

Na podlagi 24., 25. in 32. člena Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (v nadaljevanju: Uredba) ter določil Zakona o varstvu osebnih podatkov (v nadaljevanju: ZVOP-2) izdaja upravljavec osebnih podatkov KINOLOŠKA ZVEZA SLOVENIJE, ki ga zastopa predsednik Hari Arčon

## **POSLOVNA PRAVILA**

### **o postopkih in ukrepih za zavarovanje osebnih podatkov**

#### **I. SPLOŠNE DOLOČBE**

##### **1. člen**

##### **Vsebina in namen pravil**

S temi pravili se določajo tehnični, organizacijski in kadrovske postopki in ukrepi za zavarovanje osebnih podatkov v podjetju KINOLOŠKA ZVEZA SLOVENIJE (v nadaljevanju: upravljavec), z namenom zaščite pravic posameznikov, na katere se osebni podatki nanašajo. Pravila so pravno zavezujoča.

##### **2. člen**

##### **Pomen izrazov**

V teh pravilih uporabljeni izrazi imajo naslednji pomen:

1. Nosilec podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, knjige, računalniška oprema, vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofili, naprave za prenos podatkov ipd.).
2. Občutljivi osebni podatki - so podatki, ki jih Uredba v 9. členu opredeljuje kot posebno vrsto osebnih podatkov. To so podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.
3. Obdelava osebnih podatkov - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, psevdonimizacija, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave).
4. Osebni podatek - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen.
5. Posameznik - je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njegovo

fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov ali ne zahteva veliko časa.

6. Uporabnik osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki.

7. Upravljavec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki sama ali skupaj z drugimi določa namene in sredstva obdelave osebnih podatkov, oziroma oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave.

8. Obdelovalec osebnih podatkov - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki jo upravljavec zbirke osebnih podatkov pooblasti, da v njegovem imenu ali za njegove namene obdeluje osebne podatke, ki jih upravlja upravljavec.

9. Zbirka osebnih podatkov - je vsak strukturiran niz podatkov, ki vsebuje vsaj en osebni podatek, ki je dostopen na podlagi meril, ki omogočajo uporabo ali združevanje podatkov, ne glede na to, ali je niz centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi; strukturiran niz podatkov je niz podatkov, ki je organiziran na takšen način, da določi ali omogoči določljivost posameznika.

### 3. člen

#### Uporaba pravil

Ta pravila veljajo za zaposlene pri upravljavcu osebnih podatkov, za obdelovalce osebnih podatkov, ki jih upravljavec pooblasti za obdelavo osebnih podatkov pod njegovim upravljanjem, kakor tudi za osebe, ki pri upravljavcu osebnih podatkov opravljajo dela na podlagi pogodbe o delu, ter za dijake in študente, ki pri upravljavcu osebnih podatkov opravljajo dela preko napotnic oziroma so pri upravljavcu na praksi. Vsi navedeni uporabniki morajo upoštevati tveganja, ki so povezana s tehničnimi in informacijskimi sistemi in tehnologijo in morajo pri obdelavi osebnih podatkov ravnati z največjo mero skrbnosti.

## II. OBDELAVA OSEBNIH PODATKOV

### 4. člen

#### Vzpostavitev zbirke osebnih podatkov

(1) Posamezno zbirko osebnih podatkov vzpostavi odgovorna oseba za določeno zbirko osebnih podatkov (v nadaljevanju: odgovorna oseba).

(2) Odgovorne osebe iz prejšnjega odstavka so določene v seznamu, ki je sestavni del teh pravil.

### 5. člen

#### Obdelava osebnih podatkov

(1) V zbirki osebnih podatkov se lahko obdelujejo le tisti osebni podatki, ki imajo ustrezno zakonsko podlago po določbah Zakona in Uredbe.

(2) Osebni podatki se smejo zbirati samo za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če Zakon in Uredba ne določata drugače.

