

PRAVILNIK O ZAVAROVANJU OSEBNIH PODATKOV

Ta pravilnik določa postopke in ukrepe za zavarovanje pri zbiranju, obdelovanju, shranjevanju, posredovanju in uporabi osebnih podatkov, vodenih v zbirkah osebnih podatkov, s katerimi upravlja družba Toko d.o.o. (v nadaljevanju družba) z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje podatkov, njihovo spremembo ali izgubo, kakor tudi nepooblaščen dostop, obdelava, uporaba ali posredovanje.

Zaposleni in zunanji sodelavci, ki pri svojem delu obdelujejo in uporabljajo osebne podatke, morajo biti seznanjeni z Zakonom o varstvu osebnih podatkov, s področno zakonodajo, ki ureja posamezno področje njihovega dela ter z vsebino tega pravilnika.

1. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. ZVOP-1: Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/04, 113/05 s spremembami in dopolnitvami);
2. Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
3. 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;
4. 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;
5. 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, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana;

6. Upravljavec osebnih podatkov je fizična ali pravna oseba, 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;

7. Občutljivi osebni podatki so podatki o rasmem, narodnem ali narodnostnem poreklu, političnem, verskem, filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;

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

9. Nosilci podatkov so vse vrste sredstev, na katerih so zapisani ali posneti podatki: listine, akti, gradiva, spisi, računalniška oprema vključno s magnetni, optični ali drugi računalniški mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.;

3. člen

Opis zbirk osebnih podatkov, katerih upravljavec je družba, se vodi v katalogu zbirk osebnih podatkov. Katalog se vodi v skladu z določbami 26. člena ZVOP-1. Podatki iz 1., 2., 4., 5., 6., 9., 10., 12. in 13. točke katalogov zbirk osebnih podatkov se posredujejo državnemu organu, pristojnemu za vodenje Registra zbirk osebnih podatkov. Katalog zbirke osebnih podatkov se za vsako zbirko osebnih podatkov zagotovi najkasneje 15 dni pred vzpostavitvijo zbirke osebnih podatkov, v istem roku pa se podatki iz kataloga posredujejo tudi pristojnemu državnemu organu. Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki, spremembe pa se v roku 8 dni posredujejo tudi pristojnemu državnemu organu. Katalog zbirk osebnih podatkov je priloga št. 1 k temu pravilniku.

Zaposleni, ki obdelujejo osebne podatke, morajo biti seznanjeni s katalogom zbirk osebnih podatkov, vpogled v katalog zbirk osebnih podatkov pa je potrebno omogočiti tudi vsakomur, ki to zahteva.

Družba je dolžna voditi ažuren seznam, iz katerega je za vsako zbirko osebnih podatkov jasno razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo sledeči podatki: naziv zbirke osebnih podatkov, osebno ime in delovno mesto osebe, ki je odgovorna za zbirko osebnih podatkov ter osebno ime in delovno mesto oseb, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke, ki se nanašajo na zbirko osebnih podatkov. Seznam je priloga št. 2 k temu pravilniku.

II. VAROVANJE PROSTOROV IN RAČUNALNIŠKE OPREME

4. člen

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

Dostop je mogoč le v rednem delovnem času, izven tega časa pa samo na podlagi dovoljenja vodje organizacijske enote ali direktorja družbe.

Ključni varovanih prostorov se uporabljajo in hranijo v skladu s hišnim redom. Ključni 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.

Izven delovnega časa morajo biti omare in pisalne mize z nosilci osebnih podatkov zaklenjene, računalniki in druga strojna oprema izklopljeni in fizično ali programsko zaklenjeni.

Zaposleni ne smejo puščati nosilcev osebnih podatkov na mizah v prisotnosti oseb, ki nimajo pravice vpogleda vanje.

Nosilci osebnih podatkov, ki se nahajajo izven zavarovanih prostorov (hodniki, skupni prostori) morajo biti stalno zaklenjeni.

Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov.

5. člen

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

6. člen

Vzdrževanje in popravila strojne računalniške in druge opreme je dovoljeno samo z vednostjo pooblaščenih oseb ali direktorja, izvajajo pa ga lahko samo pooblaščenih servisi in vzdrževalci, ki imajo z družbo sklenjeno ustrezno pogodbo.

