

Mikrocop d. o. o.

# Smo bolj varni v oblaku ali lastni pisarni?

..HRAMBA PRI CERTIFICIRANEM ZUNANJEM PONUDNIKU STORITEV HRAMBE ELEKTRONSKEGA GRADIVA ZAGOTAVLJA VIŠJO RAVEN VARNOSTI, KOT ČE GRADIVO HRANITE PRI SEBI..

Elektronski dokumenti podjetja so še vedno pre pogosto shranjeni na nezavarovanih strežnikih, nekriptiranih trdih diskih ali omrežnih mapah, ki so prosto dostopne zaposlenim ali drugače izpostavljene zunanjim grožnjam. Evropska zakonodaja določa, da morajo podjetja sama poskrbeti za varno hrambo dokumentov, spoštovanje rokov hrambe, ki so jasno določeni glede na tip dokumenta, in zagotavljanje integritete, nespremenljivosti in celovitosti dokumentov. Elektronski dokumenti so zakonsko veljavni le, če so arhivirani na način, ki zagotavlja njihovo celovitost.

## IZZIVI VARNE DOLGOROČNE HRAMBE ELEKTRONSKIH DOKUMENTOV

V množici elektronskih dokumentov je ključno vprašanje njihova varna dolgoročna hramba. Poleg enakih zakonskih zahtev kot veljajo za hrambo fizičnih dokumentov, mora biti hramba elektronskih dokumentov skladna še z različnimi predpisi s področij elektronskega poslovanja in elektronskega podpisa. Omogočati mora preoblikovanje dokumentov v formate za dolgoročno hrambo, priznavati elektronske podpise znotraj EU (eIDAS), upoštevati smernice za podatke o zdravstvenem varstvu in varovanje osebnih podatkov (GDPR). Posledično lahko račune, zasebne listine, pogodbe, pogoje, odškodninske zahtevke, izpiske in druge tipe dokumentov shranjujemo izključno v elektronski obliki, izvirne dokumente v drugi obliki pa uničimo (če posamezen področni zakon ne predpisuje drugače).

Ustrezna zaščita dokumentov v skladu z zakonodajo zagotavlja primerno raven varnosti pred kibernetičnimi napadi, omogoča hrambo pravno veljavnih dokumentov v primeru spora in učinkovito izogibanje kraji podatkov. Ker gre pri tem za zelo zapleteno informacijsko-komunikacijsko in

postopkovno vprašanje, se v praksi vse bolj uveljavlja model hrambe dokumentov pri certificiranem zunanjem ponudniku elektronske hrambe.

## ZAGOTAVLJANJE CELOVITOSTI ARHIVIRANIH DOKUMENTOV

Elektronski dokumenti so podvrženi enakim pravnim omejitvam kot dokumenti v papirni obliki. Tudi če za dokument ni določen zakonski rok hrambe, je potrebno zaradi varovanja interesov podjetja ohraniti njegovo celovitost in zagotavljati njegovo pravno veljavnost. Dokument v formatu PDF, ki je odložen na omrežno mapo datotečnega sistema ali v necertificiran dokumentni sistem, ni skladen z visokimi standardi hrambe. Zaradi pomanjkanja sledljivosti zato ni pravno veljavni dokaz.

V primeru pravnega spora je potrebno na zahtevo predložiti tudi dokazilo o sledljivosti: opisane izvedene procese, navedene varnostne kontrole, dokaz o veljavnosti elektronskega podpisa v času podpisa dokumenta in izvedene postopke za zagotavljanje celovitosti dokumenta, skladno z uredbo eIDAS pa tudi dokaz, da varnost algoritma podpisa ni bila kršena. Vse to strokovnim izvedencem omogoča izvedbo tehničnega nadzora, s katerim ugotovijo, ali je predložen elektronski dokument veljaven kot dokaz.

## TVEGANJA NEUSTREZNEGA UPRAVLJANJA IN HRAMBE DOKUMENTOV

GDPR zahteva izjemno previdnost pri delu z osebnimi podatki. Nepooblaščen vpogledi v dokumente in njihovo deljenje predstavljajo visoko tveganje. Tri četrtine primerov vseh nenačrtovanih izbrisov dokumentov se zgodi zaradi človeške napake. Virus z zlonamerno kodo za kriptiranje nosilcev podatkov se širi z veliko hitrostjo, pri čemer je vsakih 40 sekund zabeležen napad na novo organizacijo. Enemu od petih malih in srednje velikih podjetij kljub plačilu nekaj tisoč evrov ne uspe povrniti podatkov in dokumentov. Neurejeno področje varne hrambe dokumentov omogoča krajo občutljivih poslovnih dokumentov ali celo ustvarjanje lažnih dokumentov. Če podjetja nimajo več dostopa do dokumenta, izgubijo možnost obrambe v primeru spora, kar lahko predstavlja velike finančne posledice.



Zaradi navedenih razlogov je smiselno vpeljati celovit pregled dokumentov, različic in dostopov, ki omogoča tudi zaščito dokumentov in podatkov pred možnimi tveganji. Ustrezno varovanje dokumentov zahteva posebna znanja in veščine zaposlenih ter finančne in tehnične vire, ki niso nujno na voljo vsem podjetjem.

## PODJETJA NAJ SE OSREDOTOČIJO NA SVOJO DEJAVNOST IN PREPUSTIJO HRAMBO STROKOVNJAKOM

Dokumente, ki so shranjeni v certificirani elektronski hrambi zunanjega ponudnika, je nemogoče izbrisati, potvoriti ali spremeniti. Dostop do shranjenih podatkov je dovoljen samo pooblaščenim osebam, vsi posegi pa so zabeleženi. Zagotovljeni sta revizijska sledljivost dokumentov in dogodkov ter trajna berljivost dolgoročnih formatov. S tehnološkimi rešitvami upravljajo vrhunski strokovnjaki, ki zagotavljajo celovitost, varnost, zaupnost in razpoložljivost podatkov in dokumentov v elektronski hrambi.

Vloga zunanjega ponudnika storitve elektronske hrambe je zaščita dokumentov podjetja. Certificirana elektronska hramba pri zunanjem specializiranem ponudniku, ki je skladna s trenutno veljavnimi standardi arhiviranja in varnosti, je bolj varna in ekonomsko upravičena kot če gradivo podjetje hrani pri sebi. (P. R.)

## KAKO DOSEČI KORISTI DIGITALIZACIJE?

Na 15. Mikrocop konferenci, ki bo v četrtek, 25. 10. 2018, v Kongresnem centru Brdo bodo predstavljeni trendi in izzivi digitalizacije. Konferenca je brezplačna, prijava je možna na [www.mikrocop.si/konferenca](http://www.mikrocop.si/konferenca).

### Microcop d.o.o.

Industrijska cesta 1, 1000 Ljubljana  
W: [www.mikrocop.si](http://www.mikrocop.si) | T: 01 587 42 80  
E: [info-si@mikrocop.com](mailto:info-si@mikrocop.com)