(3) Občutljivi osebni podatki se lahko obdelujejo le na podlagi Zakona in Uredbe. Pri obdelavi morajo biti ti podatki posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

(4) O obdelavi osebnih podatkov mora biti posameznik obveščen v skladu z Zakonom in Uredbo. Upravljavca ne sme pridobiti in uporabljati osebnih podatkov brez izrecne privolitve osebe, na katero se osebni podatki nanašajo. Slednja mora biti pred posredovanjem osebnih podatkov upravljavcu nedvoumno seznanjena z namenom obdelave njenih osebnih podatkov.

(5) Odgovorne osebe ter osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke (v nadaljevanju: pooblaščenih obdelovalci), morajo biti pred obdelavo osebnih podatkov seznanjene z določbami Zakona in Uredbe ter z vsebino teh pravil.

(6) O seznanjenosti iz prejšnjega odstavka morajo osebe iz prejšnjega odstavka podpisati posebno izjavo, iz katere je razvidno, da je podpisnik seznanjen s predpisi iz prejšnjega odstavka.

(7) Pooblaščenih obdelovalci iz petega odstavka tega člena so določeni v seznamu, ki je sestavni del tega pravilnika.

(8) Upravljavca se mora ravnati po priznanih pravilih za varnost informacij.

(9) Upravljavca se mora zavedati, da se zahteve za varstvo osebnih podatkov spreminjajo in prilagajajo tehnološkemu razvoju, zato mora ta pravila po potrebi ustrezno revidirati.

## 6. člen

### Posredovanje osebnih podatkov

(1) Osebni podatki se na zahtevo uporabnika posredujejo samo tistim uporabnikom, ki se izkažejo z ustrezno zakonsko podlago ali s pisno zahtevo oziroma privolitvijo posameznika, na katerega se podatki nanašajo.

(2) Posredovanje osebnih podatkov iz prejšnjega odstavka lahko uporabnik zahteva pisno ali ustno. Ob vložitvi pisne zahteve mora uporabnik jasno izkazati pravno podlago za pridobitev osebnih podatkov. Če uporabnik zahteva posredovanje osebnih podatkov ustno, sme odgovorna oseba ali pooblaščenih obdelovalec v primeru dvoma o obstoju pisne zahteve oziroma privolitve posameznika, na katerega se podatki nanašajo, od uporabnika zahtevati, naj jih predloži.

(3) Posredovanje občutljivih osebnih podatkov iz prvega odstavka tega člena lahko uporabnik zahteva le pisno. Pisna zahteva mora biti po vsebini enaka pisni zahtevi iz prejšnjega odstavka.

(4) Osebni podatki, ki se posredujejo uporabniku v fizični obliki, morajo biti posredovani s priporočeno pošto ali preko kurirja 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.

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

(6) Ne glede na prejšnji odstavek je občutljive osebne podatke dovoljeno posredovati preko komunikacijskih omrežij le, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

(7) Če se posreduje originalni dokument, ki vsebuje osebne podatke, mora biti v času odsotnosti nadomeščen s fizično (fotokopijo) ali elektronsko (skenirano) kopijo.

#### 7. člen Evidenca posredovanj

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

- kateri osebni podatki so bili posredovani,
- osebno ime/firmo/ime in naslov/sedež osebe, ki so ji bili posredovani osebni podatki,
- datum in ura posredovanja osebnih podatkov ter
- podlaga, na kateri so bili posredovani osebni podatki.

(2) Zaznamek iz prejšnjega odstavka se v pisni ali elektronski obliki, odvisno od nosilca podatkov, ki vsebuje posredovani osebni podatek, evidentira v zbirko osebnih podatkov, ki ji pripada posredovani osebni podatek, v posebno rubriko "evidenca posredovanj osebnih podatkov" v seznamu evidenc dejavnosti obdelave osebnih podatkov (10. člen teh pravil).

(3) Zaznamek iz prvega odstavka tega člena naredi odgovorna oseba ali pooblaščen obdelovalec, ki je osebne podatke posredoval uporabniku.

#### 8. člen Posredovanje osebnih podatkov znotraj upravljavca osebnih podatkov

(1) Dokumenti, ki vsebujejo osebne podatke zaposlenega pri upravljavcu osebnih podatkov, se zaposlenemu, na katerega se osebni podatki nanašajo, posredujejo v skladu s četrtem, petim in šestim odstavkom 6. člena teh pravil.

