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 (Splošna uredba o varstvu podatkov, v nadaljevanju: GDPR), in Zakona o varstvu osebnih podatkov (Uradni list RS štev. 163/22, v nadaljevanju: ZVOP-2) izdaja zastopnik ali predstojnik Zasebnega vrtca Bambi d.o.o., Rečica ob Paki 60a, 3327 Šmartno ob Paki, dne 27. 8. 2024

PRAVILNIK
o varstvu osebnih podatkov

1. člen

S tem pravilnikom se določajo organizacijski in tehnični postopki in ukrepi za zavarovanje osebnih podatkov z namenom, da se prepreči slučajno ali namerno nepooblaščeno uničevanje podatkov, njihovo spremembo ali izgubo kakor tudi nepooblaščen dostop, obdelavo, uporabo ali posredovanje osebnih podatkov.

Ukrepi iz prejšnjega odstavka se izvajajo z namenom, da:

- so osebni podatki obdelani zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo osebni podatki (načelo zakonitosti, pravičnosti in preglednosti);
- so osebni podatki zbrani za določene, izrecne in zakonite namene, in se ne obdelujejo na način, ki ni združljiv s temi nameni (načelo omejitve namena) ;
- se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave; ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove obdelave, obdobje njihove hrambe in njihovo dostopnost (načelo najmanjšega obsega podatkov in načelo omejitve shranjevanja);
- se spoštujejo in zaščitijo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki;
- da so obdelovani osebni podatki točni oziroma ustrezno posodobljeni (načelo točnosti);
- se zagotovi varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi (načelo celovitosti in zaupnosti) ;
- lahko obdelovalec dokaže skladnost z zakonodajo s področja varstva osebnih podatkov.

Upravljavec osebnih podatkov je z doslednim izvajanjem ukrepov zmožen dokazati, da obdelava poteka v skladu z veljavnimi predpisi s področja varstva osebnih podatkov, da je skladen z vsemi načeli obdelave osebnih podatkov iz 5. člena Splošne uredbe o varstvu podatkov, vključno tudi, da zagotavlja zaupnost, celovitost, razpoložljivost in točnost osebnih podatkov.

2. člen

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

V tem pravilniku uporabljeni pojmi imajo naslednji pomen:

1. »upravljavec« je zasebni vrtec/družba.

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

3. »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.

Pooblaščeno osebo za varstvo podatkov (t.i. DPO oz. PVOP) s sklepom imenuje zastopnik upravljavca in o tem v 8-ih dneh od imenovanja obvesti nadzorni organ.

4. »Interni koordinator za varstvo podatkov« je pri upravljavcu zaposlena oseba, ki je seznanjena z aktivnostmi upravljanja in obdelave osebnih podatkov pri upravljavcu ter praviloma skrbi za implementacijo navodil v primeru, da je upravljavec imenoval zunanjo pooblaščeno osebo za varstvo podatkov.

5. »osebni podatki« so katerakoli 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. »posebne vrste osebni podatki« 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 privolitev njegovega zakonitega zastopnika ali skrbnika;

9. »omejitev obdelave« je označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

10. »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;

11. »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;

12. »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;

13. »nadzorni organ« je Informacijski pooblaščenec Republike Slovenije, Dunajska cesta 22, 1000 Ljubljana, Slovenija;

14. »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 ter internetni pregledovalec, ki je del operacijskega sistema);

15. »aplikativna programska oprema« so programi ali z njimi povezane informacijske storitve, s katerimi se izvaja obdelava podatkov (npr. eAsistent, eDelovodnik, eVrtec, eGlasbenaŠola, programska oprema za eHrambo Logitus, finančno računovodski informacijski sistem, ipd..);

16. »zavezanci« po tem pravilniku so vsi zaposleni in drugi pogodbeni sodelavci upravljavca;

17. »obdelovalci« so lahko le tiste osebe, ki sklenejo z upravljavcem pogodbo o obdelavi skladno z 28. členom Splošne uredbe o varstvu podatkov.

18. »nosilec podatkov« pomeni vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki (listine, akti, gradiva, spisi, računalniška oprema, fotokopije, zvočno in slikovno gradivo, itd.).

19. »varnostni incident« pomeni 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.

