Na podlagi določb 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), Zakona o varstvu osebnih podatkov (Uradni list RS, št.163/22; ZVOP-2) ter 8. alineje prvega odstavka 11. člena Sklepa o ustanovitvi javnega zavoda Filmski studio Viba film Ljubljana (Uradni list RS, št. 67/03, 96/11, 12/13, 53/13 in 59/13-popr.) sprejema vršilec dolžnosti direktorja javnega zavoda Filmski studio Viba film Ljubljana naslednji

PRAVILNIK
o varstvu osebnih podatkov na javnem zavodu Filmski studio Viba film Ljubljana

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi za varnost osebnih podatkov na javnem zavodu Filmski studio Viba film Ljubljana (v nadaljnjem besedilu: zavod) 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.

Odgovorna oseba zavoda, vodstvo, delavci oziroma vse osebe, ki so vključene v delovni proces zavoda na podlagi pogodbe o zaposlitvi ali drugega pogodbenega temelja, ki pri svojem delu na zavodu obdelujejo in/ali uporabljajo osebne podatke, morajo spoštovati določila veljavne zakonodaje, ki ureja področje varstva osebnih podatkov, ter vsebino tega pravilnika.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. Določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika.
2. Kršitev varstva osebnih podatkov 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. Nosilec podatkov pomeni vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in/ali slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.).
4. Obdelava pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje.
5. Obdelovalec pomeni fizično ali pravno osebo, javni organ, agencijo ali drug organ, ki obdeluje osebne podatke v imenu upravljavca;
6. Osebni podatki pomenijo katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki);
7. Podatki o zdravstvenem stanju pomenijo osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju.
8. Posebne vrste osebnih podatkov so osebni podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

9. 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 za obdelavo njegovih osebnih podatkov.
10. Tretja oseba pomeni fizično ali pravno osebo, javni organ, agencijo ali drug organ, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavca, obdelovalca in osebe, ki so pooblaščene za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca.
11. Uporabnik pomeni fizično ali pravno osebo, javni organ, agencijo ali drug organ, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Evropske Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave.
12. Upravljavec pomeni fizično ali pravno osebo, javni organ, agencijo ali drug organ, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Evropske Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice.

V tem pravilniku zapisani izrazi v moškem spolu se nanašajo enakovredno na ženski in moški spol.

II. OBDELAVA OSEBNIH PODATKOV

3. člen

Na zavodu se lahko obdeluje osebne podatke, če je izpolnjen vsaj eden od naslednjih pogojev:
- posameznik, na katerega se nanašajo osebni podatki, je privolil v obdelavo njegovih osebnih podatkov v enega ali več določenih namenov;
- obdelava je potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov za sklenitev pogodbe;
- obdelava je določena z zakonom in/ali je potrebna za izpolnitev zakonske ali na zakonu temelječe obveznosti, ki velja za upravljavca;
- obdelava je potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih fizičnih oseb;
- obdelava je potrebna za opravljanje nalog v javnem interesu ali pri izvajanju javnih pooblastil, dodeljenih upravljavcu;
- obdelava je potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, mladoletna oseba do 18. leta starosti.

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

Pri obdelavi posebnih vrst osebnih podatkov morajo biti pooblaščene osebe zavoda še posebej vestne in skrbne. Posebne vrste osebnih podatkov morajo biti varovane tako, da se nepooblaščenim osebam prepreči dostop do njih.

O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z določbo 13. in 14. člena Splošne uredbe, oziroma mu morajo biti predstavljene pravice iz 15. in naslednjih členov Splošne uredbe.

4. člen

Posameznik, na katerega se nanašajo osebni podatki, ima pravico od zavoda dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, mu zavod nudi dostop do osebnih podatkov in informacije iz prvega odstavka 15. člena Splošne uredbe ter zagotavlja naslednje pravice, v kolikor je to v skladu s Splošno uredbo:

– pravico do popravka;
– pravico do izbrisa („pravico do pozabe“);
– pravico do omejitve obdelave;
– obveznost obveščanja v zvezi s popravkom ali izbrisom osebnih podatkov ali omejitvijo obdelave;
– pravico do prenosljivosti podatkov;
– pravico do ugovora in avtomatizirano sprejemanje posameznih odločitev.

5. člen

Odgovorna oseba zavoda je dolžna poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami Splošne uredbe, obveščeni o pravicah. Prav tako odgovorna oseba zavoda poskrbi za kontaktno točko, na katero se lahko obrnejo in z zavodom komunicirajo posamezniki pri uveljavljanju svojih pravic.

Posamezniki lahko uveljavljajo naslednje pravice iz naslova varstva osebnih podatkov:

