DOI: 10.5937/vojdelo1503178T

ZNAČAJ NORMIRANJA INDUSTRIJSKE BEZBEDNOSTI U REPUBLICI SRBIJI U POSTUPKU USKLAĐIVANJA SA ODLUKOM SAVETA 2013/488/EU

Katarina Terzić[*]
Vlada Republike Srbije
Goran Župac[**]
Univerzitet odbrane u Beogradu, Vojna akademija

Zaštita tajnih podataka je na veoma visokom mestu na agendi EU i predstavlja jednu od najznačajnijih oblasti reforme zakonodavstva i usklađivanja sa pravnim nasleđem EU i međunarodnim standardima. Donošenjem sistemskih zakona i podzakonskih akata kojim se propisuje postupanje tajnim podacima, Republika Srbija je učinila značajne korake u ovoj oblasti. Doneta je svojevrsna Uredba o industrijskoj bezbednosti koja je trebalo da propiše jasne procedure za sertifikovanje privrednih subjekata za pristup tajnim podacima, čime bi se, u toku procesa pridruživanja EU, izvršilo usklađivanje sa Odlukom Saveta 2013/488/EU.

Ključne reči: *Evropska unija, industrijska bezbednost, Odluka Saveta 2013/488/EU*

Uvod

Usklađivanje nacionalnog zakonodavstva sa pravnim tekovinama Evropske unije (EU), pored unapređenja ljudskih prava, jačanja pravne države, normiranja propisa u oblasti zaštite životne sredine, slobode medija i drugog podrazumeva i oblast nacionalne bezbednosti i uspostavljanje jasno definisanih instrumenata zaštite nacionalnih interesa, pri čemu se podrazumeva i zaštita regionalne i kolektivne bezbednosti. U tom smislu, neophodna reforma sektora bezbednosti podrazumeva i uspostavljanje i primenu jasnih mehanizama zaštite tajnih podataka od nacionalnog i kolektivnog značaja. Ova oblast u Republici Srbiji zanemarena je duže od dve decenije.

Značajni koraci učinjeni su uspostavljanjem širokog zakonodavnog okvira kojim se propisuje postupanje sa tajnim podacima: Zakon o tajnosti podataka[1], Zakon o slobodnom pristupu informacijama od javnog značaja[2] i Zakon o zaštiti podataka o ličnosti[3]. Po-

[*] Mr Katarina Terzić je šefica kabineta ministarke bez portfelja zadužene za EU.
[**] Pukovnik doc. dr Goran Župac je nastavnik na Visokim studijama bezbednosti i odbrane.
[1] „Службени гласник РС", бр. 104/09.
[2] „Службени гласник РС", бр. 120/04, 54/0, 104/09 и 36/10.
[3] „Службени гласник РС", бр. 97/08 и 104/09.

red sistemskih zakona ova oblast uređena je i nizom podzakonskih akata, kao i ratifikovanim međunarodnim sporazumima.

Zakon o tajnosti podataka i podzakonski akti koji su doneti, u funkciji njegove primene, u najvećoj meri usklađeni su sa pravnim tekovinama i standardima EU. Međutim, izostala je dosledna primena Zakona u praksi, pri čemu je potrebno naglasiti da odredbe Zakona u praksi primenjuju samo Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podatka (KSNBiZTP)[4] i Bezbednosno-informativna agencija. Treba dodati da je izostalo i predviđeno usklađivanje prethodno donetih zakona sa Zakonom o tajnosti podataka, dok su određeni zakoni doneti nakon stupanja na snagu ovog sistemskog zakona takođe, u pojedinim odredbama, neusklađeni.

Inače, u dosadašnjem periodu pokazalo se da je najveći problem u primeni Zakona o tajnosti podataka, pored nepoznavanja materije i nedostatka volje za njegovu primenu u okviru državnih organa, sporost institucija u donošenju podzakonskih akata za njegovu primenu, nejasna podela nadležnosti u predlaganju podzakonskih akata, kao i neadekvatan inspekcijski nadzor.

Poslednji u nizu podzakonskih akata koji je donet jeste Uredba o posebnim merama zaštite tajnih podataka koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa[5]. Ova uredba nezgrapnog naziva zapravo je svojevrsna uredba o industrijskoj bezbednosti, s obzirom na to da predstavlja kompilaciju Priloga V – Industrijska bezbednost Odluke Saveta 2013/488/EU[6] o procedurama zaštite poverljivih podataka EU i nacionalnih propisa.

Veoma značajna Uredba o industrijskoj bezbednosti, koja je trebalo da propiše jasne procedure za sertifikovanje privrednih subjekata za pristup tajnim podacima, čime bi im bilo omogućeno učešće na tenderima za tzv. poverljive nabavke EU, nije ponudila privrednicima jasne procedure za sertifikovanje. Pri tome, izostala je definicija pojma industrijske bezbednosti koji je već zaživeo u zakonu kojim se propisuje rad Vojnobezbednosne agencije[7] i koji je već definisan u dokumentima EU.

Prema Odluci Saveta 2013/488/EU, industrijska bezbednost[8] predstavlja primenu mera kojima se osigurava zaštita tajnih podataka EU od strane izvođača ili podizvođača u pregovorima pre zaključivanja ugovora i tokom celog životnog ciklusa tajnih ugovora, koje uključuju pristup podacima odgovarajućeg stepena tajnosti. U najužem smislu, industrijska bezbednost predstavlja obezbeđivanje bezbednosnih postupaka i mera potrebnih za postizanje odgovarajućeg nivoa zaštite tajnih podataka razmenjenih između države i preduzeća i predstavlja multidisciplinarnu oblast koja se sastoji od elemenata personalne, fizičke, tehničke, administrativne i informacione bezbednosti.[9]

---

[4] KSNBiZTP je stručna služba Vlade, formirana 2009. godine i u Republici Srbiji predstavlja nacionalni organ nadležan za zaštitu tajnih podataka. Pored zaštite nacionalnih tajnih podataka, nadležna je i za zaštitu stranih tajnih podataka, odnosno podataka EU, NATO, EUROPOL.

[5] „Службени гласник РС", бр. 63/13.

[6] Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488 /EU) http://eur-lex.europa.eu/l egal-content/ EN/TXT/ ?qid=1400351027215&uri=CELEX:32013D0488 (izmena Council Decision of 14 April 2014 amending Decision 2013/488/EU on the security rules for protecting EU classified information (2014/233/EU) http://eur-lex.europa.eu/legal content/EN/TXT/?qid =1400351027215&uri= CELEX:32014 D0233

[7] Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији ("Службени гласник РС", бр. 88/09, 55/12-УС и 17/13).

[8] Odluka Saveta 2013/488/EU – član 11.