3. člen

Družba, zaradi neobstoja pogojev iz petega odstavka 30. člena GDPR, ne vodi evidence dejavnosti obdelave osebnih podatkov.

4. člen

Družba pri sprejetju in izvajanju varnostnih ukrepov ter postopkov upošteva naravo osebnih podatkov in stopnjo tveganja, ki ga pomeni posamezna obdelava.

Pravno podlago za zbiranje in obdelavo osebnih podatkov predstavlja zakon ali osebna privolitev posameznika.

Če pravna podlaga za obdelavo ne obstaja, je potrebno osebne podatke takoj prenehati aktivno obdelovati in onemogočiti dostop do njih ter o neobstoju podlage obvestiti zastopnik ali predstojnikja družbe, ki določi nadaljnje ravnanje s takimi podatki.

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

Ukrepe za zagotovitev varnosti konkretnih zbirk osebnih podatkov, kot so med drugim psevdonimizacija in šifriranje, omejitev roka hrambe in dostopa, omejitev obdelave, omejitev namenov ipd., ter način izvedbe določi zastopnik ali predstojnik družbe.

Posebnih vrst osebnih podatkov družba ne obdeluje in jih ne hrani.

O pridobitvi in obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbami 12., 13. in 14. člena GDPR. Za izvedbo obvestil je pristojen vodja zasebnega vrtca oz. zastopnik ali predstojnik družbe.

Pooblaščeni obdelovavci morajo biti pred obdelavo osebnih podatkov seznanjeni z določbami ZVOP-2, GDPR ter z vsebino tega pravilnika, o čemer so dolžni podpisati posebno izjavo, Izjava o varstvu osebnih podatkov.

5. člen

Posameznik ima pravico od družbe dobiti potrditev, ali se obdelujejo njegovi osebni podatki, in če se, pravico dobiti dostop do osebnih podatkov (vpogled) in informacije iz 1. odstavka 15. člena GDPR.

Kadar obdelava temelji na privolitvi v obdelavo osebnih podatkov v enega ali več določenih namenov ima posameznik v skladu z določbami GDPR pravico, 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.

Posameznik ima pravico doseči, da družba brez nepotrebnega odlašanja popravi netočne oziroma dopolni nepopolne osebne podatke v zvezi z njim.

Posameznik ima pravico doseči, da družba brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, kadar velja eden od naslednjih razlogov:

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik prekliče privolitev, na podlagi katere poteka obdelava in za obdelavo ne obstaja nobena druga pravna podlaga;
- posameznik obdelavi ugovarja v skladu z določbami GDPR (21. člen), za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito;
- osebne podatke je treba izbrisati za izpolnitev pravne obveznosti zaradi izpolnitve zakonskih obveznosti;
- osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske družbe od mladoletnega posameznika.

Prejšnji odstavek tega člena se ne uporablja oziroma ne velja, če je obdelava potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov.

Posameznik ima pravico doseči, da družba omeji obdelavo, kadar velja en od naslednjih primerov:

- posameznik oporeka točnosti podatkov, in sicer za obdobje, ki družbi omogoča preveriti točnost osebnih podatkov;
- je obdelava nezakonita in posameznik nasprotuje izbrisu osebnih podatkov ter namesto tega zahteva omejitev njihove uporabe;
- družba osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;
- je posameznik vložil ugovor v zvezi z obdelavo, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

6. člen

Upravljavec obdeluje le tiste osebne podatke, za katere ima pravno podlago v eni od točk prvega odstavka 6. člena Splošne uredbe o varstvu podatkov oziroma 6. členu ZVOP-2 in le za namen, ki je določen z zakonom oziroma ga pred obdelavo določi upravljavec.

Upravljavec zbranih osebnih podatkov ne prenaša oziroma posreduje v tretje države.

Upravljavec obdeluje zbrane osebne podatke za namene izvajanja in izpolnjevanja svojih obveznosti iz pogodbenega razmerja in na podlagi izrecnega soglasja posameznika.

V okviru uveljavljanja pravic in izpolnjevanja pogodbenih obveznosti upravljavec obdeluje osebne podatke posameznikov za naslednje namene: identifikacija posameznika, sklenitev pogodbe, izvajanje storitve.

