



P R A V I L N I K
o varstvu osebnih in zaupnih podatkov

Datum odobritve/velja od: 20. 12. 2018

Skrbnik dokumenta: Alenka Berložnik

Na podlagi Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov, v nadaljevanju: GDPR), in Zakona o varstvu osebnih podatkov (Uradni list RS, v nadaljevanju: ZVOP-1) izdaja direktorica Zavoda SLOKVA so. p. (v nadaljevanju družba)

P R A V I L N I K

o varstvu osebnih in zaupnih podatkov

I. SPLOŠNE DOLOČBE

1. člen

S tem pravilnikom se določajo pravni, organizacijski, tehnični in logično-tehnični postopki ter ukrepi za varstvo varovanih osebnih in zaupnih podatkov, ki se obdelujejo v družbi, z namenom, da se prepreči slučajno ali namerno nepooblaščen uničevanje osebnih podatkov, njihovo spremembo ali izgubo ter da se prepreči nepooblaščen dostop, obdelava, uporaba ali posredovanje osebnih podatkov in zbirk osebnih podatkov.

Z ukrepi in postopki, določenimi v tem pravilniku, se v gospodarski družbi:

- preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika/ce pri obdelavi osebnih podatkov;
- zagotavlja varno obdelavo zaupnih podatkov;
- omogoča ugotavljanje, kdaj so bili posamezni osebni in zaupni podatki obdelani in kdo jih je obdelal, in sicer za obdobje, za katero se posamezni podatki hranijo.

Pravilnik ureja tudi vodenje kataloga zbirk osebnih podatkov (evidenc dejavnosti obdelave) v družbi in postopek v zvezi z varstvom pravic, ki gredo posamezniku na podlagi obdelave osebnih podatkov.

2. člen

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. *osebni podatek* - je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen;
2. *zaupni podatek* – je vsak podatek, ki je posebej označen kot zaupen npr. "Zaupni podatek"
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, nesorazmerno velikega napora ali ne zahteva veliko časa;
4. *obdelava osebnih in zaupnih 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 in 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 (sredstva obdelave);
5. *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;
6. *upravljalec 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 oz. oseba, določena z zakonom, ki določa tudi namene in sredstva obdelave;
 7. *pogodbeni obdelovalec*- je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki;
 8. *varovan oseben in zaupen podatek*: oseben ali zaupen podatek družbe, poslovnega partnerja ali povezanih družb in predstavništev, ki je kot tak ustrezno označen, katerega obravnavanje mora spremljati izvajanje določenih varnostnih ukrepov in postopkov;
 9. *dokument*: vsi napisani, narisani, natisnjeni, razmnoženi, fotografirani, fotokopirani, magnetno, optično, oziroma kako drugače zapisani osebni in varovani podatki;
 10. *pooblaščenec* je s strani direktorja imenovan delavec, ki skrbi za izvajanje postopkov in ukrepov za izvajanje varstva osebnih podatkov. Pooblaščenec vodi seznam skrbnikov zbirke osebnih podatkov.
 11. *delavec družbe* – je oseba, ki ima z družbo sklenjeno pogodbo o zaposlitvi, oseba, ki opravlja v družbi delo kot dijak, študent, oseba, ki opravlja delo v družbi na podlagi pogodbe med družbo in njihovim delodajalcem, ki opravlja dejavnost zagotavljanja dela drugim delodajalcem in oseba, ki opravlja delo za družbo na podlagi pogodbe civilnega prava.
 12. *varnostni incident* – pomeni kršitev, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani.

II. OSEBJE, KI OBDELUJE VAROVANE OSEBNE IN ZAUPNE PODATKE

3. člen

Varovane osebne in zaupne podatke lahko obdeluje le tisti delavec družbe ali zunanji sodelavec družbe, ki je bil pred sklenitvijo delovnega razmerja ali dodelitvijo naloge (v nadaljevanju delavec zavoda), v okviru katere bo obdeloval varovane osebne in zaupne podatke, opozorjen in se zaveda, da je vsebina njegovih del in nalog tudi obdelava varovanih osebnih in zaupnih podatkov in da bo pri svojem delu upošteval zakone s področja varstva osebnih podatkov in ta pravilnik, kar potrdi s **pisno izjavo, ki je priloga pogodbe o zaposlitvi**.

4. člen

Delavec družbe lahko varovane osebne in zaupne podatke obdeluje le pri opravljanju svojih nalog in skladno z navodili, ki urejajo način obdelovanja posameznih varovanih osebnih in zaupnih podatkov in tem pravilnikom.

5. člen

Z vsebino varovanih osebnih in zaupnih podatkov delavec družbe, ki te podatke obdeluje, ne sme seznaniti drugih oseb, razen pod pogoji in na način kot jih določa zakon s področja varstva osebnih podatkov in ta pravilnik.

Kadar opravljanje nalog družbe zahteva, da se z določenimi varovanimi osebnimi in zaupnimi podatki seznanijo tudi druge osebe in za to obstaja zakonska podlaga ali podlaga v tem pravilniku, mora delavec pred posredovanjem teh podatkov dobiti direktorjevo dovoljenje.