[9] Група аутора, Систем заштите тајних података у Републици Словенији, Систем заштите тајних података, Мисија ОЕБС у Србији, стр. 35-36. Београд 2012.

Pravni okvir Evropske unije

Odluka Saveta 2013/488/EU

Odluka Saveta 2013/488/EU o Procedurama zaštite poverljivih podataka EU, koja je stupila na snagu objavljivanjem u Službenom glasniku EU, 15. oktobra 2013. godine, zamenila je i potvrdila prethodne odluke Saveta 2011/292/EU i 2001/264/EU[10], tako da se zaštita podataka, regulisana u skladu sa ovim odlukama, nastavlja da sprovodi primenom nove Odluke Saveta 2013/488/EU. Nova odluka doneta je radi prilagođavanja jednog broja odredaba praktičnom iskustvu iz prethodnog perioda, a pojedine procedure su pojednostavljene radi lakše primene u praksi.

Odlukom Saveta 2013/488/EU propisani su osnovni principi i minimalni standardi koji se primenjuju u zaštiti tajnih podataka EU, u svim oblastima koje zahtevaju pristup tajnim podacima, dok je procedura zaštite tajnih podataka u privrednoj oblasti propisana u prilogu V Odluke (Annex V Industrial Security). Države članice su u obavezi da primenjuju Odluku Saveta u skladu sa svojim nacionalnim zakonodavstvom, u meri koja obezbeđuje ostvarivanje minimalnih bezbednosnih standarda propisanih Odlukom, dok, sa druge strane, Savet i Generalni sekretarijat štite tajne podatke države članice u skladu sa standardima koji se primenjuju za zaštitu tajnih podataka EU.

Generalni sekretarijat Saveta može, kao ugovorna strana, da poveri zadatke koji obuhvataju ili uključuju pristup, rukovanje ili čuvanje tajnih podataka stepena tajnosti COFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET privrednim i drugim subjektima koji su registrovani u državi članici ili trećoj državi koja je sa EU zaključila sporazum o bezbednosnim procedurama za razmenu i zaštitu tajnih podataka. Da bi ovi subjekti mogli da zaključe ugovor ili podugovor koji zahteva pristup podacima određenog stepena tajnosti, kojima će rukovati unutar svojih prostorija, u postupku zaključenja i izvršenja ugovora, neophodno je da nacionalni bezbednosni organ (NSA)[11], odnosno ovlašćeni bezbednosni organ (DSA) ili drugi nadležni organ države članice, obezbedi da navedeni subjekti poseduju uverenje o bezbednosnoj proveri pravog lica (FSC) za odgovarajući stepen tajnosti podatka, kao i da zaposleni kod izvođača i podizvođača, kojima je za izvršenje poverljivog ugovora potreban pristup podacima određenog stepena tajnosti, poseduje uverenje o bezbednosnoj proveri fizičkog lica (PSC), a u skladu sa svojim nacionalnim zakonodavstvom.

Osnovni principi i minimalni bezbednosni standardi za zaštitu tajnih podataka EU, koje primenjuju Savet EU i Generalni sekretarijat Saveta (u daljem tekstu: Sekretarijat), utvrđeni su Odlukom Saveta EU, a države članice su u obavezi da ih poštuju u skladu sa svojim nacionalnim zakonodavstvom. Uputstvo za primenu dela Odluke koje se odnosi na industrijsku bezbednost dato je u prilogu Odluke V[12] i sadrži opšte bezbednosne od-

[10] Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC) (OJ L 101, 11.4. 2001, p. 1) amended by Council Decision 2004/194/EC of 10 February 2004 (OJ L 63 28.2.2004), Council Decision 2005/571/EC of 12 July 2005 (OJ L 193 23.7.2005), Council Decision 2005/952/EC of 20 December 2005 (OJ L 346 29.12.2005), Council Decision 2007/438/EC of 18 June 2007 (OJ L 164 26.6.2007), http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=14003509 28118&uri=CELEX:32007D0438

[11] U Republici Srbiji nadležni organ je Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.

[12] Odluka Saveta 2013/488/EU – Prilog V.

redbe koje su primenljive na privredne i druge subjekte u pregovorima pre zaključenja ugovora i tokom važenja ugovornog odnos koji sadrži tajne podatke, a koje Sekretarijat zaključuje sa njima, kao i smernice o industrijskoj bezbednosti sa posebno definisanim zahtevima u vezi sa uverenjem o bezbednosnoj proveri pravnih lica, pismima o bezbednosnim aspektima, posetama, prenosu i transportu tajnih podataka EU.

Sekretarijat, kao ugovorna strana, pre objavljivanja poziva za podnošenje ponuda ili zaključenja ugovora određuje stepen tajnosti svih podataka koji se daju ponuđačima i izvođačima, kao i podataka koje će stvoriti izvođač, u koju svrhu priprema *vodič za stepene tajnosti,* koji će se koristiti za izvršenje ugovora, pri čemu se rukovodi određenim principima: svi važni bezbednosni aspekti, uključujući i stepen tajnosti koji je dodelio subjekt od kojeg potiču podaci, a koje je dostavio i odobrio za korišćenje u ugovoru uzimaju se u obzir; stepen tajnosti ugovora ne može da bude niži od najvišeg stepena tajnosti bilo kog od njegovih delova i, u tom smislu, neophodno je ostvarivanje saradnje sa nacionalnim bezbednosnim organima (NSA), odnosno ovlašćenim bezbednosnim organima (DSA) država članica ili drugim nadležnim bezbednosnim organima u slučaju svake promene koja se odnosi na tajnost podataka koje je stvorio izvođač ili koji su njemu dostavljeni tokom izvršenja ugovora, kao i prilikom naknadnih promena vodiča za stepene tajnosti.

Bezbednosni zahtevi koji su specifični za predmetni ugovor opisuju se u *pismu o bezbednosnim aspektima* (SAL), koje je sastavni deo ugovora sa tajnim podacima. Ovo pismo sadrži odredbe u kojima se od izvođača zahteva da ispuni minimalne standarde, kao i posebne odredbe kojima se uređuje raspolaganje tajnim podacima EU u toku izvršenja ugovora ili nakon njegovog raskida, a po potrebi može da sadrži i vodič za stepene tajnosti. Pored pisma o bezbednosnim aspektima, a u zavisnosti od obima programa ili projekta koji uključuje pristup, rukovanje i čuvanje tajnih podataka EU, izvođač može da pripremi *posebna bezbednosna uputstva (PSI)* koja mora odobriti nacionalni bezbednosni organ, odnosno ovlašćeni bezbednosni organ države članice ili drugi nadležni bezbednosni organ koji učestvuje u bezbednosnim uputstvima.