- Zahtevajo lahko informacije o tem, ali ima zavod osebne podatke o njih in, če je tako, katere podatke ima ter na kakšni podlagi jih ima in zakaj jih uporablja.
- Zahtevajo lahko dostop do svojih osebnih podatkov, kar jim omogoča, da prejmejo kopijo osebnih podatkov, ki jih ima zavod o njih, ter preverijo, ali jih zavod obdeluje zakonito.
- Zahtevajo lahko popravke osebnih podatkov, kot je popravek nepopolnih ali netočnih osebnih podatkov.
- Zahtevajo lahko izbris osebnih podatkov, kadar ni razloga za njihovo nadaljnjo obdelavo, oziroma kadar uveljavljajo svojo pravico do ugovora glede nadaljnje obdelave.
- Ugovarjajo lahko nadaljnji obdelavi osebnih podatkov, kjer se zanašajo na zakoniti poslovni interes (tudi v primeru zakonitega interesa tretje osebe), kadar obstajajo razlogi, povezani z njihovim posebnim položajem; ne glede na določilo prejšnjega stavka imajo posamezniki pravico kadar koli ugovarjati, če zavod obdeluje njihove osebne podatke za namene neposrednega trženja.
- Zahtevajo lahko omejitev obdelave osebnih podatkov, kar pomeni prekinitev obdelave njihovih osebnih podatkov, na primer če želijo, da zavod ugotovi njihovo točnost in/ali preveri razloge za njihovo nadaljnjo obdelavo.
- Zahtevajo lahko prenos osebnih podatkov v strukturirani elektronski obliki k drugemu upravljavcu, kadar in če je to mogoče in izvedljivo.
- Prekličejo lahko privolitev oziroma soglasje, ki so ga podali za zbiranje, obdelavo in prenos osebnih podatkov za določen namen; po prejemu obvestila, da so umaknili svojo privolitev, bo zavod prenehal obdelovati njihove osebne podatke, razen če ima zavod druge zakonite pravne podlage za to, da nadaljuje z obdelavo.

6. člen

V postopkih uveljavljanja pravic in zahtev, vključno z uveljavljanjem pravice do seznanitve z osebnimi podatki, ki se obdelujejo na zavodu, se uporabljajo določbe Splošne uredbe in zakona, ki ureja varstvo osebnih podatkov.

Posamezik uveljavlja pravice tako, da pošlje zahtevek po elektronski pošti na elektronski naslov zavoda ali z redno pošto na naslov zavoda. Zahtevek se lahko poda tudi ustno na zapisnik.

V primeru uveljavljanja pravic sme zavod od vlagatelja zahtevati določene informacije, ki mu bodo pomagale pri potrditvi vlagateljeve identitete, kar je le varnostni ukrep, ki zagotavlja, da se osebni podatki ne razkrijejo nepooblaščenim osebam.

Informacije, sporočila, odgovori in ukrepanja zavoda glede uveljavljanja pravic in zahtevkov s področja varstva osebnih podatkov, dostopa do osebnih podatkov, njihovega pridobivanja in obdelave se zagotavljajo brezplačno. Kadar so zahtevki posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljeni ali pretirani, zlasti ker se ponavljajo, lahko zavod kljub temu zahtevi ugodi, če je po vsebini utemeljena, in posamezniku zaračuna razumne stroške v skladu s predpisi. Če predpisi ne določajo višine stroškov, se šteje, da razumni stroški vključujejo dejanske materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja.

Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani v ovojnici, ki ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo vidna vsebina ovojnice. Ovojnica mora tudi zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

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

Posebne vrste osebnih podatkov se v fizični obliki pošilja naslovnikom v zaprtih ovojnicah proti podpisu z vročilnico. V primeru, da se posebne vrste osebnih podatkov pošilja v elektronski obliki, mora biti med prenosom zagotovljena njihova nečitljivost, tako da so šifrirani in zavarovani z geslom.

7. člen

Delavci, ki so zadolženi za sprejem in evidenco pošte na zavodu, odpirajo in pregledujejo vse poštne pošiljke in pošiljke naslovljene na zavod, ki na drug način prispejo na zavod (npr. prinesejo jih stranke ali kurirji), razen pošiljk iz drugega in tretjega odstavka tega člena.

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

Delavci, ki so zadolženi za sprejem in evidenco pošte, smejo odpirati pošiljke, ki so istočasno naslovljene na naslov zavod in delavca zavod, razen v primerih, ko je iz ovojnice razvidno, da je delavcu treba pismo vročiti osebno.

8. člen

Zavod mora voditi dnevnik obdelave osebnih podatkov v vseh z zakonom predpisanih primerih, kadar:
- se v avtomatiziranih sistemih obdelave osebnih podatkov izvajajo obsežne obdelave posebnih vrst osebnih podatkov,
- gre za redno in sistematično spremljanje posameznikov,
- je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave,
- tako določa zakon.

V primeru vodenja dnevnika obdelave osebnih podatkov se v dnevnik obdelave osebnih podatkov beležijo dejanja zbiranja, spreminjanja, vpogleda, razkritja (vključno s prenosi) in izbrisa osebnih podatkov, kot tudi druga dejanja obdelave, ki jih določa zakon. Vsebina dnevnika obdelave osebnih podatkov se hrani 2 leti od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave, razen če zakon določa drugače.

9. člen

Kadar je možno, da bi lahko načrtovana obdelava osebnih podatkov, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave osebnih podatkov, povzročila veliko tveganje za pravice in svoboščine posameznikov, se na to opozori vodstvo zavoda. V tem primeru se izvede ocena učinka v zvezi z varstvom podatkov, kot jo predvidena v 35. členu Splošne uredbe.

10. člen

Za namene dokumentiranja aktivnosti in obveščanja javnosti o delu in dogodkih na zavoda, kot so festivali, prireditve, razstave, projekcije, srečanja, izobraževanja in podobno, lahko zavod tak dogodek delno ali v celoti snema oziroma fotografira in izdelani avdio in/ali vizualni material objavi na spletnih straneh, v tiskovinah oziroma publikacijah in na družabnih omrežjih zavoda, razen v primeru zaprtih projekcij avtorskih del in izvedb, ki še niso bile premierno priobčene javnosti in imetnik materialnih pravic to izrecno prepove. Če namerava zavod izdelani avdio in/vizualni material uporabiti tudi kako

drugače, mora udeležence o tem predhodno ustrezno obvestiti in po potrebe pridobiti njihovo soglasje oziroma ustrezen prenos materialnih pravic na zavodu.