(2) Osebni podatki zaposlenih pri upravljavcu osebnih podatkov in ostalih oseb se lahko posredujejo znotraj upravljavca osebnih podatkov tistim osebam, ki jih potrebujejo v okviru opravljanja svojih del in nalog.

(3) Oseba iz tretjega odstavka prejšnjega člena mora zaznamovati vsako posredovanje občutljivih osebnih podatkov znotraj upravljavca osebnih podatkov v skladu s prejšnjim členom.

#### 9. člen Hramba osebnih podatkov

(1) Osebni podatki se lahko shranjujejo le toliko časa, kolikor je rok hrambe, razviden iz Evidence zbirk osebnih podatkov (10. člen pravil).

(2) Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če Zakon, Uredba ali drug predpis za posamezne vrste osebnih podatkov ne določajo drugače.

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

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

(5) Uničenje nosilcev podatkov in pomožnega gradiva se zagotovi v skladu tretjim in četrtem

odstavkom tega člena.

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

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

(8) Prenos nosilcev podatkov, ki vsebujejo občutljive osebne podatke, na mesto uničenja ter uničevanje takih nosilcev podatkov nadzoruje posebna tričlanska komisija, ki jo imenuje predsednik upravljavca osebnih podatkov. Komisija se posvetuje s pooblaščen osebo za varstvo osebnih podatkov, če jo je upravljavec imenoval.

(9) Komisijo iz prejšnjega odstavka sestavljajo zaposleni pri upravljavcu osebnih podatkov, en član komisije je odgovorna oseba.

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

## 10. člen

### Seznam evidenc dejavnosti obdelave osebnih podatkov

(1) Upravljavec je za namen identifikacije in popisa vseh vrst osebnih podatkov, ki jih obdeluje, dolžan voditi Evidenco zbirk osebnih podatkov (v nadaljevanju: evidenca zbirk), v katerem so zapisane vse zbirke osebnih podatkov, ki jih obdeluje, in omogoča popoln pregled nad tokom osebnih podatkov (revizijsko sled).

(2) Odgovorna oseba je dolžna skrbeti za točnost in ažurnost evidence zbirk. V ta namen mora evidenco zbirk dopolnjevati ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki osebnih podatkov.

(3) Evidenca zbirk osebnih podatkov mora za vsako evidenco dejavnosti obdelave osebnih podatkov vključevati naslednje informacije:

- katere vrste osebnih podatkov se obdelujejo;
- na katere kategorije posameznikov se osebni podatki nanašajo;
- kaj je namen obdelave osebnih podatkov;
- na kateri pravni podlagi se podatki obdelujejo;
- rok hrambe in uničenja podatkov;
- pravne ali fizične osebe, ki se jim podatki lahko razkrijejo;
- ali se podatki iznašajo v tretjo državo ali mednarodno organizacijo;
- tehnične, organizacijske in kadrovske ukrepe za zagotavljanje varnosti osebnih podatkov.

(4) Pooblaščeni obdelovalci morajo biti seznanjeni z evidenco zbirk osebnih podatkov.

## 11. člen

### Upravljanje tveganja

(1) Upravljavec ob upoštevanju narave, obsega, okoliščin in namena obdelave osebnih podatkov, razvidnih iz evidence zbirk, ugotovi, če za posamezno vrsto osebnih podatkov obstaja veliko tveganje za pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo.

(2) Če obstaja tveganje iz prejšnjega odstavka, mora upravljavec izdelati oceno tveganja za zbirko osebnih podatkov, na katero se tveganje nanaša.

(3) Upravljavec mora presoditi tveganje iz 1. odstavka tega člena ob vsaki spremembi tveganja, ki ga predstavlja obdelava osebnih podatkov, ob vzpostavitvi nove zbirke osebnih podatkov, pred uporabo novih tehnologij ali ko se spremenijo narava, obseg, okoliščine in namen obdelave osebnih podatkov.

## III. VAROVANJE PROSTOROV, NOSILCEV PODATKOV, STROJNE IN PROGRAMSKE OPREME

### 12. člen

#### Varovanje prostorov

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

(2) Varovani prostori, v katerih se nahajajo nosilci podatkov, ki vsebujejo občutljive osebne podatke, morajo biti varovani tako, da je zagotovljen popolni nadzor nad delom in gibanjem v teh prostorih. Prostor, morajo biti ognjevarni, zavarovani pred izlitjem vode, poplavami in elektromagnetnimi motnjami, v okviru predpisanih klimatskih pogojev.