7. člen

Vzdrževalci prostorov, strojne in programske opreme, obiskovalci in poslovni partnerji se smejo gibati v varovanih prostorih le ob prisotnosti pooblaščenih oseb. Osebe, kot so čistilke in varnostniki, se lahko izven delovnega časa gibljejo samo v tistih varovanih prostorih, kjer je onemogočen vpogled v osebne podatke. Nosilci podatkov morajo biti shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in druga strojna oprema morajo biti izklopljeni ali kako drugače zaklenjeni.

III. VAROVANJE SISTEMSKÉ IN APLIKATIVNO PROGRAMSKÉ RAČUNALNIŠKE OPREME TER PODATKOV, KI SE OBDELUJEJO Z RAČUNALNIŠKO OPREMO

8. člen

Dostop do programske opreme mora biti varovan tako, da dovoljuje dostop samo za to v naprej določenim zaposlenim ali pravnim ali fizičnim osebam, ki v skladu s pogodbo opravljajo dogovorjene storitve.

9. člen

Popravljanje, spreminjanje in dopolnjevanje systemske in aplikativne programske opreme je dovoljeno samo na podlagi odobritve pooblaščenih oseb, izvajajo pa ga lahko samo

pooblašteni servisi in organizacije in posamezniki, ki imajo z družbo sklenjeno ustrezno pogodbo.

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

10. člen

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka določila, kot za ostale podatke iz tega pravilnika.

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora skrbeti, da se v primeru servisiranja, popravila, spreminjanja ali dopolnjevanja sistemske ali aplikativne programske opreme ob morebitne kopiranje osebnih podatkov, po prenehanju potrebe po kopiji, kopija uniči.

Delavec, pooblaščen za obdelavo in ravnanje z osebnimi podatki na računalniku, mora biti v času servisiranja računalnika in programske opreme ves čas prisoten in mora nadzirati, da ne pride do nedopustnega ravnanja z osebnimi podatki.

V primeru izkazane potrebe po popravilu računalnika, na čigar disku se nahajajo osebni podatki, izven zavoda in brez kontrole pooblaščenega delavca zavoda, se morajo podatki z diska računalnika izbrisati na način, ki onemogoča restavracijo. Če tak izbris ni mogoč, se mora popravilo opraviti v poslovnih prostorih zavoda v prisotnosti pooblaščenega delavca.

11. člen

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

Ob pojavu računalniškega virusa je potrebno storiti vse, da s pomočjo ustrezne strokovne službe virus odpravi in da se ugotovi vzrok pojava virusa.

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

12. člen

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

13. člen

Pristop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov in podatkov, sistem gesel pa mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

Pooblaščen osebni določi režim dodeljevanja hranjenja in spreminjanja gesel.

14. člen

Vsa gesla in postopki, ki se uporabljajo za vstop in administriranje mreže osebnih računalnikov, 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.

15. člen

Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj.

Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena.

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

16. člen

Z vsako zunanjo pravno ali fizično osebo, ki opravlja posamezna opravila v zvezi z zbiranjem, obdelovanjem, shranjevanjem ali posredovanjem osebnih podatkov in je registrirana za opravljanje takšne dejavnosti, se sklene pisna pogodba. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja. Omenjeno velja tudi za zunanje osebe, ki 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 naročnikovih pooblastil in podatkov ne smejo obdelovati ali drugače uporabljati za noben drug namen.

Pooblaščená pravna ali fizična oseba, ki za družbo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva ta pravilnik.

V. SPREJEM IN POSREDOVANJE OSEBNIH PODATKOV

17. člen

Delavec, ki je zadolžen za sprejem in evidenco pošte, mora izročiti poštno pošiljko z osebniimi podatki direktno posamezniku, ali službi, na katero je ta pošiljka naslovljena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, odpira in pregleduje vse poštné pošiljke in pošiljke, ki na drug način prispejo v družbo - prinesejo jih stranke ali kurirji, razen pošiljk iz tretjega in četrtega odstavka tega člena.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne odpira tistih pošiljk, ki so naslovljene na drug organ ali organizacijo in so pomotoma dostavljena ter pošiljk, ki so

označene kot osebni podatki ali za katere iz označb na ovojnici izhaja, da se nanašajo na natečaj ali razpis.