Obvestilo o tem, da bo dogodek sneman ali fotografiran, se zapiše na vabilo oziroma na obvestilo o dogodku. Navede se tudi namen snemanja ali fotografiranja. Na ta način se šteje, da so udeleženci in obiskovalci obveščeni o snemanju ali fotografiranju dogodka.

Kadar je to bolj primerno (ob dogodkih z manjšim številom udeleženih, dogodkih, ki niso odprti za javnost, udeleženci pa utemeljeno pričakujejo večjo stopnjo zasebnosti), se snemanje ali fotografiranje ustno napove in udeležencem pusti možnost, da izrazijo svojo voljo glede zajema njihove podobe s kamero.

11. člen

Odgovorna oseba zavoda lahko v utemeljenih primerih v skladu s Splošno uredbo in zakonom, ki ureja varstvo osebnih podatkov, pisno določi zunanji videonadzor ali, kadar je to še posebej utemeljeno in omogočeno na podlagi zakona, videonadzor dostopa v uradne službene oziroma poslovne prostore in videonadzor znotraj delovnih prostorov. O tem se objavi obvestilo, ki mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem in da se lahko vstopu v nadzorovano območje odpove. Namesto objave v obvestilu se lahko obveščanje izvede tudi z objavo zakonsko določenih informacij na spletnih straneh zavoda.

Video nadzorni sistem mora biti zavarovan pred dostopom nepooblaščenih oseb.

V primeru uvedbe videonadzora veljajo zanj vsi splošni organizacijski, tehnični in logično tehnični ukrepi za zavarovanje osebnih podatkov, pri čemer lahko odgovorna oseba zavoda določi tudi dodatne ukrepe, o čemer obvesti delavce. Vzpostavi se evidenca video nadzornega sistema, iz katere je mogoče pozneje ugotoviti, kdaj so bili posamezni osebni podatki iz evidence video nadzornega sistema uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je možno zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

12. člen

Zavod lahko za zagotavljanje varnosti ljudi in premoženja, varovanja tajnih podatkov ter reda v prostorih zavoda, od posameznika, ki namerava vstopiti ali izstopiti iz prostorov zavoda, zahteva navedbo naslednjih osebnih podatkov in razlog vstopa ali izstopa:
- osebno ime,
- številka in vrsta uradnega identifikacijskega dokumenta,
- datum in uro vstopa ali izstopa v prostore ali izstopa iz njih,
- razlog vstopa ali izstopa v prostore ali izstopa iz njih.

Po potrebi lahko zavod osebne podatke preveri tudi z vpogledom v uradni identifikacijski dokument.

III. POOBLAŠČENA OSEBA ZA VARSTVO PODATKOV

13. člen

Odgovorna oseba zavoda imenuje pooblaščeno osebo za varstvo podatkov s sklepom ali sklenitvijo pogodbe in poskrbi za objavo informacij o pooblaščeni osebi na spletni strani zavoda. Določi se lahko tudi namestnika pooblaščene osebe za varstvo osebnih podatkov, ki ga lahko pooblaščena oseba pooblasti, da opravlja s pooblastilom določene naloge pooblaščene osebe. Zavod poskrbi za ustrezni vpis kontaktnih podatkov pooblaščene osebe in njenega namestnika, ki jih tudi sporoči pristojnemu nadzornemu organu.

Pooblaščena oseba in morebitni namestnik pooblaščene osebe za varstvo podatkov se imenujeta na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi s področja varstva osebnih podatkov ter zmožnosti za izpolnjevanje nalog iz 39. člena Splošne uredbe in veljavne zakonodaje s področja varstva osebnih podatkov. Izpolnjevati morata pogoje, ki jih določa zakon, ki ureja varstvo osbenih podatkov.

Zavod zagotavlja, da sta pooblaščena oseba za varstvo podatkov in njen morebitni namestnik ustrezno in pravočasno vključena v vse zadeve v zvezi z varstvom osebnih podatkov, ter da so jima zagotovljena ustrezna sredstva, potrebna za kvalitetno opravljanje svojih nalog ter da jima je omogočen dostop do osebnih podatkov in dejanj obdelave.

Zavod zagotovi, da pooblaščena oseba za varstvo osebnih podatkov in njen morebitni namestnik pri opravljanju svojih nalog ne prejemata nobenih navodil. Ne smeta biti razrešena ali kaznovana zaradi opravljanja svojih nalog. Pooblaščena oseba za varstvo podatkov neposredno poroča odgovorni osebi zavoda, morebitni namestnik pa pooblaščeni osebi in odgovorni osebi zavoda.

14. člen

Posamezniki, na katere se nanašajo osebni podatki, lahko s pooblaščeno osebo za varstvo podatkov stopijo v stik glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov, in uresničevanjem njihovih pravic na podlagi Splošne uredbe in zakona, ki ureja varstvo osebnih podatkov.

Zavod preko pooblaščene osebe za varstvo osebnih podatkov redno obvešča delavce o pomenu in novostih s področja varstva osebnih podatkov in izvaja izobraževanja s tega področja ter področja informacijske varnosti.