Uverenje o bezbednosnoj proveri pravnog lica (FSC) izdaje nacionalni bezbednosni organ, odnosno ovlašćeni bezbednosni organ ili drugi nadležan bezbednosni organ države članice, u skladu sa nacionalnim zakonodavstvom. Pre izdavanja uverenja, bezbednosni organ, kao minimum uslova koje privredni ili drugi subjekt mora da ispunjava, po tačno utvrđenoj metodologiji procenjuje sledeće reference: integritet privrednog ili drugog subjekta, vlasništvo, kontrolu ili mogući nedozvoljen uticaj koji se može smatrati bezbednosnim rizikom, te da li je privredni ili drugi subjekat uspostavio bezbednosni sistem u objektu koji mora da obuhvata sve potrebne mere bezbednosti za zaštitu podataka ili materijala stepena tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET[13], da li je utvrđen personalni bezbednosni status rukovodstva, vlasnika i zaposlenih kojima je potreban pristup podacima stepena tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET i da li je privredni ili drugi subjekat imenovao rukovaoca tajnim podacima u objektu, koji je odgovoran svom rukovodstvu za primenu bezbednosnih mera u okviru tog subjekta.

[13] Označavanje stranih tajnih podataka i njihovi odgovarajući stepeni tajnosti, kao i upotreba engleskog jezika prilikom označavanja stranih tajnih podataka u Republici Srbiji propisani su članom 15. Zakona o tajnosti podataka („Службени гласник РС", бр. 104/09).

Kada utvrdi da privredni ili drugi subjekt ispunjava navedene uslove, bezbednosni organ izdaje tom subjektu odgovarajuće uverenje kao potvrdu da on može da zaštiti tajne podatke EU odgovarajućeg stepena tajnosti unutar svog objekta, odnosno svojih poslovnih prostorija. Uverenje se najčešće izdaje u fazi sklapanja ugovora ili za izvršavanje ugovora, ali se može tražiti da ga privredni ili drugi subjekt poseduje mnogo pre, ako se radi o tajnim podacima EU koji su označeni stepenom tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, a moraju da se dostave tokom postupka nadmetanja, odnosno postupka tzv. poverljive nabavke. Nadležni bezbednosni organ države članice u kojoj je registrovan ponuđač sa kojim Sekretarijat treba da zaključi ugovor, dužan je da potvrdi Sekretarijatu da je izdao uverenje o bezbednosnoj proveri pravog lica (FSC), kao i da ga obavesti o svakoj promeni koja utiče na izdato uverenje. Takođe, u slučaju da se uverenje u međuvremenu ukine, to može biti razlog zbog kojeg će Sekretarijat da raskine ugovor ili da isključi ponuđača iz daljeg nadmetanja.

Izvođač može, ako je to navedeno u pozivu za podnošenje ponuda i ugovoru, da zaključi podugovor sa podizvođačem za bilo koji deo ugovora, pod uslovom da je taj podizvođač registrovan u državi članici EU koja ima zaključen sporazum o bezbednosti podataka sa EU, i uz obavezu da se sve aktivnosti podugovaranja preduzimaju u skladu sa propisanim minimalnim standardima, uz prethodnu pisanu saglasnost Sekretarijata.

Kada zaključi ugovor sa najboljim ponuđačem, Sekretarijat je dužan da o bezbednosnim odredbama iz ugovora obavesti nacionalni bezbednosni organ, odnosno ovlašćeni bezbednosni organ ili drugi nadležni bezbednosni organ države članice u kojoj je ponuđač registrovan. U slučaju kada nastupe okolnosti zbog kojih svaka od ugovornih strana može da raskine ugovor, Sekretarijat je dužan da o tome obavesti bezbednosni organ i da traži od izvođača da mu vrati sve tajne podatke EU koje poseduje, s tim da on i posle raskida ugovora može da zadrži tajne podatke EU i nastavi da štiti njihovu tajnost, samo ako ima ovlašćenje za to.

Radi izvršenja ugovora, ugovorne strane mogu da pristupaju podacima stepena tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET koji se nalaze u prostorijama jednih ili drugih, pri čemu te posete organizuje nacionalni bezbednosni organ, odnosno ovlašćeni bezbednosni organ ili drugi nadležni bezbednosni organ države članice. Prilikom ovih poseta, svi posetioci moraju da imaju odgovarajuće uverenje o bezbednosnoj proveri, kao i opravdani razlog za pristup tajnim podacima EU, pri čemu će se dozvoliti pristup samo onim tajnim podacima EU koji su u vezi sa svrhom posete.

Za transport tajnih podataka EU i njihov prenos elektronskim sredstvima ugovorne strane su dužne da primenjuju posebne procedure[14] u skladu sa nacionalnim zakonodavstvom, odobrene kriptografske proizvode i posebne procedure[15] u slučaju vanrednih situacija.

U slučaju da se tajni podaci EU transportuju kao teret, postoje određena pravila koja ugovorne strane moraju poštovati: bezbednost treba da bude garantovana tokom celog transporta od mesta porekla do konačnog odredišta; stepen tajnosti pošiljke se određuje na osnovu najvišeg stepena tajnosti materijala koji ona sadrži; preduzeća koja pružaju uslugu transporta moraju da poseduju uverenje o bezbednosnoj proveri pravnog lica za odgovarajući stepen, a osoblje koje rukuje pošiljkom mora da bude bezbednosno prove-

[14] Odluka Saveta 2013/488/EU – Prilog III – Upravljanje tajnim podacima.

[15] Odluka Saveta 2013/488/EU – Prilog IV – Zaštita tajnih podataka EU sa kojima se postupa u komunikaciono-informacionim sistemima.

reno; pravac kretanja treba da bude kroz države članica kad god je to moguće, a pravci kretanja koji bi prolazili kroz države koje nisu članice treba da se preduzimaju samo ako ih odobri nacionalni bezbednosni organ, odnosno ovlašćeni bezbednosni organ ili drugi nadležni bezbednosni organ države pošiljaoca i države primaoca; pre svakog prekograničnog kretanja materijala stepena tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ili SECRET UE/EU SECRET, pošiljalac treba da sastavi plan transporta koji odobrava nacionalni bezbednosni, odnosno ovlašćeni bezbednosni organ ili drugi nadležni bezbednosni organ; u slučaju da je izvođač iz treće države, tajni podaci se prenose u skladu sa merama bezbednosti koje dogovaraju Sekretarijat i nacionalni organ, odnosno ovlašćeni bezbednosni organ treće države u kojoj je izvođač registrovan.