(3) Pisarne morajo biti stalno pod nadzorom zaposlenih, ki v njih delajo. Ob odsotnosti mora zaposleni pisarno zakleniti. Ključi se ne smejo puščati v ključavnici v vratih.

(4) V varovanih prostorih morajo biti po zaključku delovnega časa oziroma po končanem delu izven delovnega časa omare in pisalne mize z nosilci podatkov, ki vsebujejo osebne podatke, zaklenjene, računalniki in druga strojna oprema pa izklopljeni in fizično ali programsko zaklenjeni.

(5) Omare, mize in drugo pohištvo z nosilci podatkov, ki vsebujejo osebne podatke, ki se nahajajo izven varovanih prostorov (hodniki, skupni prostori) mora biti stalno zaklenjeno.

(6) Osebe, ki niso zaposlene pri upravljavcu osebnih podatkov (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, poslovni partnerji) se smejo gibati v varovanih prostorih samo z vednostjo zaposlenega, ki nadzoruje varovani prostor, kjer se oseba giba.

(7) Zaposleni, kot so čistilke, varnostniki idr., se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema so izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

### 13. člen

#### Varovanje nosilcev podatkov, ki vsebujejo osebne podatke

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

(2) Nosilci podatkov, ki vsebujejo občutljive osebne podatke, se ne smejo hraniti izven varovanih prostorov.

(3) Nosilce podatkov, ki vsebujejo osebne podatke, lahko zaposleni pri upravljavcu osebnih podatkov odnašajo izven prostorov upravljavca osebnih podatkov samo z dovoljenjem, ki ga da Šinko Štefan, Zastopnik.

(4) Nosilcev podatkov, ki vsebujejo občutljive osebne podatke, zaposleni pri upravljavcu osebnih podatkov ne smejo odnašati izven prostorov upravljavca osebnih podatkov, razen izjemoma z dovoljenjem, ki ga da Šinko Štefan, Zastopnik, če je to nujno potrebno za reševanje zadeve, ki vsebuje te občutljive osebne podatke.

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

(6) Zaposleni, ki je zadolžen za sprejemanje in evidentiranje pošte:

(a) mora izročiti poštno pošiljko z osebniimi podatki neposredno posamezniku ali službi, na katero je naslovljena;

(b) odpira in pregleduje vse poštno pošiljke, ki na drug način prispejo k upravljavcu, razen tistih, ki so navedene pod (c) in (d);

(c) ne odpira pošiljk, ki so naslovljene na nekoga drugega in so pomotoma prispele k upravljavcu;

(d) ne sme odpreti pošiljk, naslovljenih na zaposlenega, na katerih je navedeno, da je obvezna osebna vročitev, ter tistih pošiljk, na katerih je najprej navedeno ime zaposlenega brez označbe njegovega uradnega položaja in šele nato naslov upravljavca.

### 14. člen

#### Varovanje strojne in programske opreme

(1) Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z odobritvijo osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblašчени servisi in vzdrževalci, ki imajo z upravljavcem osebnih podatkov sklenjeno ustrezno pogodbo.

(2) Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo zaposlenim pri upravljavcu osebnih podatkov, ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

(3) Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve osebe, zadolžene za delovanje računalniškega informacijskega sistema, izvajajo pa ga lahko samo pooblašчени servisi in organizacije ter posamezniki, ki imajo z upravljavcem osebnih podatkov sklenjeno ustrezno pogodbo.

Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

(4) Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila kot za ostale podatke iz teh pravil.

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

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

(7) Zaposleni pri upravljavcu osebnih podatkov ne smejo nameščati programske opreme in odnašati programske opreme iz prostorov upravljavca osebnih podatkov brez vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

(8) Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov. Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelani ter kdo je to storil. Vsi dogodki morajo biti opremljeni s časovnim žigom.

