

VODIČ ZA IMPLEMENTACIJU ZAKONA O TAJNOSTI PODATAKA



web: www.nsa.gov.rs

Prof.dr Goran D. Matić

Beograd, 2026. godina

SADRŽAJ

NEOPHODNI KORACI.....	2
SISTEM ZAŠTITE TAJNIH PODATAKA	3
PLAN ZAŠTITE TAJNIH PODATAKA U ORGANU JAVNE VLASTI	7
REGISTARSKI SISTEM	14
PERSONALNA BEZBEDNOST	17
FIZIČKA BEZBEDNOST.....	21
ADMINISTRATIVNA BEZBEDNOST	23
INDUSTRIJSKA BEZBEDNOST	26
UNUTRAŠNJA KONTROLA.....	28
STRUČNI NADZOR	32
PRIMERI LOŠE PRAKSE SISTEMA RADA SA TAJNIM	33
PODACIMA.....	33
GODIŠNJI IZVEŠTAJ O RADU SA TAJNIM PODACIMA U REPUBLICI	35
SRBIJI	35
POJMOVNIK O RADU SA TAJNIM PODACIMA	37
OBRASCI, MODELI ODLUKA I ZAHTEVA ZA IMPLEMENTACIJU	52
ZAKONA O TAJNOSTI PODATAKA	52
KATALOG PROPISA ZA RAD SA TAJNIM PODACIMA	53
O AUTORU.....	55

Podizanje bezbednosne svesti i kulture sa primarnim i težišnim zadatkom zaštite interesa Republike Srbije koji se odnose na nacionalnu i javnu bezbednost, unutrašnje i spoljne poslove Republike Srbije, odbranu, zaštitu ustavnog poretka, kao i ljudskih i manjinskih prava!

NEOPHODNI KORACI

Implementacija Zakona o tajnosti podataka u organu javne vlasti
(organizaciona bezbednost)

1. Procena stanja i bezbednosti
2. Donošenje normative za rad sa tajnim podacima
3. Određivanje rukovaoca tajnih podataka
4. Uspostavljanje i sprovođenje unutrašnje kontrole
5. Kreiranje liste «potrebno da zna» za zaposlene
6. Proces sertifikacije fizičkih i pravnih lica (poverljive nabavke)
7. Uspostavljanje opštih i posebnih mera zaštite tajnih podataka
8. Formiranje registra za rad sa tajnim podacima (stranim tajnim podacima)
9. Uspostavljanje sistema internih edukacije za rad sa tajnim podacima u organu javne vlasti
10. Uspostavljanje IKT sistema za rad sa tajnim podacima
11. Nadzor (stručni) od strane Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka
12. Inspekcijski nadzor Ministarstva pravde

PRIRUČNICI I SKRIPTE:

1. Osnove obrade i zaštite podataka
([https://nsa.gov.rs/extfile/sr/4326/Osnove obrade i zast TP .pdf](https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf))
2. Sistem zaštite tajnih podataka
([https://nsa.gov.rs/extfile/sr/1776/Sistem zastite tajnih podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf))
3. Postupak izdavanja bezbednosnog sertifikata
([https://nsa.gov.rs/extfile/sr/1464/Postupak izdavanja BS-skripta.pdf](https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja_BS-skripta.pdf))
4. Unutrašnja kontrola nad radom sa tajnim podacima
([https://nsa.gov.rs/extfile/sr/1761/Unutrasnja kontrola nad radom sa tp 1 .pdf](https://nsa.gov.rs/extfile/sr/1761/Unutrasnja_kontrola_nad_radom_sa_tp_1_.pdf))
5. Umanjivanje insajderske pretnje
([https://nsa.gov.rs/extfile/sr/1485/Umanjivanje insajderske pretnjeskripta .pdf](https://nsa.gov.rs/extfile/sr/1485/Umanjivanje_insajderske_pretnjeskripta_.pdf))

SISTEM ZAŠTITE TAJNIH PODATAKA

Sistem zaštite tajnih podataka osmišljen je prvenstveno sa ciljem da se obezbedi usaglašenost sa zakonskim i institucionalnim zahtevima, da se realizuje koncept „zaštite nacionalne bezbednosti“ i uspostavi međunarodna saradnja, kao i visoki standardi kvaliteta korporativnog upravljanja i adekvatnog ponašanja, te da se osigura stvarna odgovornost i dobri sistemi zaštite tajnih podataka.

SISTEM ZAŠTITE TAJNIH PODATAKA OBUHVATA:

1. REGISTARSKI SISTEM;
2. PERSONALNU BEZBEDNOST;
3. ADMINISTRATIVNU BEZBEDNOST;
4. FIZIČKU BEZBEDNOST;
5. INFORMACIONU BEZBEDNOST;
6. INDUSTRIJSKU BEZBEDNOST;
7. KONTROLU I NADZOR.

REGISTARSKI SISTEM predviđa rukovanje tajnim podacima samo u uređenom sistemu koji mora biti uspostavljen u skladu sa propisima i standardima iz oblasti zaštite tajnih podataka.