Kada je reč o pristupu tajnim podacima EU koji sadrže stepen tajnosti RESTRIENT UE/EU RESTRICTED izvođač ne mora da poseduje uverenja o bezbednosnoj proveri pravnih lica i fizičkih lica za izvođača i njegovo osoblje. Sekretarijat će razmotriti svaki odgovor na poziv za učešće na tenderu za ugovore koji zahtevaju pristup tajnim podacima EU stepena RESTRIENT UE/EU RESTRICTED, nezavisno od toga da li postoje zahtevi za uverenja o bezbednosnoj proveri pravnih i fizičkih lica.

Takođe, Sekretarijat može, u saradnji sa nacionalnim bezbednosnim organom, odnosno ovlašćenim bezbednosnim organom ili drugim nadležnim bezbednosnim organom države članice, da sprovede inspekciju objekta izvođača na osnovu ugovornih odredbi, kako bi proverio da li su uspostavljene odgovarajuće bezbednosne mere za zaštitu tajnih podataka EU stepena tajnosti RESTRIENT UE/EU RESTRICTED, u skladu sa zahtevima definisanim u ugovoru. Ukoliko to propisuje nacionalno zakonodavstvo, Sekretarijat će obavestiti o ugovorima koji sadrže tajne podatke stepena RESTRIENT UE/EU RESTRICTED, nacionalni bezbednosni organ, odnosno ovlašćeni bezbednosni organ ili drugi nadležni bezbednosni organ države članice.

Pravni okvir u Republici Srbiji

Stanje pravnog okvira

U skladu sa propisima u Republici Srbiji, organ javne vlasti može da dostavi tajne podatke drugom licu (pravnom ili fizičkom) na osnovu ugovornog odnosa pod određenim uslovima: da ispunjava određene organizacione i tehničke uslove utvrđene zakonom[16] i podzakonskim aktima donetim na osnovu zakona; da je za njega izvršena bezbednosna provera i izdat odgovarajući sertifikat (izdaje se na osnovu zahteva i ispunjenosti određenih uslova – da je sedište registrovano na teritoriji Republike Srbije; da obavlja delatnost u skladu sa članom 8. Zakona o tajnosti podataka; da je nadležni organ izvršio bezbednosnu proveru; da se ne nalazi u postupku likvidacije ili stečaja; da nije kažnjeno merom zabrane vršenja delatnosti i da uredno plaća poreze i doprinose); da je pisanom izjavom potvrdio da je upoznat sa zakonom i drugim propisima koji uređuju rad sa tajnim podacima, da se obaveže da će sa tajnim podacima postupati u skladu sa tim propisima i da mu je potreban pristup tajnim podacima radi realizacije poslova predviđenih konkretnim ugovorom.

[16] Члан 46. Закона о тајности података („Службени гласник РС”, бр. 104/09).

Uredbom o posebnim merama zaštite tajnih podataka, koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa, propisano je da lice kome organ javne vlasti na osnovu ugovora dostavlja tajne podatke treba da ispunjava organizacione uslove koji podrazumevaju: dobro organizovan proces rada, zaštitu pristupa tajnim podacima, zaštitu od neovlašćenog korišćenja tajnih podataka, određivanje odgovornog lica zaduženog za sprovođenje mera zaštite i utvrđivanje postupka u slučaju vanrednih i hitnih situacija. Pored organizacionih uslova, u skladu sa Uredbom, ovo lice mora da ispunjava i određene tehničke uslove, kao što su: fizičko-tehnička zaštita prostora, odnosno prostorija u kojima se čuvaju tajni podaci; protivpožarna zaštita; zaštita tajnih podataka prilikom prenošenja i dostavljanja izvan prostorija u kojoj se čuvaju; transport tajnih podataka; obezbeđivanje i zaštita informaciono-telekomunikacionih sredstava kojima se vrši prenošenje i dostavljanje tajnih podataka i sprovođenje propisanih mera kriptozaštite.

Pre započinjanja postupka pregovora izbora ugovarača, zaključenja i izvršenja ugovora, organ javne vlasti mora da donese odluku kojom se određuje predmet ugovora, stepen tajnosti podataka koje će taj ugovor da sadrži i radnje koje je potrebno da se preduzmu radi njegovog zaključenja i izvršenja, a nakon toga sledi upućivanje poziva ponuđačima za učešće u postupku zaključenja poverljivog ugovora na način utvrđen propisom kojim se uređuju javne nabavke[17].

Pregovori i postupak za izbor ugovorača sprovode se u prostoriji za čuvanje tajnih podataka koja treba da ispunjava posebne fizičko-tehničke mere zaštite tajnih podataka,[18] pri čemu se u radu sa tajnim podacima u potpunosti primenjuju uslovi predviđeni Zakonom i odgovarajućim podzakonskim aktima.

Tokom postupka vođenja pregovora i izbora ugovarača može da nastane situacija kada je neophodno da se izvrši razmena tajnih podataka između organa javne vlasti i ponuđača koji nema registar tajnih podataka. U tom slučaju uspostaviće se *privremeni registar tajnih podataka* u okviru registra tajnih podataka u organu javne vlasti ili kod tog ponuđača, koji će biti zatvoren po okončanju postupka izbora i uspostavljen novi registar. Po okončanju postupka izbora, lice koje je izabrano za ugovarača dužno je da uspostavi registar tajnih podataka.

Ispunjenost organizacionih i tehničkih uslova za čuvanje tajnih podataka označenih stepenom tajnosti „DRŽAVNA TAJNA", „STROGO POVERLjIVO", ili „POVERLjIVO", utvrđuje ovlašćeno lice organa javne vlasti pre zaključenja poverljivog ugovora. Ovo lice je dužno da izvrši određenu proveru i o tome obavesti rukovodioca organa javne vlasti.

Provera koju ovlašćeno lice vrši obuhvata više različitih segmenata: da li je pristup tajnim podacima fizičkih lica koja će obavljati poverene poslove neophodan radi realizacije poslova koji se predviđaju ugovorom (utvrđivanje tzv. Lista – treba da zna:); da li ugovarač ima sertifikat koji odgovara najmanje onom stepenu tajnosti kojim su označeni tajni podaci koji se dostavljaju i da li su za fizička lica koja obavljaju poverene poslove izdati sertifikati; da li je prostor, odnosno prostorija ugovarača u kojoj će se čuvati tajni podaci, opremljena u skladu sa propisom koji uređuje posebne mere fizičko-tehničke zaštite tajnih podataka; da li postoji akt ugovarača o postupanju sa tajnim podacima, merama zaštite tajnih podataka kao i postupanju sa tajnim podacima u slučaju vanrednih situacija; da li su označeni ormari i kasa u kojima se čuvaju i deponu-

[17] Čl. 127. do 131. Zakona o javnim nabavkama („Службени гласник РС", бр. 124/12) definišu postupak javnih nabavki u oblasti odbrane i bezbednosti na koje se ne primenjuju odredbe Zakon o javnim nabavkama.