15. člen

Pooblaščena oseba in namestnik sta pri opravljanju dela in po njegovem zaključku zavezana k varstvu tajnosti obdelovanih osebnih podatkov. Pridobljene informacije smeta uporabljati izključno za opravljanje nalog pooblaščene osebe.

16. člen

Pooblaščena oseba za varstvo podatkov ima vsaj naslednje naloge:

- obveščanje zavoda, njegovih pogodbenih obdelovalcev in pooblaščenih delavcev zavoda, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s Splošno uredbo in drugimi zakonskimi določbami o varstvu osebnih podatkov;
- spremljanje skladnosti organizacije s Splošno uredbo in nacionalnim pravom, vključno z dodeljevanjem nalog v zvezi z varstvom osebnih podatkov ter osveščanjem in usposabljanjem delavcev na zavodu, ki pri svojem delu obdelujejo osebne podatke;
- svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom osebnih podatkov in spremljanje izvajanja v skladu s členom 35. členom Splošne uredbe;
- sodelovanje z nadzornim organom in drugimi organi zavoda;
- delovanje kot kontaktna točka za nadzorni organ in druge organe zavoda pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz 36. člena Splošne uredbe;
- posvetovanje glede katere koli druge zadeve, ki se nanaša na osebne podatke.

Pooblaščena oseba za varstvo podatkov pri opravljanju svojih nalog upošteva tveganje, povezano z dejanji obdelave, ter naravo, obseg, okoliščine in namene obdelave.

IV. POGODBENA OBDELAVA OSEBNIH PODATKOV

17. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov na zavodu, se sklene pisna pogodba o opravljanju storitev ali aneks k pogodbi oziroma oseba poda in podpiše pisno izjavo, ki vsebuje tudi določila o predmetu obdelave (zlasti vsebino in trajanje obdelave, naravo in namen obdelave, vrste osebnih podatkov in kategorije posameznikov), pravicah in obveznostih pogodbenega obdelovalca in upravljavca ter postopke in ukrepe za zavarovanje osebnih podatkov skladno s Splošno uredbo in zakonom, ki ureja varstvo osebnih podatkov.

Obdelovalci so tudi zunanji sodelavci (pravne ali fizične osebe), ki imajo pri svojem delu dostop do osebnih podatkov, kot npr. sodelavci, ki opravljajo službo varovanja prostorov zavoda ali vzdržujejo strojno in programsko opremo ter izdelujejo in instalirajo novo strojno ali programsko opremo.

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

Pooblaščena pravna ali fizična oseba, ki za zavod opravlja dogovorjene storitve izven prostorov upravljavca (zavoda), mora imeti določene vse obvezne zahteve za zagotavljanja varnosti osebnih podatkov, kot jih sicer določa ta pravilnik.

V. BRISANJE PODATKOV

18. člen

Osebni podatki se lahko obdelujejo le toliko časa, kolikor je določen rok hrambe oziroma dokler obstaja pravna podlaga iz 6. člena Splošne uredbe in zakona, ki ureja varstvo osebnih podatkov. Po preteku roka hrambe se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt določa drugače.

Osebne podatke, ki jih zavod obdeluje na osnovi pogodbenega razmerja s posameznikom, zavod hrani za obdobje, ki je potrebno za izvršitev pogodbe in še 10 let po njenem prenehanju, razen v primerih, če zakon določa za tovrstno hrambo drugačen rok ali če pride med posameznikom in zavodom do spora v zvezi s pogodbo. V takem primeru hrani zavod podatke še 6 let po pravnomočnosti sodne odločbe, arbitraže ali poravnave ali mirne razrešrešitve spora.

Tiste osebne podatke, ki jih zavod obdeluje na podlagi osebne privolite posameznika ali zakonitega interesa, zavod hrani do preklica te privolitve oziroma do zahteve do izbrisa. Po prejemu preklica ali zahteve za izbris se podatki izbrišejo najkasneje v 15 dneh. Zavod lahko te podatke izbriše tudi pred preklicem, kadar je bil dosežen namen obdelave osebnih podatkov ali če tako določa zakon.

Izjemoma lahko zavod zavrne zahtevo za izbris iz naslednjih razlogov:
- uresničevanje pravice do svobode izražanja in obveščanja,
- izpolnjevanje pravne obveznosti obdelave,
- razlogi javnega interesa na področju javnega zdravja,
- nameni arhiviranja v javnem interesu,
- znanstveni ali zgodovinskoraziskovalni nameni ali statistični nameni,
- izvajanje ali obramba pravnih zahtevkov.

19. člen

Za brisanje podatkov iz nosilcev podatkov se uporabi takšna metoda brisanja, da restavracija vseh ali dela brisanih podatkov ni mogoča.

Podatki na klasičnih medijih (listine, kartoteke, register, seznam ipd.) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov. Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

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

Pri prenosu nosilcev osebnih podatkov na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prenos nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje posebna najmanj 3-članska komisija, ki jo s sklepom imenuje odgovorna oseba zavoda in ki o uničenju sestavi ustrezen zapisnik, oziroma se uničenje preda ustrezni zunanji službi na osnovi sklenjene pogodbe.

VI. INFORMACIJSKO VARNOSTNA POLITIKA

20. člen

Delavci zavoda uporabljajo različno informacijsko tehnologijo (kot npr. računalnik, telefon, čitalec osnovnih sredstev) ter različne elektronske storitve (kot npr. dostop do interneta, elektronska pošta, dostop do skupnega strežnika), ki jim jo dodeli zavod (delodajalec), izključno za službene namene.

