstavka poleg informacij iz 26. člena predmetnega pravilnika vsebuje naslednje informacije:

1. pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;

2. namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov;
3. informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave;
4. kontaktne podatke pooblaščenih oseb (telefonska številka ali naslov e-pošte);
5. neobičajne nadaljnje obdelave, kot so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.

Namesto objave v obvestilu po tretjem odstavku tega člena se lahko obveščanje posameznika izvede tudi na način, da upravljavec informacije iz 26. člena in informacije iz 3. do 5. točke prejšnjega odstavka objavi na spletnih straneh. V tem primeru mora na obvestilu iz prejšnjega odstavka objaviti spletni naslov, kjer so te informacije dostopne.

Šteje se, da je z obvestilom posameznik obveščen o obdelavi osebnih podatkov.

Zbirka posnetkov videonadzornega sistema vsebuje posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma, če je to posebej nujno potrebno, pa tudi zvok.

Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan, kot to določata 24. in 32. člen Splošne uredbe.

Posnetki videonadzora se lahko hranijo največ eno leto od trenutka nastanka posnetka.

Vpogled, uporaba ali posredovanje posnetkov videonadzornega sistema so dopustni samo za namene, ki so zakonito obstajali ali bili navedeni na obvestilu v času zajema posnetka. Zavod za vsak vpogled ali uporabo posnetkov zagotovi možnost naknadnega ugotavljanja, kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi. Te podatke hrani v dnevniku obdelave dve leti po koncu leta, ko so nastali.

43. člen

Zavod lahko izvaja videonadzor dostopa v uradne službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa v te prostore ali izstopa iz njih ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih.

O izvajanju videonadzora in o vsebinah iz prejšnjega člena so pisno obveščeni vsi zaposleni, ki opravljajo delo v nadzorovanem prostoru.

Zbirka osebnih podatkov po tem členu lahko vsebuje poleg podatkov prejšnjega člena tudi datum in čas vstopa v uradni službeni prostor in izstopa iz njega, osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlog vstopa, če se navedeni osebni podatki zbirajo skupaj s posnetkom videonadzornega sistema.

IX. ODGOVORNOST ZA IZVAJANJE UKREPOV ZAVAROVANJA OSEBNIH PODATKOV

44. člen

Za neposredno izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov ter za nadzor nad tem, je odgovoren direktor, ki mora:

- poslovanje organizirati tako, da zagotovijo spoštovanje določb tega pravilnika in drugih predpisov o varstvu osebnih in drugih varovanih podatkov;
- seznaniti uslužbence z dolžnostjo varovati osebne podatke;
- v primeru dejavnosti, ki usmerjena v ogrožanje integritete osebnih podatkov, takoj ukreniti vse, da se tako ogrožanje onemogoči oziroma prepreči.

Direktor izda delavcu pooblastilo za obdelavo osebnih podatkov v zbirki ali zbirkah osebnih podatkov, s katerim določi obseg pooblastila in vrsto zbirke ali zbirk, za obdelavo katere ali katerih je delavec pooblaščen.

45. člen

Vsak, ki obdeluje osebne podatke, je dolžan izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je izvedel oziroma je bil z njimi seznanjen pri opravljanju svojega dela.

Pred nastopom dela delavca na delovnem mestu, kjer se obdelujejo osebni podatki ali nosilci osebnih podatkov, mora delavec podpisati izjavo, ki ga zavezuje k varovanju osebnih podatkov kot poklicne skrivnosti in ki ga opozarja na posledice kršitve zaveze. Obveza varovanja osebnih podatkov, s katerimi se delavec seznanja pri svojem delu, traja tudi po prenehanju delovnega razmerja.

46. člen

Ravnanja uslužbencev, ki so v nasprotju z določili tega pravilnika, pomenijo neizpolnjevanje pogodbenih oziroma drugih obveznosti iz delovnega razmerja, pogodbeni obdelovalci pa za kršitve odgovarjajo na temelju pogodbenih obveznosti.

Vsako postopanje delavcev v nasprotju z določbami predmetnega Pravilnika predstavlja hujšo kršitev delovne dolžnosti.

Odgovornost iz prejšnjega odstavka ne izključuje kazenske in odškodninske odgovornosti.

47. člen

Zavod določi pooblaščen osebo za varstvo osebnih podatkov.

Naloga pooblaščen osebe za varstvo osebnih podatkov so:

- obveščanje ter svetovanje o obveznostih v zvezi z varstvom osebnih podatkov;

- spremljanje skladnosti obdelave osebnih podatkov s predpisi, vključno z nalogami osveščanja in usposabljanja zaposlenih, ki so vključeni v postopke obdelave osebnih podatkov in s tem povezanih rednih pregledov;
- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom osebnih podatkov in spremljanje njenega izvajanja;
- sodelovanje z nacionalnim nadzornim organom za varstvo osebnih podatkov;
- kontaktna točka za nacionalni nadzorni organ;
- in druge naloge v skladu z določbami predpisov o varovanju osebnih podatkov.

IX. PREHODNE IN KONČNE DOLOČBE

48. člen

Ta pravilnik začne veljati in se uporablja osmi dan po dnevu sprejema.