V primeru, da posameznik ne poda privolitve, jo poda delno ali privolitev (delno) prekliče, bo upravljavec osebne podatke obdeloval le v primerih in v obsegu dane privolitve, storitev pa izvedel le v primeru in v obsegu kot mu bo privolitev za obdelavo pridobljenih osebnih podatkov to omogočila.

Posameznik, na katerega se nanašajo osebni podatki, lahko svoje soglasje kadarkoli umakne oziroma spremeni na enak način, kot je bilo soglasje dano. Vsak posameznik lahko kadarkoli prekliče svojo privolitev oziroma ugovarja zbiranju in obdelavi svojih osebnih podatkov. Ko posameznik v delu ali v celoti prekliče svojo privolitev, upravljavec njegovih podatkov za namene, za katere je podan preklic, ne bo več uporabljal.

7. člen

Trajanje obdelave posameznih vrst osebnih podatkov je natančneje opredeljeno v 9. členu tega Pravilnika, zabeleženo je tudi v posamezni evidenci dejavnosti obdelave osebnih podatkov.

8. člen

Za vsako posredovanje osebnih podatkov mora vlagatelj (pravna ali fizična oseba), ki je do podatkov upravičen, predložiti pisno vlogo (lahko kot elektronsko sporočilo) v vsebini, kot jo določa 41. člen

ZVOP-2. Pisna vloga mora vsebovati:

- podatke o vlagatelju zahteve (za fizično osebo: osebno ime, naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika posameznika, posameznika, ki samostojno opravlja dejavnost, ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis vlagatelja oziroma pooblaščene osebe;

- pravno podlago za pridobitev zahtevanih osebnih podatkov;

- namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve;

- predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo;

- vrste osebnih podatkov, ki naj se mu posredujejo;

- obliko in način pridobitve zahtevanih osebnih podatkov.

Pred posredovanjem osebnih podatkov, se je upravljavec dolžan prepričati, da bo osebne podatke posredoval upravičeni osebi. V ta namen preveri identiteto vlagatelja zahteve, lahko tudi z vpogledom v uradni osebni dokument. Če je prosilec upravljavcu osebno znan, se o tem napravi uradni zaznamek.

Osebni podatki se vlagatelju zahteve posredujejo na naslov bivališča, ki ga je navedel v zahtevi, ali na elektronski naslov, s katerega je posredoval zahtevo.

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.

Upravljavec ne sme posredovati originalnih dokumentov, razen v primeru pisne odredbe sodišča oziroma, če tako zahtevajo veljavni predpisi, sicer vselej pošlje le kopijo, ki jo na željo vlagatelja zahteve lahko označi s pripisom, da je enaka originalu.

Upravljavec vodi in hrani evidenco o posredovanju osebnih podatki v papirni ali digitalni obliki. Evidenca vsebuje informacije o tem: 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.

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

Obveznost beleženja v evidenci posredovanj osebnih podatkov ne velja, kadar je upravljavec osebne podatke zakonito objavil na svojih spletnih straneh ali na drug ustrezen način, in kadar gre za osebne

podatke, za katere zakon določa, da so javni ali javno dostopni oziroma je obdelava dogovorjena s pogodbo.

9. člen

Osebni podatki se obdelujejo, dokler ni dosežen namen obdelave, potem se anonimizirajo ali izbrišejo. Če je rok hrambe določen z zakonom, se osebni podatki hranijo v tem času, sicer pa v odvisnosti od pravnega temelja za obdelavo.

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.

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.

10. člen

Izvajanje organizacijskih ukrepov za varnost osebnih podatkov so dolžni zagotoviti vsi zavezanci po tem pravilniku (zaposleni in drugi pogodbeni sodelavci, ki prihajajo v stik z osebnimi podatki) skladno z delovnim mestom oz. vlogo na katerem so zaposleni.

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

Dostop do programske opreme, s katero ali s pomočjo katere se obdelujejo osebni podatki, mora biti varovan na način, ki dovoljuje dostop samo za to vnaprej določenim zaposlenim in osebam, ki za družbo po pogodbi opravljajo servisiranje ali vzdrževanje strojne ali programske opreme, pri čemer si zaposleni med seboj ali s tretjimi osebami ne smejo izmenjevati ali razkrivati podatkov za dostop (ne glede na nivo pravic, ki jim je dodeljen).