V omejenem obsegu in razumnih mejah se s strani zavoda dodeljena informacijska tehnologija in elektronske storitve lahko uporabljajo tudi v zasebne namene ali jih lahko uporabljajo tudi pogodbeni sodelavci zavoda, če interni akti zavoda to omogočajo. Pri tem morajo delavci in sodelavci zavoda varovati ugled zavoda, tehnologije in storitev pa ne smejo uporabljati za neprimerne ali žaljive namene.

21. člen

Dostop do svetovnega spleta je omogočen delavcem in sodelavcem zavoda za njihovo delo, izobraževanje in informiranje.

Delavci in sodelavci zavoda morajo uporabljati svetovni splet v skladu z etičnimi in moralnimi normami. Vsi uporabniki informacijskih sistemov se morajo zavedati, da se v medmrežju izkazujejo z mrežnim naslovom organa javnega zavoda (IP naslov).

Posredovanje službenih elektronskih naslovov na zunanje spletne strežnike za namene prijave določene storitve (npr. seznam poštnih naslovov, prijava na izobraževanja ipd.) ni dovoljeno, razen če je povezano s poslovnim procesom zavoda.

V omrežju zavoda se lahko izdeluje statistika obiskanih spletnih strani, ki mora biti anonimizirana in ni za javno objavo. Statistika se lahko uporablja npr. za načrtovanje in varovanje informacijskega sistema, anketiranje, statistiko obiska spletnih stranbi itd. V ta namen lahko zavod uporablja analitične piškotke.

Odgovorna oseba zavoda lahko zaradi zagotavljanja informacijske varnosti in razpoložljivosti informacijskih virov ter zaradi preprečevanja kršitev odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede oseba, zadolžena za delovanje računalniškega informacijskega sistema zavoda, in sicer na podlagi pisne odredbe odgovorne osebe zavoda. O blokadi se obvesti vse delavce in sodelavce zavoda po elektronski pošti.

22. člen

Službena elektronska pošta se na zavodu lahko uporablja kot orodje za komunikacijo s posamezniki, strankami, delavci in zunanjimi izvajalci. Pri tem se morajo delavci zavoda držati ne le etičnih in moralnih norm, temveč tudi bontona. Pošiljatelj se mora zavedati, da se vsako sporočilo s službenega elektronskega naslova pri prejemniku lahko razloži kot mnenje zavoda, v katerem je pošiljatelj delavec zavoda.

Ni priporočljivo, da delavci svoje službeni elektronski naslov uporabljajo v zasebno – trženjske namene in z njega pošiljajo oglasno pošto na znane in/ali neznane naslove. Prav tako ni priporočljivo, da se delavci prijavljajo na oglasno pošto ali novice z elektronskimi naslovi zavoda, razen če je to povezano s potrebami delovnega mesta.

Delavci morajo biti previdni pri odpiranju elektronske pošte s priponkami neznanih pošiljateljev. Če sumijo, da gre za nezaželeno pošto, ki bi lahko bila škodljiva, je ne odpirajo, temveč o tem obvestijo pristojno osebo zavoda, zadolženo za delovanje računalniškega informacijskega sistema.

Delavci ne smejo pošiljati posebnih vrst osebnih podatkov ali gesel po elektronski pošti, razen v ustrezno akreditiranih sistemih, oziroma mora biti podatkom med prenosom zagotovljena njihova nečitljivost, tako da so zavarovani z geslom, ki ga podeli pooblaščena oseba zavoda.

Uporaba zasebne elektronske pošte (npr. Gmail, Yahoo, ipd.) za službene namene ni dovoljena, saj potencialno predstavlja neupravičeno obdelavo osebnih podatkov. Izjemoma, kadar to utemeljujejo posebne okoliščine, je na osnovi dovoljenja odgovorne osebe zavoda dovoljeno uporabljati zasebno elektronsko pošto.

Mobilnim telefonom, ki so v lasti zavoda in v uporabi posameznega delavca, se ne sme slediti in v ta namen se v te mobilne naprave ne sme namestiti naprav oziroma aplikacije za sledenje. Zavod lahko poskrbi za protivirusno zaščito službenih mobilnih telefonov.

23. člen

Oddaljeni dostop do informacijskega sistema zavoda je dovoljen le na podlagi odobrene metode z ustrezno ravnjo varnosti, in sicer le za tiste delavce zavoda, ki dostop potrebujejo zaradi opravljanja delovnih nalog, vendar v omejenem obsegu. Treba je upoštevati tudi načelo praznega zaslona. Po končanem delu se je treba obvezno odjaviti iz sistema in zagotoviti, da katerikoli podatki in sledi ne ostanejo na delovni postaji (»private mode«).

24. člen

Oseba, zadolžena za delovanje informacijskega sistema na zavodu, lahko na posebej utemeljeno pisno zahtevo pooblaščene osebe zavoda v prisotnosti tri članske komisije v izrednih primerih (nenadna odpoved delavca, smrt delavca, nepričakovane, nenadne in dalj časa trajajoče ali trajne odsotnosti delavca, odpoved delovnega razmerja s strani delavca brez odpovednega roka, odpoved delovnega razmerja iz krivdnih razlogov zaradi neopravičene odsotnosti in podobni izredni primeri) vpogleda v informacijsko tehnologijo (npr. v računalnik) ali druge elektronske storitve (npr. v elektronsko pošto) delavca le, če je to nujno potrebno za izpolnjevanje zakonskih obvez zavoda oziroma za vodenje delovnega procesa.