[18] Уредба о посебним мерама физичко-теничке заштите тајних података („Службени гласник РС", бр. 97/11 у примени од 29.12.2011. године).

ju tajni podaci; kako se pristupa tajnim podacima i kako se oni koriste i uništavaju; kako se evidentiraju, čuvaju i arhiviraju tajni podaci; kako se vode i čuvaju propisane evidencije, a posebno evidencija o pristupu tajnim podacima; kako se tajni podaci umnožavaju, pakuju i dostavljaju unutar i van bezbednosne zone; da li postoji evidencija ulaza i izlaza lica i vozila; kako se koriste bezbednosne propusnice i posebne bezbednosne propusnice i način funkcionisanja fizičkog i elektronskog sistema za obezbeđenje objekata i prostora; kako se čuvaju sertifikati; kako se obavlja prijem, obrada, prenos, čuvanje, arhiviranje i uništavanje tajnih podataka u elektronskoj formi i način čuvanja kripto-zaštite i poverljivog ugovora koji sadrži tajne podatke.

Pre nego što izabrani ugovarač pristupi zaključenju poverljivog ugovora koji sadrži tajne podatke označene stepenom tajnosti „DRŽAVNA TAJNA"19, „STROGO POVERLjIVO", ili „POVERLjIVO", on je dužan da sačini uputstvo o merama zaštite tajnih podataka koje će da sadrži njegove obaveze: imenovanje lica koje će biti odgovorno za sprovođenje mera zaštite tajnih podataka; održavanje neprekidne veze sa ovlašćenim licem ili drugim licem organa javne vlasti odgovornim za nadzor nad izvršenjem poverljivog ugovora; da ne umnožava tajne podatke iz poverljivog ugovora, osim ako je to predviđeno ugovorom ili uz saglasnost organa javne vlasti sa kojim je zaključen poverljivi ugovor; obezbeđivanje podataka o licima koja će imati pristup tajnim podacima iz poverljivog ugovora; vođenje evidencije zaposlenih koji imaju sertifikat, a koji će učestvovati u izvršenju ugovora; da o uočenim nepravilnostima u vezi sa zaštitom tajnih podataka ili njihovom otkrivanju neovlašćenom licu bez odlaganja o tome obavesti organ javne vlasti; da omogući organu javne vlasti da za vreme izvršenja poverljivog ugovora vrši kontrolu preduzetih mera zaštite tajnih podataka iz tog ugovora; da upozna podugovarača sa merama zaštite tajnih podataka koje je dužan da sprovede; da koristi tajne podatke kojima ima pristup po osnovu poverljivog ugovora samo u svrhe određene tim ugovorom; da po izvršenju ugovora vrati poverljive podatke organu javne vlasti; da obezbedi uništavanje tajnih podataka u skladu sa propisom kojim su uređene posebne mere fizičko-tehničke zaštite tajnih podataka; da obezbedi da se zaposleni upoznaju sa merama zaštite tajnih podataka i da se pridržavaju tih mera; da izradi spisak tajnih podataka i oblasti u kojima mogu nastati tajni podaci. Poverljiv ugovor koji zaključuju organ javne vlasti i izabrani ugovarač mora da sadrži mere zaštite tajnih podataka i ugovarač je dužan da se u toku izvršenja ugovora pridržava obaveza sadržanih u uputstvu.

Prenos i predaja tajnih podataka ugovaraču prilikom zaključenja, odnosno izvršenja ugovora, vrši se u skladu sa propisima koji uređuju posebne mere fizičko-tehničke zaštite tajnih podataka i posebne mere zaštite tajnih podataka u informaciono-telekomunikacionim sistemima[20].

Ako strano lice (fizičko ili pravno) pristupa prostorijama ugovarača sa kojim je organ javne vlasti zaključio ugovor i ako takav pristup podrazumeva i pristup tajnim podacima, ugovarač mora da poseduje odobrenje tog organa javne vlasti, osim ako međunarodnim ugovorom nije drugačije predviđeno.

U slučaju da dođe do raskida poverljivog ugovora, ugovarač je dužan da bez odlaganja vrati dokumenta i druge materijale koji sadrže tajne podatke organu javne vlasti od koga ih je dobio, kao i da zatvori registar tajnih podataka, osim ako se taj registar ne vodi po nekom drugom osnovu.

[19] Pristup dokumentima stepena tajnosti „DRŽAVNA TAJNA" koji odgovara stepenu tajnosti „TOP SECRET" nije predviđen Odlukom Saveta 2013/488/EU.

[20] Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Службени гласник РС", бр. 53/11).

Neophodnost usklađivanja i dorade pravnih akata Republike Srbije

Otvaranje pregovora Republike Srbije sa EU i aktivnosti koje se sprovode u okviru Programa Partnerstvo za mir, kao i promene poslovnog ambijenta na domaćem i međunarodnom tržištu stvorili su preduslove za značajnije učešće naših privrednih subjekata u naučnim, tehnološkim, informacionim projektima u regionu i šire, ekonomskoj saradnji sa najrazvijenijim državama, na tenderima koje raspisuju pojedine evropske i svetske organizacije i njihove članice sa kojima Republika Srbija ima potpisane bilateralne sporazume, uz punu ispunjenost svih predviđenih kriterijuma i standardizaciju postupaka za učešće na tenderima.

Do danas, Republika Srbija je potpisala ukupno devet sporazuma o razmeni i zaštiti tajnih podataka. Sporazumi sa NATO21, EU22, Slovačkom23 i Bugarskom24 su i ratifikovani, dok se ratifikacija očekuje za sporazume potpisane sa Češkom (2013. god.), Slovenijom (2013. god.), Bosnom i Hercegovinom (2013. god.), Makedonijom (2014. god.) i Španijom (2014. god.).

Zaštita tajnih podataka u Srbiji predstavlja proces koji je u toku i za čiju adekvatnu primenu je neophodan novi bezbednosni pristup, odnosno reforma sistema državne uprave i sektora bezbednosti i prevashodno edukacija zaposlenih u državnoj upravi. Reformu rada sa tajnim podacima, a posebno u segmentu industrijske bezbednosti, nemoguće je ostvariti bez normativno uređene saradnje između organa državne uprave i drugih pravnih subjekata, pre svega u smislu sprovođenja postupka sertifikacije i ispunjenosti odgovarajućih organizaciono-tehničkih uslova za rukovanje, odnosno rad sa tajnim podacima i primene svih propisanih mera zaštite tajnih podataka. Serifikovanje privrednih subjekata omogućava njihovo učešće na raspisanim tenderima u drugim državama sa kojima Srbija ima zaključene i ratifikovane međunarodne sporazume o uzajamnoj razmeni i zaštiti tajnih podataka, ali i ugovaranje poslova sa Generalnim sekretarijatom.