III. STORITVE, KI JIH OPRAVLJA POGODBENI OBDELOVALEC

6. 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 (pogodbeni obdelovalec), se sklene pisna pogodba, predvidena v splošni uredbi o varstvu podatkov. Pogodba mora obvezno vsebovati vrste obdelave osebnih podatkov, ki jih bo izvajal pogodbeni obdelovalec, vrste osebnih podatkov, ki jih upravljaavec za izvajanje pogodbene obdelave zaupa pogodbenemu obdelovalcu, zbirke, katerih del so osebni podatki ter namene obdelave posameznih osebnih podatkov. V pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja kot so določeni s tem pravilnikom.

Pogodbeni obdelovalec sme opravljati samo storitve obdelave osebnih podatkov v okviru naročnikovih pooblastil in podatkov ne sme obdelovati ali drugače uporabljati za noben drug namen.

Pogodbeni obdelovalec, ki za družbo opravlja dogovorjene storitve izven prostorov upravljavca, mora imeti vsaj enako strog način varovanja osebnih podatkov, kakor ga predvideva pravilnik.

Kadar je v obdelovanje podatkov ali v izgradnjo, oziroma vzdrževanje infrastrukture računalniško-informacijskega in telekomunikacijskega sistema družbe vključen zunanji izvajalec, mora biti določilo o dolžnosti varovanja osebnih in zaupnih podatkov, katere upravlja družba, vključeno v pogodbo, s katero se uredijo razmerja in odnosi med družbo in izvajalcem pogodbenih del. Izvajalčev delavec mora s pisno izjavo potrditi, da je seznanjen z dolžnostjo varovanja osebnih in zaupnih podatkov družbe, ki jih bo obravnaval pri izvajanju pogodbenih del. Pisna izjava je sestavni del pogodbene dokumentacije.

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

IV. SPLOŠNI VARNOSTNI UKREPI

7. člen

Zaradi varstva osebnih in zaupnih podatkov so delavci družbe dolžni izvajati sledeče splošne varnostne ukrepe:

1. obdelovanih osebnih podatkov nikoli ne puščajo nenadzorovanih;
2. kadar zapuščajo svoje delovne prostore, morajo zakleniti pisalne mize, omare, blagajne in pisarne, v katerih hranijo varovane osebne in zaupne podatke;
3. medijev z varovanimi osebnimi in zaupnimi podatki med svojo odsotnostjo ne smejo puščati na pisalnih mizah;
4. dostop do osebnih podatkov v elektronski obliki bodo zaščitili z uporabniškim imenom in geslom, ki ga bodo ustrezno menjali;
5. brezžično omrežje, preko katerega dostopajo do osebnih podatkov bodo ustrezno zavarovali z geslom;
6. operacijski sistem, programe in aplikacije, preko katerih dostopajo do podatkov na napravah (računalniki, tablice, telefoni) bodo protivirusno zaščitili proti zlonamernim kodam in jih redno posodabljali;

7. dosledno morajo izvajati postopek prijave oziroma odjave v informacijski sistem s svojim osebnim geslom na začetku oziroma ob zaključku dostopa do varovanih osebnih in zaupnih podatkov;
8. po končani izdelavi dokumentov z varovanimi osebnimi in zaupnimi podatki morajo poskrbeti za uničenje pomožnega gradiva, ki so ga uporabili oziroma, ki je nastalo pri izdelavi dokumenta;
9. upoštevati zakonodajo s področja varstva osebnih podatkov, ta pravilnik in druge predpise, ki določajo, kako naj pri svojem delu ravnajo z varovanimi osebnimi in zaupnimi podatki.

V. KATALOG ZBIRK OSEBNIH PODATKOV / EVIDENCA DEJAVNOSTI OBDELAVE OSEBNIH PODATKOV

8. člen

Opis zbirk osebnih podatkov, katerih upravljavec je družba, se vodi v Katalogu zbirk osebnih podatkov (v nadaljevanju: Katalog), ki je sestavni del in Priloga 2 tega pravilnika.

Podatki iz Kataloga se vodi v elektronski obliki in je shranjena družbinem osebnem računalniku.

VI. OBDELAVA OSEBNIH PODATKOV

9. člen

V družbi se lahko obdelujejo le tisti osebni podatki, za katere obstaja pravna podlaga, v nasprotnem primeru pa je potrebno osebne podatke takoj nehati obdelovati in onemogočiti dostop ter o tem obvestiti direktorja družbe.