Vpogled opravi tri članska komisija, ki jo vsakokrat imenuje pooblaščena oseba zavoda. V njej mora biti vsaj en predstavnik delavcev, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik, ki vsebuje:
– obrazložitev razloga vpogleda,
– zapisnik o vstopu z morebitnimi pripombami delavca, če je ta navzoč,
– navedbe prisotnih oseb,
– seznam oziroma izpis pridobljenih podatkov.

Če se pojavi utemeljen sum, da delavci ne spoštujejo določil informacijsko varnostne politike tega pravilnika, lahko oseba, zadolžena za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo odgovorne osebe zavoda opravi nadzor uporabe elektronskih storitev, a zgolj z vidika pregleda dnevniških zapisov o količini prometa in shranjenih podatkov, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati vsebin.

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

O namenu uporabe informacijske tehnologije in elektronskih storitev iz tega člena ter možnosti vpogleda mora biti delavec pisno obveščen. Kot zadostno obvestilo se šteje obvestilo skupaj s temi pravili, poslano vsem delavcem po e-pošti.

25. člen

Ob prenehanju delavnega razmerja oziroma po izčrpanju temelja za opravljanje dela je delavec dolžan vrniti zavodu službeno informacijsko tehnologijo oziroma tehnologijo, ki jo je uporabljal v službene namene, pri čemer mora pred vrnitvijo delavec sam poskrbeti, da so iz uporabljane informacijske in elektronskih storitev očiščene oziroma izbrisane vse njegove zasebne vsebine, službene pa ohranjene v celoti.

26. člen

Delavec lahko za namene opravljanja dela poleg službene opreme uporablja svojo zasebno opremo in druge tehnične naprave (predvsem mobilni telefon), če takšno uporabo odobri odgovorna oseba zavoda in delavec poda prostovoljno pisno soglasje, da lahko zavod (delodajalec) za namene izvajanja delovnega procesa pri tem obdeluje njegovo zasebno telefonsko številko in/ali zasebni elektronski naslov.

V primeru prenehanja delovnega razmerja je delavec dolžan z zasebne opreme ali drugih naprav in njihovih nosilcev podatkov, ki jih je v soglasju z zavodom uporabljal za službene namene, izbrisati vse osebne podatke, ki so bili preneseni v okviru opravljanja delovnega procesa, in vse datoteke, ki jih je uporabljal v službene namene, ne glede na to, ali vsebujejo osebne podatke.

VII. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

27. člen

Prostori, v katerih se nahajajo nosilci osebnih, zaupnih in drugih občutljivih podatkov, kot tudi nosilci z občutljivimi podatki in zapisi kot so avtorske pravice in izvedbe, strojna in programska oprema (varovani prostori), morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki onemogočajo nepooblaščenim osebam dostop do podatkov.

Kot varovani prostor so opredeljeni prostori vodstva, upravnega oddelka, glavne pisarne (tajništva), strežniške sobe, prostori programerske in servisne službe, pisarne, kabineti in drugi prostori, v katere nepooblaščene osebe nimajo vstopa.

Dostop do varovanih prostorov je mogoč tudi izven rednega delovnega časa na podlagi del in nalog ali pooblastila.

Vsi ključi zavoda se uporabljajo in hranijo v skladu z internimi pravili zavoda, ki jih sprejme direktor. S posameznimi ključi lahko razpolagajo le za to posebej pooblaščeni delavci zavoda. Ključi se ne puščajo v ključavnici v vratih od zunanje strani.

Varovani prostori ne smejo ostajati nenadzorovani, oziroma se morajo zaklepati ob odsotnosti delavcev, ki jih nadzorujejo.

Delavci svojega delovnega mesta ne smejo pustiti nenadzorovanega, oziroma morajo poskrbeti, da so takrat originalne listine in nosilci osebnih, zaupnih ter drugih občutljivih podatkov shranjeni tako, da nepooblaščene osebe do njih nimajo dostopa. Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih, zaupnih in drugih občutljivih podatkov zaklenjene (politika čiste mize).

Računalniki in druga informacijska tehnologija oziroma oprema, ki omogoča dostop do osebnih, zaupnih in drugih občutljivih podatkov, morajo biti v času odsotnosti delavca bodisi izklopljeni bodisi fizično ali programsko zaklenjeni (politika čistega zaslona).

Delavci ne smejo puščati nosilcev osebnih, zaupnih in drugih občutljivih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci osebnih, zaupnih in drugih občutljivih podatkov, ki se morebiti nahajajo izven varovanih prostorov (npr. avla, hodniki, skupni prostori, sejna soba ipd.), morajo biti stalno zaklenjeni v omarah.

Posebne vrste osebnih podatkov se ne sme hraniti izven varovanih prostorov.

28. člen

V prostorih, ki so namenjeni poslovanju s strankami ali nimajo statusa varovanega prostora in je vanje dovoljen dostop nezaposlenim, morajo biti nosilci podatkov in računalniški zasloni nameščeni tako, da stranke nimajo neposrednega vpogleda vanje. V takih prostorih na oglasnih deskah ali kakorkoli

drugače ne smejo biti izpostavljeni taki podatki, na osnovi katerih bi se lahko nepooblaščene osebe seznanile z osebnimi, zaupnimi in drugimi občutljivimi podatki.