(9) Oseba, zadolžena za delovanje računalniškega informacijskega sistema, določi način dodeljevanja, hranjenja in spreminjanja gesel in o tem seznanji vse zaposlene pri upravljavcu osebnih podatkov.

(10) Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov (nadzorniška gesla), administriranje elektronske pošte in administriranje aplikativnih programov se hranijo v zapečatenih ovojnica in se jih varuje pred dostopom nepooblaščenih oseb. Uporabi se jih samo v izrednih okoliščinah oziroma ob nujnih primerih. Vsaka uporaba vsebine zapečatenih ovojnic se dokumentira. Po vsaki takšni uporabi se določi nova vsebina gesel.

(11) Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki nahajajo tam. Administrativno osebje mora imeti v nujnem primeru dostop do varnostnih kopij. Določiti se morajo roki za shranjevanje in izbris varnostnih kopij.

(12) Kopije iz prejšnjega odstavka se hranijo na za to določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev, zaklenjena in prostorsko ločena od vira informacij.

(13) Dostop do programske opreme mora biti urejen s politiko dostopnih pravic. Dostop je dovoljen samo za to vnaprej določenim delavcem in zunanjim ponudnikom storitev. Računalniško omrežje mora biti zaščiteno s požarnim zidom in protivirusno programsko opremo.



(14) Dostop do informacijskih sistemov je omejen na pravice, ki so potrebne za izvajanje določene naloge. Uporabniki ne smejo prejeti več pravic, kot jih potrebujejo za izvajanje svojih nalog.

(15) Za preprečitev morebitnega napada se beležijo vsi uspešni in neuspešni poskusi dostopa do informacijskega sistema.

(16) Zunanji dostopi, namenjeni vzdrževanju, se omogočijo le za čas vzdrževanja po predhodno dokumentiranem zahtevku. Po prenehanju vzdrževalnih del se podeljeni dostopi za vzdrževanje deaktivirajo oziroma onemogočijo.

(17) Če zaposleni zamenja delovno mesto ali naravo dela, se njegove pravice ponovno preveri in po potrebi prilagodi.

(18) Če zaposleni preneha z delom pri upravljavcu, mu mora slednji najkasneje na zadnji delovni dan odvzeti vsa izdana dovoljenja za dostop. Enako velja za vse zunanje ponudnike storitev.

(19) Če zaposleni za krajši čas zapusti delovno mesto, se mora zaslon, ki ga je uporabljal, po določenem času zakleniti z geslom.

(20) Če je tehnično izvedljivo, se mora zgoditi avtomatska odjava uporabnika, kadar v določenem časovnem obdobju ni bil aktiven.

(21) Vsaka operacija s podatki se beleži v sistemskih dnevniških datotekah. Beleženje mora omogočiti administrator v skladu z zahtevami in zmožnostmi operacijskega sistema in aplikacij.

#### IV. STORITVE, KI JIH OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

##### 15. člen

##### Pogodbena obdelava

(1) Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z obdelavo osebnih podatkov in je registrirana za opravljanje takšne dejavnosti (v nadaljevanju: pogodbeni obdelovalec), upravljavec osebnih podatkov sklene pisno pogodbo.

(2) Pogodba iz prejšnjega odstavka mora obvezno vsebovati tudi pogoje in ukrepe za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

(3) Prejšnji odstavek velja tudi za pogodbene obdelovalce, ki vzdržujejo obstoječo strojno in programsko opremo ter izdelujejo in inštalirajo novo strojno ali programsko opremo.

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

(5) Pogodbeni obdelovalci, ki za upravljavca osebnih podatkov opravljajo pogodbeno dogovorjene storitve izven njegovih službenih prostorov, morajo imeti vsaj enako stopnjo varovanja osebnih podatkov, kakor jo predvidevajo ta pravila.

## V. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

### 16. člen Obveščanje

Zaposleni pri upravljavcu osebnih podatkov 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 odgovorno osebo ali nadrejenega in pooblaščen osebno za varstvo osebnih podatkov (če je imenovana), sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.

