

## Prilog 8: Pravilnik o upravljanju povjerljivim informacijama

### Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o zaštiti tajnosti podataka objavljenim u Narodnim novinama br. 114/01 i zakonom o zaštiti osobnih podataka od 12. lipnja 2003. godine.

Prema vrsti tajnosti, informacije se dijele na vojnu, državnu, službenu, poslovnu i profesionalnu tajnu.

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne.

Kategorije službene, državne i vojne tajne pripadaju tijelima državne uprave.

Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice KBF-u ili njegovim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.).

Profesionalna tajna odnosi se na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u tajništvu, referadi, pravnoj službi, osoba koje unose podatke u baze podataka o korisnicima ili sistem administratora poslužitelja, koji u nekim situacijama može doći u dodir s podacima koji pripadaju korisnicima računala.

Dokumenti koji ulaze na KBF s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će KBF proizvesti kao odgovor. U tom slučaju može se koristiti neka od kategorija tajnosti koje su rezervirane za tijela državne uprave (službena, državna ili vojna tajna).

Dokumenti koji se smatraju povjerljivima moraju biti jasno označeni isticanjem vrste i stupnja tajnosti.

Javnima se smatraju sve informacije koje nisu označene kao povjerljive. Izuzetak su osobne informacije, za koje se podrazumijeva da su povjerljive i ne treba ih posebno označavati.

Pravila za čuvanje povjerljivosti odnose se na informacije bez obzira na to u kom su obliku: na papiru, u elektroničkom obliku, zabilježene ili usmeno prenesene, ili su objekti poput maketa, slika, itd.

### Raspodjela odgovornosti

Za klasificiranje povjerljivih informacija zadužen je dekan, koji će izraditi listu osoba koje imaju pravo proglasiti podatke tajnima, te listu osoba koje imaju pristup povjerljivim podacima.

Pravila za čuvanje povjerljivih informacija odnose se na sve zaposlenike KBF-a i vanjske suradnike koji dolaze u doticaj s osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

### Čuvanje povjerljivih informacija

Povjerljive informacije, tiskane na papiru ili u elektroničkom obliku, snimljene na neki medij za pohranu podataka, čuvaju se u zaključanim metalnim, vatrootpornim ormarima, u prostorijama u koje je ograničen pristup.

Pristup povjerljivim informacijama regulira se izradom liste zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vraćanja dokumenata, kako bi se u svakom trenutku znalo gdje se oni nalaze.

### Informacije o zaposlenicima

Socijalni inženjering je metoda koju primjenjuju hackeri kako bi prikupili informacije potrebne za provalu na računala.

Ustanova može informacije o zaposlenima koje se smatraju javnima objaviti na svojim web stranicama. Javnim informacijama smatraju se:

- ime i prezime
- posao koji zaposlenik obavlja
- broj telefona na poslu
- službena e-mail adresa

Na upite o zaposlenicima davati će se samo informacije objavljene na web stranicama. Daljnje informacije o zaposlenima ne smiju se davati bez suglasnosti osobe kojoj podaci pripadaju (npr. adresa stanovanja, broj privatnog telefona, podaci o primanjima, porezu, osiguranju, itd.).

Povjerljive informacije u načelu se ne daju putem telefona jer se sugovornik može lažno predstaviti. Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podacima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik KBF-a će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

### Prenošenje povjerljivih informacija

Informacije koje su klasificirane kao povjerljive zahtijevaju posebne procedure pri slanju i prenošenju.

Povjerljive informacije ne šalju se običnom poštom, već kurirskom. Na odredištu se predaju u ruke osobi kojoj su upućeni, što se potvrđuje potpisom.

Ako se povjerljive informacije šalju elektronički, na primjer kao poruke elektroničke pošte, tada se moraju slati kriptirane.

### Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dođu na KBF ne smiju se kopirati bez izričite dozvole pošiljatelja.

Dokumenti koji pripadaju KBF-u smiju se kopirati samo uz dozvolu osobe koja ih je proglasila povjerljivim, odnosno uprave. Kopija se numerira i o njenom izdavanju vodi se evidencija kao i za original s kojeg je proizvedena.

Osoblje koje posluhuje uređaje za kopiranje treba obučiti i obavezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

### Uništavanje povjerljivih informacija

Mediji koji sadrže povjerljive informacije ne bacaju se, već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi sadržaj (spaljivanjem, usitnjavanjem, prešanjem).

Ukoliko se zastarjela i rashodovana računalna oprema daje na korištenje trećoj strani, obavezno je uništavanje podataka sa diskova posebnim programom koji nepovratno prebriše sadržaj diska.

### Nepridržavanje

Zaposlenici i suradnici koji dolaze u dodir s klasificiranim informacijama potpisuju izjavu o čuvanju povjerljivosti informacija.

Protiv zaposlenika koji ne poštuju pravila o čuvanju povjerljivih informacija bit će pokrenut stegovni postupak, a može ih se i premjestiti na drugo radno mjesto na kojem neće dolaziti u dodir s povjerljivim podacima.

S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti

će se ugovor. Stoga ustanova treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.