Posebne vrste osebnih podatkov se lahko v družbi obdeluje le v skladu z določbami zakonodaje s področja varstva osebnih podatkov. Pri obdelavi morajo biti ti podatki posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

VII. PRAVICE POSAMEZNIKOV

10. člen

Posameznik ima možnost od družbe zahtevati oziroma ima naslednje pravice:

- pravica do dostopa oziroma posredovanja osebnih podatkov, ki jih upravljavec vodi o posamezniku vključno z namenom, pravno podlago in rokom hranjenja,
- pravico do popravka oziroma dopolnitve svojih podatkov,
- pravico do izbrisa (pravico do pozabe) v kolikor to ni v neskladju z zakonsko potrebnimi roku hranjenja njegovih podatkov,
- pravico do omejitve obdelave,
- pravico do prenosa svojih podatkov ter
- pravico do ugovora obdelavi podatkov.

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

- osebni podatki niso več potrebni v namene, za katere so bili zbrani ali kako drugače obdelani;
- posameznik prekliče privolitev, na podlagi katere poteka obdelava in za obdelavo ne obstaja nobena druga pravna podlaga;

- posameznik obdelavi ugovarja, za njihovo obdelavo pa ne obstajajo nobeni prevladujoči zakoniti razlogi;
- osebni podatki so bili obdelani nezakonito;
- osebne podatke je treba izbrisati za izpolnitev pravne obveznosti zaradi izpolnitve zakonskih obveznosti;
- osebni podatki so bili zbrani v zvezi s ponudbo storitev informacijske družbe od mladoletnega posameznika.

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

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

Posameznik ima pravico, da prejme osebne podatke ki jih je posredoval družbi, v strukturirani, splošno uporabljani in strojno berljivi obliki, in pravico, da te podatke posreduje drugemu upravljavcu, ne da bi ga družba pri tem ovirala, kadar:

- obdelava temelji na privolitvi in
- se obdelava izvaja z avtomatiziranimi sredstvi.

Direktor družbe je dolžan poskrbeti za to, da so posamezniki na primeren način, ki je skladen z zahtevami zakonodaje s področja varstva osebnih, obveščeni o pravicah iz prejšnjih odstavkov tega člena. Direktor tudi poskrbi za enotno kontaktno točko, na katero se lahko obrnejo posamezniki pri uveljavljanju svojih pravic.

VIII. BRISANJE PODATKOV, ANONIMIZACIJA IN UNIČENJE NOSILCEV OSEBNIH PODATKOV

11. člen

Osebni podatki se lahko vodijo v zbirki osebnih podatkov le toliko časa, kolikor je potrebno, da se doseže namen, za katerega se zbirajo in vodijo. Rok je določen v Katalogu.

Osebne podatke je treba po preteku roka iz prvega odstavka tega člena obvezno izbrisati ali uničiti in to tako, da je nemogoče njihovo restavriranje. Uničenje in brisanje osebnih podatkov se opravi komisijsko. Vodja organizacijske enote za splošne posle imenuje tričlansko komisijo, ki o uničenju osebnih podatkov izda zapisnik.

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

12. člen

Za brisanje osebnih podatkov na računalniških medijih se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela brisanih podatkov.

Osebni podatki na klasičnih medijih (listine, kartoteke, register, seznam ipd.) se brišejo z uničenjem nosilcev. Nosilci se fizično uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov

Uničevanje osebnih podatkov na nosilcih iz prejšnjega odstavka se mora izvajati tekoče in ažurno.

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

IX. UKREPANJE OB VARNOSTNIH INCIDENTIH OZIROMA UGOTOVITVI ZLORABE OSEBNIH PODATKOV

13. člen

Delavci so dolžni izvajati ukrepe za preprečevanje zlorabe osebnih podatkov in morajo z osebnimi podatki, s katerimi se seznanijo pri svojem delu, ravnati vestno in skrbno na način in po postopkih, ki jih določa ta pravilnik in zakonodaja s področja varstva osebnih podatkov.

Delavec, ki izve ali opazi, da je prišlo do zlorabe osebnih podatkov (odkrivanje osebnih podatkov, nepooblaščen uničenje, zlonamerno ali nepooblaščen uporabo, prilaščanje, spreminjanje ali poškodovanje) mora takoj obvestiti direktorja oziroma pooblaščen osebo, ki vodi in ureja zbirko osebnih podatkov, sam pa poskuša zlorabo osebnih podatkov preprečiti.

Direktor družbe mora ob vsakem sumu kršitve varstva osebnih podatkov takšno kršitev sporočiti Informacijskemu pooblaščenju v 72 urah. Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, mora direktor družbe poskrbeti za to, da so prizadeti posamezniki brez nepotrebnega odlašanja obveščeni o tem, da je prišlo do kršitve varstva osebnih podatkov.

X. NADZOR NAD IZVAJANJEM UKREPOV IN POSTOPKOV VAROVANJA

14. člen

Nadzor nad izvajanjem ukrepov in postopkov varovanja varovanih osebnih in zaupnih podatkov po zakonodaji s področja varstva osebnih podatkov in tem pravilniku, opravlja direktor družbe.

XVI. PREHODNE IN KONČNE DOLOČBE

15. člen

Pravilnik kakor tudi njegove spremembe sprejme direktorica družbe in stopi v veljavo z dnem sprejema.

V Slovenj Gradcu, 21. 12. 2018

Direktorica: Alenka Berložnik