Za dodeljevanje dostopa do programske opreme za zaposlene in vodenje evidence o tem je pristojen zastopnik ali predstojnik.

Popravljanje, spreminjanje in dopolnjevanje (posodabljanje) programske opreme oziroma sestava navodil v zvezi s tem so v pristojnosti zastopnik ali predstojnikja.

Zaposleni ne smejo brez odobritve zastopnik ali predstojnikja na strojno opremo in druge naprave, ki so v lasti ali uporabi družbe, namestiti nobene programske opreme. Zaposleni v družbi ne smejo odnašati programske opreme iz prostorov družbe brez vednosti zastopnik ali predstojnikja.

Popravljanje, spreminjanje in dopolnjevanje (posodabljanje) programske opreme s strani zunanjih izvajalcev je dovoljeno samo na podlagi odobritve zastopnik ali predstojnikja, izvajajo pa ga lahko samo pooblaščeni servisi in organizacije in posamezniki, ki imajo z družbo sklenjeno pogodbo, ki vključuje ustrezne določbe o pogodbeni obdelavi osebnih podatkov.

Vse spremembe in dopolnitve programske opreme, je potrebno dokumentirati na način, ki omogoča sledljivost sprememb ali dopolnitev.

Zaposleni, ki v okviru svojih delovnih nalog ustvari ali dovoli ustvariti kopijo (baze) osebnih podatkov za namene servisiranja, popravila, spreminjanja ali dopolnjevanja programske opreme ali za nudenje podpore, je dolžan poskrbeti, da se, ko preneha potreba, kopija učinkovito uniči ali izbriše.

Zastopnik ali predstojnik družbe podrobneje določi oziroma predpiše izdelavo kopij (baz) osebnih podatkov, tako da je mogoča restavracija osebnih podatkov v primeru neželenega izbrisa, spremembe ali uničenja osebnih podatkov ali nosilca, na katerem se nahajajo osebni podatki.

11. člen

Dostop do osebnih podatkov preko programske opreme mora biti varovan z enotnim in centraliziranim sistemom gesel ali drugih varnih sredstev za avtorizacijo in identifikacijo uporabnikov. Pri programski opremi mora biti spremljanje dogodkov v posamezni aplikaciji, ki omogoča možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil, in sicer za obdobje 5 let od zadnje obdelave osebnih podatkov.

Vsi računalniki oziroma programska oprema družbe so zavarovani z licencirano antivirusno opremo, ki onemogoča tudi nepooblaščene vdore v sistem in se samodejno posodablja v skladu z navodili proizvajalca omenjene opreme. Ob pojavu računalniškega virusa se tega čim prej odpravi, obenem pa se ugotovi vzrok pojava virusa v računalniškem informacijskem sistemu družbe. Vsak računalnik je dodatno zaščiten z osebnim varnostnim geslom, ki onemogoča odklepanje sistema nepooblaščenim uporabnikom. Vse zbirke osebnih podatkov, ki se vodijo v elektronski obliki, se varnostno shranjuje tudi na zunanjem trdem disku zaradi nevarnosti uničenja ali nepovratne onesposobitve trdega diska v računalniku, v katerem se nahaja.

Za določitev režima sistema oziroma načina dodeljevanja, hranjenja in spreminjanja gesel je pristojen zastopnik ali predstojnik družbe.

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervisorska gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hrani in varuje pred dostopom nepooblaščenih oseb. V primeru nepooblaščenega dostopa do teh podatkov se določi nova vsebina gesel.

12. člen

Osebni podatki se lahko zgolj izjemoma, kadar je to glede na naravo dela nujno potrebno, shranjujejo in obdelujejo lokalno (na lokalnih računalnikih in drugih podobnih napravah). Po prenehanju potrebe po takem shranjevanju in obdelavi osebnih podatkov, se morajo osebni podatki prenesti v centralizirane baze podatkov ali pa se trajno izbrisati.

Morebitne kopije vsebin zbirk osebnih podatkov na lokalnih nosilcih (zunanji diski, USB-ključi in drugo) se hranijo v zaklenjenih omarah.

Morebitne kopije vsebine mrežnega strežnika in lokalnih postaj za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se hranijo na za to določenih mestih, ki morajo biti ustrezno varovana ter zaklenjena.