29. člen

Vzdrževanje in popravila informacijske tehnologije in elektronskih storitev ter druge opreme je dovoljeno samo z vednostjo odgovorne osebe zavoda, oziroma ga lahko izvajajo pooblaščeni servisi ali vzdrževalci, ki imajo z zavodom sklenjeno ustrezno pogodbo.

30. člen

Vzdrževalci prostorov, informacijske tehnologije oziroma strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih samo z vednostjo odgovorne ali pristojnein za to pooblaščene osebe zavoda. Delavci in drugi sodelujoči z zavodom, kot so čistilke, varnostniki ipd., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne, zaupne in druge občutljive 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).

VIII. VAROVANJE SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME

31. člen

Dostop do elektronskih storitev oziroma programske opreme zavoda mora biti varovan tako, da dovoljuje dostop samo za to vnaprej določenim delavcem na zavodu ali zunanjim sodelavcem – fizičnim ali pravnim osebam – ki v skladu s pogodbo opravljajo dogovorjene storitve.

32. člen

Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve odgovorne osebe zavoda, izvajajo pa ga lahko samo pooblaščeni servis ali vzdrževalec, ki ima z zavodom sklenjeno ustrezno pogodbo. Izvajalci morajo izvedene spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati. V primeru, da je potrebno za delo izdelati kopije, morajo biti le-te po prenehanju namena, s katerim so bile izdelane, ustrezno uničene. Enako velja za ostale izpise, izvoze podatkov ali druge pripomočke za izvedbo storitve servisiranja.

33. člen

Vsebine na nosilcih podatkov na mrežnih strežnikih in lokalnih delovnih postajah, kjer se nahajajo osebni, zaupni in drugi občutljivi podatki, se mora redno preverjati zaradi potencialne prisotnosti računalniških virusov in druge oblike zlonamerne kode. V primeru odkritja virusa, se ta odpravi s strani ustrezne strokovne službe oziroma pristojne osebe zavoda, zadolžene za delovanje računalniškega informacijskega sistema, obenem pa se skuša ugotovi tudi vzrok pojava virusa.

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

34. člen

Delavci ne smejo inštalirati programske opreme brez odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema zavoda. Prav tako ne smejo odnašati programske opreme iz zavoda brez odobritve odgovorne osebe zavoda ali vodje organizacijske enote in vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

35. člen

Dostop do podatkov in uporaba sistemske in aplikativno programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programske opreme in podatkov. Vsak uporabnik ima svoje geslo za dostopanje do posameznih elektronskih storitev. Posojanje gesel in uporaba skupinskih gesel je prepovedana.

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (supervizorska oziroma nadzorna gesla), administriranje elektronske pošte in administriranje aplikativnih programov, se hranijo na ustrezen način tako, da je dostop nepooblaščenih oseb onemogočen. Uporabi se jih samo v izrednih okoliščinah ali v nujnih primerih. Vsako uporabo teh gesel sme dovoliti odgovorna ali pooblaščena oseba zavoda. Po vsaki takšni uporabi se določi nova vsebina gesel.

36. člen

Za potrebe obnovitve računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se redno izdelujejo varnostne kopije podatkov. Na zavodu se izvaja avtomatsko obnavljanje računalniškega sistema. Najmanj enkrat letno se napravi redna obnovitev računalniškega sistema zavoda z izdelavo varnostne kopije podatkov, ki se hrani na internem strežniku zavoda.

Varnostne kopije podatkov se, če je le možno, hranijo zaklenjene v zavarovanih ognjevarnih omarah, zaščitene pred poplavami in elektromagnetnimi motnjami.

IX. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

37. člen

Delavci so dolžni o aktivnostih, ki so povezane z odkrivanjem, nepooblaščenim dostopom ali uničenjem podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju takoj obvestiti pooblaščeno osebo zavoda, sami pa poskušajo takšno aktivnost preprečiti.

Kršitev varstva osebnih, zaupnih in drugih občutljivih podatkov 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 obdelan. Kršitev je lahko storjena nehote (npr. iz malomarnosti) ali pa je načrtovana oziroma naklepna. Na splošno ta kršitev pomeni varnostni incident, ki ogroža zaupnost, celovitost in dostopnost osebnih podatkov.

Delavci so dolžni pri svojem delu spremljati in biti pozorni na morebitne varnostne incidente ter v skladu tem pravilnikom ustrezno ravnati.

38. člen

Če delavci, zunanji izvajalci ali zunanji sodelavci zavoda zasledijo, da se je na zavodu zgodil varnostni incident, morajo nujno o tem obvestiti pooblaščeno osebo zavoda, ta pa direktorja.

Vodstvo mora najprej izvedeti, kaj se je zgodilo, oceniti, kakšne so potencialne škodljive posledice za pravice in svoboščine posameznikov in na predlog pooblaščene osebe sprejeti ustrezne ukrepe za odpravo posledic ali vsaj zmanjšanje tveganj. Priporočljivo je, da se vodstvo za pripravo ocene verjetnosti in resnosti posledic za pravice in svoboščine posameznikov posvetuje s pooblaščeno osebo zavoda za varstvo podatkov.