Pravno lice dobija sertifikat pod uslovima koji su propisani zakonom i u slučaju kada sklapa poverljiv ugovor sa organom javne vlasti. Međutim, osim propisivanja shodne primene odredaba uredbe o industrijskoj bezbednosti na zaključenje i izvršenje poverljivog ugovora koji sadrži strane tajne podatke, osim ako zaključenim međunarodnim sporazumom nije drugačije predviđeno, nije razrađena detaljnija procedura za sertifikovanje domaćih kompanija kako bi bile konkurentne i u mogućnosti da učestvuju na tenderima u zemljama članicama EU i za kompanije koje imaju interes za rad na poslovima NATO i na koji način ova pravna lica mogu da se upišu u registar poslovnih subjekata NATO. U slučaju kada pravno lice iskazuje interes za sklapanje poverljivog ugovora sa organom javne vlasti, taj organ upućuje zahtev KSNBiZTP-u za sertifikovanje pravnog lica, a u slučaju kada pravno lice sklapa ugovor sa organom javne vlasti članice EU/NATO, telo dr-

[21] Закон о потврђивању Споразума између Владе Републике Србије и Организације северноатлантског пакта о безбедности информација и кодекса о поступању („Службени гласник РС” – Међународни уговори бр. 6/11).

[22] Закон о потврђивању Споразума између Републике Србије и Европске уније о безбедносним процедурама за размену и заштиту тајних података („Службени гласник РС” – Међународни уговори бр. 1/12).

[23] Закон о потврђивању Споразума између Владе Републике Србије и Владе Словачке Републике о узајамној заштити тајних података („Службени гласник РС” – Међународни уговори бр. 6/12).

[24] Закон о потврђивању Споразума између Владе Републике Србије и Владе Републике Бугарске о размени и узајамној заштити поверљивих информација у области одбране („Службени гласник РС” – Међународни уговори бр. 1/10, 4/13 – други пропис).

žave članice nadležno za poslove nacionalne bezbednosti trebalo bi da uputi zahtev nadležnom telu Republike Srbije, odnosno KSNBiZTP.

Međutim, procedura ne predviđa mogućnost sertifikovanja pravnog lica ukoliko ono ima interes za rad na poslovima EU/NATO i ukoliko želi da se uključi u registar poslovnih subjekata NATO i unapred sertifikuje i pripremi uslove za učešće u poverljivim tenderima. Naime, pravnim licima Republike Srbije trebalo bi omogućiti da se unapred pripreme i budu već kvalifikovani za sklapanje poverljivih ugovora, kako bi bili konkurentni na tržištu. U tom slučaju trebalo bi da se iznađe model da pravno lice može samostalno, uz određenu novčanu nadoknadu, da aplicira za izdavanje sertifikata. Jedan od modela koji bi mogao da bude razmotren u prevazilaženju trenutnih problema, a koji se već pokazao efikasnim u pojedinim članicama EU i NATO, jeste da pravno lice za dobijanje sertifikata podnese zahtev KSNBiZTP-u preko privredne komore ili ministarstva nadležnog za trgovinu.

Da bi pravna lica mogla da se specijalizuju za pružanje usluga ili proizvodnju u oblasti odbrane i nacionalne bezbednosti u zemljama EU i NATO, ali i u samoj Srbiji, potrebno je da primene sve propisane mere zaštite tajnih podataka koje ne podrazumevaju samo fizičku, nego i personalnu i informacionu bezbednost. U suprotnom, domaće kompanije naći će se u situaciji u kojoj neće moći da sklapaju ugovore sa organima javne vlasti Republike Srbije. U tom smislu, neophodno je u što kraćem roku izraditi uputstvo o industrijskoj bezbednosti, sa jasnim smernicama i veoma konkretnim i preciznim uputstvima o merama bezbednosti i zaštite koje pravna lica moraju da primenjuju u odnosu na stepen tajnosti ugovora koje će potencijalno sklapati u budućnosti. Takođe, neophodno je u što kraćem roku zakonski regulisati oblast informacione bezbednosti, urediti oblast kriptozaštite tajnih podataka i nadležnosti u oblasti kriptozaštite na nacionalnom nivou i doneti strategiju sajber bezbednosti, te odrediti organ nadležan za sprovođenje sajber bezbednosti.

Inspekcijski nadzor, kojim bi se utvrdio stepen ne/primenjivanja Zakona o tajnosti podataka, potrebno je sprovesti u što kraćem roku u svim državnim organima i organima državne uprave, kao i prema pravnim licima koja već imaju sklopljene poverljive ugovore sa organima javne vlasti. Postupak pripreme pravnih lica i samog sertifikovanja treba da bude sproveden u tesnoj i koordiniranoj saradnji KSNBiZTP, ministarstva nadležnog za trgovinu i privredne komore.

Inače, KSNBiZTP je, pored zaštite nacionalnih tajnih podataka i stranih tajnih podataka, nadležna i za zaštitu tajnih podataka stranih zemalja, usaglašavanje bilateralnih sporazuma u oblasti razmene tajnih podataka, izdavanje sertifikata za pristup tajnim podacima, kontrolu i stručni nadzor nad primenom Zakona o tajnosti podataka i potpisanih međunarodnih sporazuma, kao i za obuku kadrova organa javne vlasti u oblasti zaštite tajnih podataka. Politika zaštite tajnih podataka i inspekcijski nadzor nad primenom Zakona o tajnosti podataka u nadležnosti je Ministarstva pravde.

Ipak, zbog navedenih anomalija i otpora u primeni Zakona o tajnosti, sam sistem zaštite tajnih podataka još uvek nije do kraja uređen u Srbiji i predstavlja ozbiljnu potencijalnu pretnju sistemu nacionalne bezbednosti, i istovremeno podriva međunarodni ugled naše zemlje. Pored same primene mera propisanih Zakonom, neophodna je edukacija i razvijanje svesti zaposlenih u organima javne vlasti, i sprovođenje kaznene politike koja je propisana zakonima Republike Srbije. Posebnu pažnju u narednom periodu potrebno je posvetiti zaštiti podataka u telekomunikaciono-informacionim sistemima i urediti oblast informacione bezbednosti, gde se nadležnosti organa prepliću, zbog čega je neophodna jasna politika države i donošenje strategije iz ove oblasti.