13. člen

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

Organizacijski ukrepi:

- 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 pomenu varstva osebnih podatkov v pogodbe o zaposlitvi in druge pogodbe z delavci, ki so pod neposrednim vodstvom upravljavca,

- ozaveščanje vseh (zaposlenih in drugih pogodbenih sodelavcev) 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,

- izvajanje rednih obdobnih (predvidoma letnih, lahko pa tudi pogostejših) pregledov nad ravnanjem oz. obdelavo osebnih podatkov (notranje kontrole),

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 brezpogojne periodične menjave gesel v informacijskih sistemih

- preprečevanje možnosti skupinske prijave v informacijske sisteme,

- uporaba osebnih kvalificiranih digitalnih potrdil za elektronsko podpisovanje ter dostopa do eHrambe

- sprotno ažuriranje pooblastil odgovornih oseb v informacijskih sistemih skladno z dejanskim stanjem in organizacijskimi spremembami

- uporaba zgolj elektronske pošte, ki jo dodeli upravljavec,

- zagotavljanje varnosti pri dostopu do spleta,

- zagotavljanje uredništva spletne stran z uporabno namenskih gesel in izvajanjem namenske varnostne kopijo za obnovo na drugi lokaciji

- vzpostaviti požarno pregrado ter dvojno avtentikacijo (za administratorske dostope), če le mogoče.

14. člen

Pooblaščene osebe za obdelavo osebnih podatkov so odgovorne za zakonito obdelavo ter varstvo in varnost 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 oziroma dela zanj, in sicer časovno neomejeno.

Pooblaščene osebe oz. delovna mesta se vpiše v Katalog pooblastil v odvisnosti od presoje upravljavca pri čemer se pri poimenskem vpisu pooblaščenih oseb praviloma navede:

- naziv delovnega mesta ali ime in priimek posamezne pooblaščene osebe za obdelavo osebnih podatkov,

- datum podelitve, spremembe in ukinitve pooblastila (v kolikor le-ta ni razvidna iz revizijske sledi posameznega informacijskega sistema oz. ni sklenjena pogodba o zaposlitvi oz. pogodba o poslovnem sodelovanju iz katere je mogoče razbrati pričetek in zaključek pooblastila povezanega z razporeditvijo na delovno mesto ali opravljanjem dogovorjenih del)

- navedba vrst OP (npr. dokumentacija o vzgojno izobraževalnem procesu), za katere so pooblaščeni zaposleni,

- raven dostopa do osebnih podatkov znotraj posameznega informacijskega sistema, kadar je to relevantno (opcijsko).

Vse pooblaščene osebe, ki dostopajo do osebnih podatkov pri upravljavcu podpišejo izjavo o varstvu osebnih podatkov .

15. člen

Osebni podatki se lahko shranjujejo le toliko časa, kolikor določa zakon ali za čas, ki je potreben za izpolnitev pogodbe, vključno z jamčevalnimi in zastaralnimi roki (običajno znašajo ti 5 let), ali za čas, za katerega je posameznik privolil v obdelavo svojih osebnih podatkov. Rok hrambe za konkretne (baze) osebnih podatkov določi zastopnik ali predstojnik družbe.

Po prenehanju potrebe po vodenju osebnih podatkov se osebni podatki učinkovito izbrišejo, uničijo ali anonimizirajo, razen če zakon ali drug akt določa drugače. Uničenje, izbris ali anonimizacijo osebnih podatkov odredi zastopnik ali predstojnik. O uničenju, izbrisu ali anonimizaciji osebnih podatkov se napravi zapisnik, ki ne sme vsebovati osebnih podatkov posameznikov, katerih podatki so se izbrisali, uničili ali anonimizirali.

Za brisanje podatkov z računalnikov, strežnikov in podobnih naprav oziroma nosilcev osebnih podatkov v elektronski obliki se uporabi takšna metoda brisanja, da je nemogoča rekonstrukcija brisanih podatkov.

Podatki na fizičnih nosilcih, ki jih ni mogoče izbrisati, se uničijo na način, ki zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv. Točen način uničenja za posamezne tipe osebnih podatkov ali nosilcev določi zastopnik ali predstojnik družbe.