Odgovorna oseba, nadrejeni oziroma pooblaščen osebno za varstvo osebnih podatkov mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev nemudoma, najkasneje pa v roku 72 ur po seznanitvi, sporočiti državnemu nadzornemu organu za varstvo osebnih podatkov, v primeru suma storitve kaznivega dejanja pa tudi policiji ali tožilstvu. Kadar je verjetno, da bo kršitev povzročila veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec brez nepotrebne odlašanja o kršitvi obvestiti tudi posameznike, na katere se zadevni osebni podatki nanašajo.

Upravljavec mora evidentirati vse varnostni incident v kronološkem zaporedju. Zlasti mora beležiti kršitve zaupnosti podatkov (na primer nepooblaščen razkritje podatkov), kršitve v zvezi z možnostjo dostopa do podatkov in kršitve integritete podatkov.

## VI. ODGOVORNOST ZA IZVAJANJE POSTOPKOV IN UKREPOV ZA ZAVAROVANJE OSEBNIH PODATKOV

### 17. člen Izvajanje postopkov in ukrepov

Vsak, ki obdeluje osebne podatke, je dolžan izvajati s temi pravili predpisane postopke in ukrepe za zavarovanje osebnih podatkov in varovati osebne podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela. Obveza varovanja podatkov ne preneha s prenehanjem delovnega razmerja.

### 18. člen Odgovornost za izvajanje in nadzor nad izvajanjem

(1) Oseba, odgovorna za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov, določenih s temi pravili, je Šinko Štefan, Zastopnik.

(2) Oseba, ki opravlja nadzor nad izvajanjem postopkov in ukrepov, določenih s temi pravili, je Šinko Štefan, Zastopnik, oziroma pooblaščen osebno za varstvo osebnih podatkov (21. člen), če je imenovana.

### 19. člen Izjava

(1) Pred nastopom dela na delovnem mestu, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

(2) Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami teh pravil ter

določbami Zakona in Uredbe, izjava pa mora vsebovati tudi pouk o posledicah kršitve teh pravil, Zakona in Uredbe.

#### 20. člen Odgovornost za kršitev

- (1) Za kršitev določil iz 17., 18. in 19. člena teh pravil so zaposleni pri upravljavcu osebnih podatkov disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.
- (2) Odgovornost iz prejšnjega odstavka ne izključuje prekrškovne, kazenske ali odškodninske odgovornosti.

#### 21. člen Pooblaščen osebja za varstvo osebnih podatkov

- (1) Upravljavec mora v skladu s 37. členom Uredbe s posebnim sklepom imenovati pooblaščen osebja za varstvo osebnih podatkov, razen če Uredba določa drugače.
- (2) Podatke o pooblaščen osebju za varstvo osebnih podatkov mora upravljavec v zakonsko predpisanem roku od imenovanja ali spremembe sporočiti nadzornemu organu.
- (3) Upravljavec se posvetuje s pooblaščen osebju za varstvo osebnih podatkov, kot to določa Uredba.
- (4) Kontaktne podatke o pooblaščen osebju (najmanj telefonsko številko ali e-naslov) mora upravljavec objaviti na takem mestu, da so vidni vsem zainteresiranim (na primer na svoji spletni strani).
- (5) Če je pooblaščen osebja za varstvo osebnih podatkov zaposlena v kolektivu upravjavca, ji mora ta omogočiti ustrezno izobraževanje o predpisih, povezanih z varstvom osebnih podatkov.
- (6) Upravljavec mora od pooblaščen osebja za varstvo osebnih podatkov pridobiti dokazila o njeni ustreznih usposobljenosti.

### VII. KONČNA DOLOČBA

#### 22. člen Veljavnost pravil

Ta pravila začnejo veljati z dnevom objave.

#### 23. člen Način objave

Pravila upravljavec objavi na zanj običajen način, tako da se lahko z njimi seznanijo vsi zaposleni in pogodbeni partnerji, ki so udeleženi pri obdelavi osebnih podatkov.

#### 24. člen

Vse spremembe in dopolnitve teh pravil se sprejmejo na enak način kot ta pravila in v pisni obliki.

25. člen

Z dnem sprejetja predmetnih Poslovnih pravil, prenehajo veljati Poslovna pravila o postopkih in ukrepih za varovanje osebnih podatkov z dne 10. 5. 2019.

V Vodica, dne 21.11.2024

Hari Arčon  
Predsednik KZS