Dosledna primena Zakona o tajnosti podataka i podzakonskih akata koji propisuju mere zaštite tajnih podataka predstavlja i osnovni preduslov pravnih lica iz Srbije za razvoj i jačanje odbrambene industrije. Naime, Administrativni sporazum Ministarstva odbrane Republike Srbije i Evropske odbrambene agencije (EDA) usledilo je nakon potpisivanja sporazuma sa EU o razmeni tajnih podataka i o uključivanju Srbije u operacije zajedničke bezbednosne i odbrambene politike. Pod uslovom da pravna lica ispunjavaju uslove propisane Zakonom o tajnosti podataka, sporazum sa EDA omogućiće izlazak našim kompanijama na evropsko tržište, učestvovanje u zajedničkim projektima sa državama članicama EU u oblasti istraživanja i razvoja naoružanja i doprineće sveukupnom razvoju postojećih kapaciteta naše namenske industrije. Ovaj sporazum omogućava kompanijama i pristup fondovima koji mogu da se iskoriste za unapređenje istraživanja, modernizaciju i razvoj odbrambene industrije, kao i povećanje kapaciteta NVO i ukupnog sistema odbrane.

Član 4. Sporazuma između Republike Srbije i Evropske unije o uspostavljanju okvira za učešće Republike Srbije u operacijama Evropske unije za upravljanje krizama[25] propisuje da će Srbija preduzeti odgovarajuće mere kako bi obezbedila da tajni podaci EU budu zaštićeni u skladu sa bezbednosnim pravilima Saveta EU, koja su sadržana u Odluci Saveta 2001/264/EU od 19. marta 2001, kojom se usvajaju bezbednosna pravila Saveta i, u skladu sa daljim smernicama koje su izdali nadležni organi, uključujući komandanta operacije EU u pogledu vojne operacije EU za upravljanje krizama ili šefa misije EU u vezi sa civilnom operacijom EU za upravljanje krizama.

Takođe, u slučajevima kada EU ili neka od njenih članica, sa jedne, i Republika Srbija, sa druge strane, zaključe sporazum o bezbednosnim procedurama za razmenu tajnih podataka, odredbe takvog sporazuma primenjuju se u kontekstu operacije EU za upravljanje krizama. Ovakva odredba zahteva sprovođenje čitavog niza mera i postojanje kompletne strukture koja će omogućiti ispunjavanje ove obaveze, naročito prilikom učešća u EU misijama. Sa druge strane, pristup i razmena tajnih podataka između Srbije i EU propisana je i Sporazumom između Republike Srbije i Evropske unije o bezbednosnim procedurama za razmenu i zaštitu tajnih podataka[26].

Pitanje industrijske bezbednosti usko je povezano sa pitanjem odbrane i bezbednosti, ali i sa pitanjem trgovina naoružanjem i vojnom opremom. Naime, jedno od veoma važnih pitanja u procesu pregovora i usklađivanja propisa biće i pitanje javnih nabavki naoružanja i vojne opreme, kao i izvođenja radova i pružanja usluga u oblasti odbrane i bezbednosti.

Naime, Direktiva 2009/81/EC[27] Evropskog parlamenta i Saveta o usklađivanju postupka nabavke za određene ugovore o radovima, ugovora o nabavkama robe i ugovora

[25] Закон о потврђивању Споразума између Републике Србије и Европске уније о успостављању оквира за учешће Републике Србије у операцијама Европске уније за управљање кризама („Службени гласник РС“ – Међународни уговори бр. 1/12); Agreement between the European Union and the Republic of Serbia establishing a framework for the participation of the Republic of Serbia in European Union crisis management operations, Official Journal of the European Union, L 163, 23 June 2011, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv :OJ.L_.2011.163.01.0001.01.ENG

[26] „Службени гласник РС” – Међународни уговори бр. 1/12

[27] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0081

o uslugama u oblasti odbrane i bezbednosti, koje sklapaju javni naručioci ili naručioci, izmenjena direktivama 2004/17/EZ i 2004/18/EZ, predviđa postepeno uspostavljanje evropskog tržišta odbrambene opreme, kao ključne pretpostavke evropske odbrambene tehnološke i industrijske baze, kao i razvoja vojnih sposobnosti nužnih za sprovođenje evropske bezbednosne i odbrambene politike.

Direktiva 2009/81/EC propisuje obavezu država članica EU za sprovođenje javnih tendera prilikom nabavke dobara ili usluga čija vrednost prelazi 412.000,00 eura, odnosno 5 miliona eura za nabavku usluga. Naravno, državama je ostavljena i mogućnost sprovođenja poverljivih nabavki pod određenim uslovima. Naime, sklapanje ugovora iz oblasti predviđenih ovog direktivom ne mora biti javno u slučajevima kada je to opravdano razlozima javne bezbednosti ili neophodno radi zaštite bitnih bezbednosnih interesa država članica. To može biti slučaj sa ugovorima u oblasti odbrane i bezbednosti, kada su bezbednosni zahtevi u tolikoj meri poverljivi i važni za nacionalni suverenitet da čak ni specifične odredbe ove direktive nisu dovoljne za zaštitu tih interesa. Direktivom se, kao posebno osetljive, izuzimaju nabavke koje pružaju obaveštajno-bezbednosne službe ili nabavke svih vrsta obaveštajnih aktivnosti, uključujući i protivobaveštajne aktivnosti. Takođe, izuzete su i druge posebno osetljive nabavke koje zahtevaju visok stepen tajnosti, kao što su nabavke koje se obavljaju radi zaštite granica, borbe protiv terorizma ili organizovanog kriminala, nabavke vezane za šifrovanje ili namenjene posebno za tajno delovanje ili druge podjednako osetljive aktivnosti koje sprovodi policija i snage bezbednosti. S obzirom na specifičnost sektora odbrane i bezbednosti, nabavka opreme, kao i radova i usluga jedne vlade od druge treba da bude izuzeta od primene Direktive.

Istovremeno, ono što je najbitnije za oblast industrijske bezbednosti u smislu sertifikovanja pravnih lica jeste da Direktiva predviđa mogućnost da javni naručioci mogu prethodno zahtevati garanciju od ugovarača ili proizvođača za zaštitu poverljivih podataka od nedozvoljenog pristupa, kao i dovoljno podataka o njihovoj sposobnosti da to i učine, što znači da mogu da konkurišu ako već poseduju bezbednosni sertifikat.

Umesto zaključka – zapažanja i preporuke

Zaštita tajnih podataka, koja je na veoma visokom mestu na agendi EU, jedna je od najznačajnijih oblasti reforme zakonodavstva i usklađivanja sa pravnim nasleđem EU i međunarodnim standardima.

Sporost u primeni Zakona o tajnosti podataka i podzakonskih akata kojima se propisuju mere zaštite tajnih podataka odražava se na nacionalnu bezbednost, ali i sve druge aspekte svakodnevnog života i rada, pa i na međunarodni ugled Republike Srbije. Svest rukovodilaca srednjeg nivoa i zaposlenih u organima državne uprave o značaju poštovanja propisa o zaštiti tajnih podataka u Srbiji i dalje nije na zadovoljavajućem nivou.