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

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa, zlasti tako, da je onemogočena razpoznavnost ali obnovitev osebnih podatkov.

16. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov (obdelovalec), se sklene pisna pogodba, predvidena v 28. členu GDPR. Družba s takšnim obdelovalcem sklene pogodbo zgolj ob zagotovilu, da ima implementirane vse ustrezne ukrepe za varstvo osebnih podatkov in izpolnjuje svoje dolžnosti, kot jih določa ZVOP-2 in GDPR ter ta pravilnik.

V pogodbi, sklenjeni v skladu s prvim odstavkom tega člena, morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Pred sklenitvijo pogodbe z obdelovalcem je zakoniti zastopnik družbe dolžan od upravljalca pridobiti podatke, ki omogočajo preveritev, ali obdelovalec izpolnjuje zahteve zakonodaje s področja varstva osebnih podatkov; to vključuje tudi razkritje vseh podpogodbenih obdelovalcev, vključno z njihovimi nazivi in sedeži.

Že zgolj možnost dostopa do podatkov, četudi na izrecno zahtevo družbe (npr. v okviru servisnega posega na strojni opremi ipd.), se šteje za pogodbeno obdelavo v smislu 1. odstavka tega člena.

Obdelovalci smejo opravljati storitve obdelave osebnih podatkov samo v okviru pooblastil, podeljenih v pogodbi, in v okviru drugih ustrezno dokumentiranih navodil družbe in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen, k čemur se jih zaveže s pogodbo.

Obdelovalec mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

Poleg drugih zahtev si mora družba v pogodbah z obdelovalci zagotoviti pravico, da najmanj enkrat letno pri pogodbenem obdelovalcu izvede pregled ali revizijo na področju varstva osebnih podatkov. Pregled ali revizijo je potrebno izvesti ob vsakem sumu ali indicu, da obdelovalec krši sklenjeno pogodbo ali da ne zagotavlja zadostne ravni varstva osebnih podatkov. Revizija se izvede na stroške družbe, pri čemer obdelovalec morebitnega angažmaja svojih ljudi in/ali podpogodbenih obdelovalcev družbi ne sme zaračunati.

17. člen

Upravljavec določi in imenuje pooblaščeno osebo za varstvo podatkov skladno z določbami ZVOP-2. O imenovanju pooblaščene osebe za varstvo podatkov se obvestijo tudi zaposleni, ki se lahko za posvetovanje obračajo neposredno nanjo.

18. člen

Upravljavec mora redno izvajati interne presoje skladnosti izvajanja dejavnosti obdelave osebnih

podatkov z veljavnimi predpisi. Presoje skladnosti se izvajajo praviloma enkrat letno.

19. člen

Delavec lahko za namene opravljanja dela poleg službene opreme in naprav v lasti upravljavca uporablja svoj zasebni računalnik in/ali mobilni telefon in druge tehnične naprave, če takšno uporabo odobri zastopnik oz. predstojnik ali od njega pooblaščena oseba, ki preveri uporabo z vidika varnosti za obdelavo osebnih podatkov upravljavca.

V primeru prenehanja delovnega razmerja je delavec dolžan s zasebnih računalnikov in/ali mobilnih telefonov ali drugih naprav (tudi USB ključev ipd.), ki jih je v soglasju z delodajalcem uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni s službenega omrežja, in vse datoteke, ki jih je zaposleni uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

Ob prenehanju delovnega razmerja delodajalec delavcu v podpis praviloma ponudi izjavo, da je s službenega računalnika, drugih tehničnih naprav in iz predala elektronske pošte izbrisal vsebine, ki so bile zasebne narave (kot na primer fotografije), in je naprava primerna za čiščenje podatkov z nje« oziroma za predajo v uporabo drugemu uporabniku opreme.

Delavec s podpisom izjave potrdi, da z vidika varstva osebnih podatkov in varstva zasebnosti širše ni zadržkov glede dostopanja delodajalca ali z njegove strani pooblaščenega pogodbenega sodelavca do delovnih sredstev, vključno s predalom e-pošte, ki jih je do tedaj uporabljal sam. Kolikor ima zadržke, se delavcu omogoči, da ob prisotnosti pooblaščenega delavca z delovnih sredstev prenese zasebne vsebine na zunanji nosilec in jih na delovnem sredstvu izbriše. Vzorec izjave je bil pripravljen sočasno s tem pravilnikom.