Delavec, ki je zadolžen za sprejem in evidenco pošte, ne sme odpirati pošiljk, naslovljenih na delavca, na katerih je na ovojnici navedeno, da se vročijo osebno naslovniku, ter pošiljk, na katerih je najprej navedeno osebno ime delavca brez označbe njegovega uradnega položaja in šele nato naslov družbe.

18. člen

Prenašanje osebnih podatkov preko telekomunikacijski sredstev, elektronske pošte ali drugih računalniških medijev izven prostorov družbe mora biti zavarovano s postopki in ukrepi na način, ki nepooblaščenim preprečuje prilaščanje, uničenje ali nedovoljeno seznanjanje z njihovo vsebino.

Občutljivi osebni podatki se pošiljajo naslovnikom v zaprtih ovojnicah proti podpisu v dostavni knjigi ali z vročilnico.

Osebni podatki se pošiljajo priporočeno.

Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da ovojnica ne omogoča, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno lučjo vidna vsebina ovojnice. Prav tako mora ovojnica zagotoviti, da odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice.

19. člen

Obdelava občutljivih osebnih podatkov mora biti posebej označena in zavarovana.

Podatki iz prejšnjega odstavka se smejo posredovati preko telekomunikacijskih omrežij samo, če so posebej zavarovani s kriptografskimi metodami in elektronskim podpisom tako, da je zagotovljena nečitljivost podatkov med njihovim prenosom.

20. člen

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

Za vsako posredovanje osebnih podatkov mora upravičenec vložiti pisno vlogo, v kateri mora biti jasno navedena določba zakona, ki uporabnika pooblašča za pridobitev osebnih podatkov, ali pa mora biti k vlogi priložena pisna zahteva oziroma privolitev posameznika, na katerega se podatki nanašajo.

Vsako posredovanje osebnih podatkov se beleži v evidenco posredovanj, iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

Nikoli se ne posredujejo originali dokumentov, razen v primeru pisne odredbe sodišča. Originalni dokument se mora v času odsotnosti nadomestiti s kopijo.

VI. BRISANJE PODATKOV

21. člen

Po preteku roka hranjenja se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, razen če zakon ali drug akt ne določa drugače.

Roki, po katerih se osebni podatkov izbrišejo iz zbirke podatkov, so razvidni iz kataloga zbirk osebnih podatkov.

22. člen

Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Podatki na klasičnih medijih, kot so listine, kartoteke, register, seznam, se uničijo na način, ki onemogoča čitanje 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 komisija, ki o uničenju sestavi tudi ustrezen zapisnik.

VII. UKREPANJE OB SUMU NEPOOBLAŠČENEGA DOSTOPA

23. člen

Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščno uničenje, nepooblaščno spreminjanje, poškodovanje zbirke, prilaščanje osebnih podatkov) ali do vdora v zbirko osebnih podatkov, mora takoj o tem obvestiti direktorja in pooblaščenega delavca, ki vodi in ureja zbirko osebnih podatkov, ki so bili zlorabljeni ali v katero se je vdrla.

VIII. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

24. člen

Za izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vodje organizacijskih enot in pooblašcene osebe, ki jih imenuje direktor.

Nadzor nad izvajanjem postopkov in ukrepov, določenih s tem pravilnikom, opravlja splošna služba.

25. člen

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

Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora zaposleni podpisati posebno izjavo, ki ga zavezuje k varovanju osebnih podatkov.

Iz podpisane izjave mora biti razvidno, da je podpisnik seznanjen z določbami tega pravilnika ter določbami ZVOP-1, izjava pa mora vsebovati tudi pouk o posledicah kršitve.

26. člen

Za kršitev določil iz prejšnjega člena so zaposleni disciplinsko odgovorni, ostali pa na temelju pogodbenih obveznosti.

IX. KONČNE DOLOČBE

27. člen

Ta pravilnik prejmejo delavci, katerih delovne obveznosti so med drugim tudi zbiranje, urejanje, obdelava, spreminjanje, shranjevanje, posredovanje ali uporaba osebnih podatkov ali nosilcev osebnih podatkov.

28. člen

Ta pravilnik prične veljati 8. dan po objavi.

V Ljubljani, 21.05.2018

Toko d.o.o.