Industrijska bezbednost, koja zauzima posebno značajno mesto u oblasti zaštite tajnih podataka, podrazumeva upotrebu mera i procedura kojima se sprečava kompromitovanje i otkrivanje tajnih podataka, a kojima raspolaže ugovarač ili podugovarač od trenutka započinjanja pregovaračkog procesa, tokom realizacije ugovora i nakon završenog posla. Propisima koji su doneti u Republici Srbiji nije regulisano pitanje podugovarača i njihovog sertifikovanja, u slučaju kada je za realizaciju ugovora potrebno razmeniti tajne podatke i sa podugovara-

čem. U ovom delu nedostaje i čitav set proaktivnog pristupa u regulisanju tzv. poverljivih ugovornih odnosa sa konzorcijumima, holdinzima, javnim i drugim preduzećima, koja čine sastavni deo kritične infrastrukture Srbije, a u koje je ušao „strani kapital".

Primena propisa koji se odnose na zaštitu tajnih podataka i industrijsku bezbednost omogućava razmenu tajnih podataka između pravnih lica i organa javne vlasti (Srbije i EU) u slučajevima kada ugovor sadrži tajne podatke ili druge poverljive informacije. Bezbednosni sertifikat za pravno lice predstavlja preduslov za sklapanje poverljivih ugovora kojima se razmenjuju tajni podaci između organa javne vlasti i pravnog lica, a sertifikatom se potvrđuje ispunjenost određenih kriterijuma koji omogućavaju primenu propisanih mera i standarda za zaštitu tajnih podataka.

Kako bi domaće kompanije bile ravnopravni učesnici u postupcima sklapanja poverljivih ugovora, na putu ka punopravnom članstvu u EU, u domenu industrijske bezbednosti, pored do sada učinjenog, neophodno je:

– inicirati izmene i dopune Zakona o tajnosti podataka, kako bi se stvorila platforma za njegovu efikasniju primenu;

– otpočeti sa punom primenom Zakona o tajnosti podataka u organima državne uprave i svim javnim preduzećima koja imaju sklopljene poverljive ugovore sa organima javne vlasti;

– doneti priručnik za industrijsku bezbednost, kojim će se pravnim licima pojasniti procedura sertifikovanja i u jednom dokumentu predstaviti neophodni uslovi koje pravno lice treba da ispuni da bi bilo sertifikovano za sklapanje poverljivih ugovora;

– omogućiti pravnim licima sertifikovanje za sklapanje poverljivih ugovora i pre raspisivanja poverljive nabavke, s obzirom na to da postoji realna mogućnost da posedovanje odgovarajućeg sertifikata bude preduslov za učešće na tenderu;

– obezbediti permanentnu edukaciju lica koja rade na zaštiti tajnih podataka i koja rukuju tajnim podacima;

– razmotriti mogućnost da obavljanje inspekcijskih poslova u oblasti primene Zakona o tajnosti podataka bude u nadležnosti Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, s obzirom na to da je to jedini organ koji poseduje ekspertizu u oblasti zaštite tajnih podataka u svim njenim segmentima;

– doneti Zakon o informacionoj bezbednosti i Strategiju sajber bezbednosti;

– regulisati oblast kriptozaštite i nadležnosti organa u ovoj oblasti.

Literatura

1. Bareš, P., Хеуристика и законска регулатива у области заштите тајних података у функцији едукације система одбране, *Војнотехнички гласник*, Београд, 2014.

2. Група аутора, *Систем заштите тајних података,* Мисија ОЕБС у Србији, Београд 2012. год.

3. Група аутора, *Тајност података, заштита и слободан приступ информацијама,* Правни информатор, Intermex, Београд, 2010.

4. Група аутора, *Приступ информацијама од јавног значаја и заштита тајних података*, Зборник радова, Мисија ОЕБС у Србији, Београд, 2012.

5. Ковачевић, Н., *Заштита тајних података*, Канцеларија Савета за националну безбедност и заштиту тајних података, Београд, 2013.

Propisi u Republici Srbiji

1. Закон о тајности података, *Службени гласник Републике Србије*, бр. 104/09

2. Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа, *Службени гласник Републике Србије*, бр. 63/13

3. Уредба о начину и поступку означавања тајности података, односно докумената, *Службени гласник Републике Србије*, бр. 8/11

4. Уредба о посебним мерама физичко-техничке заштите тајних података, *Службени гласник Републике Србије*, бр. 97/11

5. Уредба о посебним мерама надзора над поступањем са тајним подацима, *Службени гласник Републике Србије*, бр. 90/11

6. Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима, *Службени гласник Републике Србије*, бр. 53/11

7. Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима, *Службени гласник Републике Србије*, бр. 89/10

8. Закон о слободном приступу информацијама од јавног значаја, *Службени гласник Републике Србије*, бр. 120/04 , 54/07 , 104/09 , 36/10

9. Закон о заштити података о личности, *Службени гласник Републике Србије*, бр. 97/08, 104/09

10. Закон о потврђивању Споразума између Владе Републике Србије и Организације северноатлантског пакта о безбедности информација и кодекса о поступању, *Службени гласник Републике Србије*, (Међународни уговори) бр. 6/11

11. Закон о потврђивању Споразума између Републике Србије и Европске уније о безбедносним процедурама за размену и заштиту тајних података, *Службени гласник Републике Србије*, (Међународни уговори) бр. 1/12)

12. Закон о потврђивању Споразума између Владе Републике Србије и Владе Словачке Републике о узајамној заштити тајних података, *Службени гласник Републике Србије*, (Међународни уговори) бр. 6/12

13. Закон о потврђивању Споразума између Владе Републике Србије и Владе Републике Бугарске о размени и узајамној заштити поверљивих информација у области одбране, *Службени гласник Републике Србије*, (Међународни уговори) бр. 1/10, 4/13

14. Закон о потврђивању Споразума између Републике Србије и Европске уније о успостављању оквира за учешће Републике Србије у операцијама Европске уније за управљање кризама, *Службени гласник Републике Србије*, (Међународни уговори) бр. 1/12

Propisi Evropske unije

1. Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488 /EU),
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1400 35102725&uri=CELEX:32013 D0488

2. Council Decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC) (OJ L 101, 11.4. 2001, p. 1) amended by Council Decision 2004/194/EC of 10 February 2004 (OJ L 63 28.2.2004), Council Decision 2005/571/EC of 12 July 2005 (OJ L 193 23.7.2005), Council Decision 2005/952/EC of 20 December 2005 (OJ L 346 29.12.2005), Council Decision 2007/438/EC of 18 June 2007 (OJ L 164 26.6.2007),
http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1400350928118&uri=CELEX:320 07D0438

3. Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC
http://eur-lex. europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0081