20. člen

Nosilci osebnih podatkov so vsak računalniški ali elektronski nosilec podatkov, vsak dokument (v papirni ali elektronski obliki), na katerem je zapisan osebni podatek, in strojna ter programska oprema. Varovani morajo biti z organizacijskimi ukrepi, določenimi s tem pravilnikom, 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 uporabniki 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 (na največ 180 sekund).

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 zastopnika oz. predstojnika ustanove. Slednji, po potrebi s posvetovanjem s 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.

21. člen

Za dostop do pisarne je potrebno imeti ključe pisarne. Ključe in dostopne kode dodeli zastopnik upravljavca. Dvojnike ključev pisarne je delavcem prepovedano izdelovati, razen v kolikor to ni izrecno naročeno delavcu s strani zastopnika oz. predstojnika.

Ključev se ne sme puščati v ključavnici v vratih z zunanje ali notranje strani.

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.

22. člen

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 v zvezi z računalniško opremo in temu primerno računalnike tudi uporabljati.

Upravljavec zagotavlja, 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.

Pooblaščena oseba 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.

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 kršitev varstva osebnih podatkov, ter kršitev obveznosti iz pogodbe o zaposlitvi. Lahko predstavlja tudi razlog za odškodninske zahteve, pa tudi naznanitev pristojnim organom za kazenski pregon.

VIDEONADZOR (opcijsko, se uporabi in prilagodi samo v kolikor se videonadzor izvaja)

23. člen

Videonadzor je namenjen varnosti ljudi ali premoženja in zagotavljanju nadzora vstopa v te prostore ali izstopa iz njih. Odločitev o videonadzoru je sprejel zastopnik upravljavca. Sledeč načelu minimalnega obsega osebnih podatkov, ki se obdelujejo, se video-nadzor izvaja pri vhodu v vrtec.

Obvestilo o izvajanju video-nadzora je nameščeno pred vstopom v področje videonadzora. Posamezniku je na ta način omogočeno, da se seznani z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove.

Obvestilo o izvajanju videonadzora mora poleg informacij iz 13. člena Splošne uredbe vsebovati 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 pooblaščene osebe (telefonska številka ali naslov e-pošte);

Namesto objave v obvestilu iz prejšnjega odstavka se lahko obveščanje o videonadzoru izvaja na način, da se informacije iz 13. člena Splošne uredbe in informacije iz 3. do 5. točke prejšnjega odstavka objavijo na spletnih straneh upravljavca. Na obvestilu iz o izvajanju videonadzora dostopa v poslovne prostore pa je objavljen spletni naslov, kjer so dostopne vse informacije.

Video-nadzorni sistem, s katerim se izvaja videonadzor, je zavarovan pred dostopom nepooblaščenih oseb. V kolikor se izvaja videonadzor s pomočjo računalniške opreme, ki je v rabi tudi za druge namene (npr. omrežni diski z možnostjo shranjevanja in upravljanja videonadzora) mora biti dostop do te opreme zaščiten s prijavnim imenom in geslom ter dvofaktorsko prijavo na drugem sredstvu (npr. telefon).

24. člen

Zbirka osebnih podatkov, ki nastaja samodejno na video-nadzornem sistemu, vsebuje posnetek posameznika: slika oziroma glas, če to kamera omogoča in beleži tudi datum in čas, ki je povezan z vstopom, premikanjem ali izstopom iz poslovnega prostora oz. področja v njem, kjer se videonadzor izvaja.

Posnetki se hranijo največ 60 dni od nastanka, potem se samodejno nepovratno uničijo.

O izvajanju videonadzora in o vsebinah iz obvestila o izvajanju videonadzora so pisno obveščeni vsi zaposleni ter vsi drugi z obvestilom na mestu vstopa v poslovni prostor. Vsi zaposleni se ob seznanitvi s tem pravilnikom še dodatno seznanijo z dejanskim obsegom izvajanjem videonadzora – vključno z informacijami iz 13. člena tega pravilnika.

V kolikor v ustanovi ne deluje reprezentativni sindikat, svet delavcev ali delavski zaupnik, posvetovanje po 78/VI členu ZVOP-2 ni potrebno izvesti.