V primeru, da vodstvo oceni, da bo zaradi incidenta nastalo tveganje za pravice in svoboščine posameznikov, mora o tem obvestiti Informacijskega pooblaščenca brez odlašanja, najkasneje pa v 72 urah po zaznani kršitvi. V primeru, da se je incident zgodil v zvezi s podatki, pri katerih je zavod v vlogi obdelovalca, mora o kršitvi obvestiti upravljavca v najkrajšem možnem času po zaznani kršitvi.

Za prijavo se uporabi obrazec, ki ga priporoča Informacijski pooblaščenec. Ob prijavi mora Informacijski pooblaščenec pridobiti vsaj naslednje informacije:

- opis vrste kršitve,
- kategorije in približno število posameznikov, na katere se nanašajo osebni podatki,
- vrste in približno število evidenc osebnih podatkov,
- kontaktne podatke pooblaščene osebe zavoda za varstvo podatkov,
- opis verjetnih posledic kršitve varstva osebnih podatkov,
- opis ukrepov, ki jih je upravljavec sprejel, ali pa predvidenih ukrepov za ublažitev tveganj za kršitve.

V vsakem primeru varnostnega incidenta se zabeležijo okoliščine oziroma podatki o varnostnem incidentu (datum varnostnega incidenta, vrsta osebnih podatkov, pri katerih je prišlo do varnostnega incidenta, način izvršitve, obvestilo pooblaščeni osebi za informatiko, kadar gre za tovrstni incident ipd.).

39. člen

Za obveščanje Informacijskega poblaščenca o kršitvah varstva osebnih podatkov po 33. členu Splošne uredbe in zakona, ki ureja varstvo osebnih podatkov, je odgovorna odgovorna oseba zavoda.

Določbe IX. poglavja tega pravilnika se smiselno uporabljajo tudi za zunanje izvajalce, ki imajo z zavodom podpisano pogodbo ali zanj opravljajo dogovorjene storitve, če pri svojem delu ali izvajanju storitev za zavod zaznajo nepooblaščen dostop ali uničenje podatkov, zlonamerno ali nepooblaščeno uporabo, prilaščanje, spreminjanje ali poškodovanje podatkov.

X. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

40. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi delavci na zavodu, kot tudi zunanji izvajalci, ki imajo z zavodom podpisano pogodbo ali zanj opravljajo dogovorjene storitve.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja pooblaščena oseba zavoda.

Odgovorna oseba zavoda s pisnim sklepom ali pisnim pooblastilom pooblasti posamezne delavce zavoda za dostop in obdelavo posameznih kategorij oziroma evidenc osebnih podatkov. V primeru vzpostavitve videonadzornega sistema se posebej določi in pooblasti osebo, ki je odgovorna za evidenco video nadzornega sistema, ter osebe, ki lahko zaradi narave njihovega dela obdelujejo podatke v evidenci video nadzornega sistema.

41. člen

Vsak delavec na zavodu in sodelujoči z zavodom, ki se pri svojem delu seznani in/ali obdeluje osebne podatke, je dolžen izvajati predpisane postopke in ukrepe za zavarovanje podatkov in varovati podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela ali izvajanju storitev. Obveza varovanja podatkov ne preneha s prenehanjem delovnega ali pogodbenega razmerja.

42. člen

V primeru kršitev določil tega pravilnika je delavec ali drugi sodelujoči z zavodom odškodninsko odgovoren zavodu za škodo, ki bi zaradi njegovega ravnanja ali opustitve nastala zavodu oziroma fizičnim ali pravnim osebam, s katerimi zavod sodeluje.

Kršitev določil pravilnika lahko predstavlja kršitev delovnih obveznosti po pogodbi o zaposlitvi ali bistveno kršitev druge pogodbe, iz česar lahko izhajajo posledice, ki so predpisane za tovrstne kršitve.

Kršitev določil pravilnika ima lahko za posledico tudi kazensko, prekrškovno in/ali odškodninsko odgovornost delavca oziroma osebe, ki ne spoštuje določil tega pravilnika.

XI. KONČNE DOLOČBE

43. člen

Ta pravilnik je sprejet z dnem podpisa direktorja zavoda, veljati pa začne naslednji dan po objavi.

Z dnem ko je sprejet ta pravilnik, preneha veljati obstoječi Pravilnik o varovanju osebnih podatkov na Filmskem studiu Viba film v Ljubljani z dne 19. 6. 2008 in Pravilnik o spremembah in dopolnitvah Pravilnika o varovanju osebnih podatkov na Filmskem studio Viba film v Ljubljani z dne 9. 3. 2018.

Vse spremembe in dopolnitve tega pravilnika se sprejmejo na enak način kot pravilnik.

Pravilnik se objavi na pri delodajalcu običajen način.

Pravilnik je na razpolago in vpogled delavcem v Glavni pisarni (tajništvu) delodajalca.

Priloga temu pravilniku in sestavni del tega pravilnika so vrste evidenc osebnih podatkov, ki se po posameznih zbirkah vodijo in obdelujejo na zavodu. V roku 1 meseca od sprejetja tega pravilnika se preverijo obstoječa oz. podelijo nova pooblastila za obdelavo in vpogled v posamezne zbirke osebnih podatkov.

Zavod sprejme interna pravila za uporabo in razpolaganje s ključi zavoda na podlagi četrtega odstavka 27. člena v roku 2 mesecev od sprejetja tega pravilnika.

Datum: 23. 12. 2024

Filmski studio Viba film Ljubljana

Mitja Bravhar
v. d. direktorja