25. člen

Video posnetki videonadzora pri upravljavcu se hranijo izključno na snemalni napravi. Dostop do posnetkov se avtomatizirano beleži v snemalni napravi (t.i. log datoteke, ki predstavljajo evidenco o videonadzoru) ter je omogočen samo pooblaščenim osebam za videonadzor.

Vzroki za vpogled v video posnetke videonadzora so lahko zahteva po zakonu upravičenega subjekta, odredba sodišča ali policije, varnostni incident (kot npr. vlom, kraja, alarmni dogodek, samodejno zaznano gibanje v službenih prostorih izven delovnega časa, ipd.) ter po nalogu zastopnika ustanove, kadar je izven v prejšnji alineji naštetih primerov podan sum, da je prizadeta z videonadzorom varovana dobrina.

Vsak dostop do posnetkov videonadzornega sistema se dokumentira s podatki:

- razlog za dostop,

- obseg dostopa,

- pooblaščena oseba, ki je dostop opravila (ime, priimek, delovno mesto, delodajalec),

- datum, kraj in čas dostopa,

- pooblaščena oseba, ki je posnetke prevzela (ime, priimek, delovno mesto, delodajalec), kraj in datum prevzema posnetkov,

- podatek o tem, kje se hranijo iz sistema eventualno izvzeti posnetki.

Evidenca dostopov ter evidenca posredovanja posnetkov tretjim osebam (po prilogah b in c tega pravilnika) ter log datoteka snemalne naprave, se hrani tri leta po opravljenem dostopu oz. posredovanju.

26. člen

Zaposleni so dolžni izvajati ukrepe za preprečevanje zlorabe 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.

Zaposleni so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti zastopnik ali predstojnikja družbe, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.

Zastopnik ali predstojnik družbe mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev sporočiti Informacijskemu pooblaščencu v 72 urah. Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora zastopnik ali predstojnik družbe poskrbeti za to, da so prizadeti posamezniki brez nepotrebnega odlašanja obveščeni o tem, da je prišlo do kršitve varstva osebnih podatkov. V primeru suma storitve kaznivega dejanja je potrebno varnostni incident prijaviti policiji ali tožilstvu.

27. člen

Zastopnik ali predstojnik družbe je dolžan poskrbeti za to, da se po varnostnem incidentu opravi analiza vzrokov in predlog ukrepov, ki naj zmanjšajo ali izničijo tveganje za take in bodoče varnostne incidente, ter da se, če je to smiselno in mogoče, predlagani ukrepi tudi izvedejo.

Če se izkaže, da je varnostni incident povzročil ali bil pri njem udeležen zaposleni ali je do varnostnega incidenta prišlo zaradi malomarnosti s strani zaposlenega, zastopnik ali predstojnik družbe, ne glede na ostale določbe tega pravilnika, sprejme ustrezne delovnopravne ukrepe zoper zaposlenega.

28. člen

Upravljavec mora posameznikom zagotoviti vse pravice, ki jih ima slednji po veljavnih predpisih kar opredeli v Informacijah za posameznike, ki so javno objavljene.

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 (ime, priimek, naslov bivališča, elektronski naslov ali drug podatek za komunikacijo),

- vsebino zahteve ali opravilno številko, pod katero se zadeva rešuje ter

- status reševanja zadeve,

- vrsta odločitve

- postopek s pravnimi sredstvi.

Posamezne zahteve iz naslova uresničevanja pravic posameznikov upravljavec hrani v papirni ali elektronski obliki.

29. člen

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 po določbah Zakona, ki ureja 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.

30. člen

Zavezanci so seznanjeni, da lahko ravnanje, ki ni skladno s tem pravilnikom, povzroči negativne posledice, kot so izguba zaupanja uporabnikov storitev ali dobaviteljev upravljavca, sodne, 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 (delovnopravni postopek redne odpovedi iz krivdnega razloga zaradi kršitve pogodbe o zaposlitvi, odškodninski postopek, predlog za kazenski pregon...).

31. člen

Ta pravilnik začne veljati naslednji dan po podpisu zastopnika upravljavca.

Taja Steblovnik, direktorica

Taja Steblovnik

Digitally signed by Taja Steblovnik
Date: 2024.08.27 11:31:26 +02'00'