PERSONALNA BEZBEDNOST obuhvata niz procedura čiji je osnovni cilj da se utvrdi da li neko lice može biti ovlašćeno da dobije pristup tajnim podacima, a da pri tome ne predstavlja neprihvatljiv rizik za nacionalnu bezbednost.

ADMINISTRATIVNA BEZBEDNOST je adekvatna i efikasna klasifikacija i zaštita zvaničnih informacija koje zahtevaju zaštitu u interesu nacionalne bezbednosti kao i njihova deklasifikacija kada više ne zahtevaju zaštitu.

FIZIČKA BEZBEDNOST predstavlja primenu fizičkih i tehničkih mera zaštite radi sprečavanja neovlašćenog pristupa tajnim podacima i u suštini predstavlja kombinaciju bezbednosnih procedura i tehničkih standarda koji se zasnivaju na preporukama, proceni i praksi.

INFORMACIONA BEZBEDNOST predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT(IKT- informaciono komunikacione tehnologije) sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.

INDUSTRIJSKA BEZBEDNOST predstavlja primenu mera radi obezbeđenja zaštite tajnih podataka od strane izvođača ili podizvođača u pregovorima koji prethode zaljučivanju ugovora i tokom celog veka trajanja tajnih/poverljivih ugovora. Izvršenje poverljivog ugovora podrazumeva sve radnje preduzete nakon njegovog zaključenja do izvršenja ugovornih obaveza, odnosno do prestanka njegovog važenja.

KONTROLA I NADZOR – podrazumeva posebne mere nadzora nad postupanjem sa tajnim podacima u organu javne vlasti. Posebne mere nadzora obuhvataju neposredan uvid, odgovarajuće provere i razmatranje podnetih izveštaja u vezi sa sprovođenjem svih mera zaštite tajnih podataka ili jedne, odnosno određenih mera zaštite tajnih podataka i sprovode se u okviru unutrašnje kontrole organa javne vlasti.

- **UNUTRAŠNJA KONTROLA** – rukovodilac organa javne vlasti a u slučaju potrebe sistematizuje se posebno radno mesto ili se zadužuje posebna organizaciona jedinica u sastavu organa javne vlasti
- **KONTROLA I STRUČNI NADZOR** – Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka
- **KONTROLA I INSPEKCIJSKI NADZOR** - Ministarstvo nadležno za poslove pravosuđa



Obaveze koje proizilaze iz Zakona o tajnosti podataka - Zakon o tajnosti podataka koji je stupio na snagu 2010. godine, uneo je u pravni sistem Republike Srbije jedan nov sistemski pristup utemeljen na bezbednosnim, pravnim i tehničkim

standardima koji se primenjuju u Evropskoj uniji, NATO, Ruskoj Federaciji, SAD, Narodnoj Republici Kini, ali i zemljama u okruženju koje su ga implementirale u svoje pravne sisteme.

Sam Zakon o tajnosti podataka je nametnuo određene obaveze organima javne vlasti koje se ogledaju u sledećem:

- 1) primena podzakonske regulative o određivanju kriterijuma za stepen tajnosti Interno (I) i Poverljivo (P), kao i Strogo poverljivo (SP) i Državna tajna (DT);
- 2) primena podzakonske regulative koja se odnosi na pojedine posebne mere zaštite;
- 3) usaglašavanje sistemskih i resornih propisa sa Zakonom o tajnosti podataka koji se odnose na rad sa tajnim podacima (informaciona bezbednost, odbrana, unutrašnji poslovi, krivično zakonodavstvo, upravni postupci, pravosuđe, lokalna samopurava, javna preduzeća, kancelarijsko poslovanje i slično);
- 4) izmene zaključenih međunarodnih sporazuma koji podrazumevaju razmenu tajnih podataka i formiranje posebnih registara za rad sa stranim tajnim podacima, a za te namene;
- 5) izmene akata o unutrašnjoj organizaciji i sistematizaciji ili formaciji, uvođenjem stepena tajnosti kome lice ima pristup u obavljanju svojih poslova, kao i obaveze posedovanja odgovarajućeg sertifikata za pristup tajnim podacima (bezbednosni kriterijumi);
- 6) izrada internih akata o prenosu tajnih podataka (kurirskom službom ili digitalno), primeni opštih i posebnih mera i slično (formiranje registarskog sistema, bezbednosnih zona, ustrojavanje posebnih evidencija i slično);
- 7) određivanju rukovaoca tajnih podataka i unutrašnje kontrole u organu javne vlasti i formiranje registarskog sistema za rad sa tajnim podacima Republike Srbije (po potrebi i registara za rad sa stranim tajnim podacima);
- 8) organizovanju sistema permanentne edukacije iz oblasti zaštite tajnih podataka u: Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Nacionalnoj akademiji za javnu upravu, organima javne vlasti i na visokoškolskim ustanovama kroz odgovarajuće programe;
- 9) vođenju posebnih službenih evidencija u skladu sa Zakonom o tajnosti podataka (koje ne spadaju u opšte kancelarijsko poslovanje); 10) uspostavljanje neposredne saradnje i komunikacije sa Kancelarijom Saveta za nacionalnu bezbednost i zaštitu tajnih podataka oko implementacije propisa o zaštiti tajnih podataka;
- 11) donošenjem unutrašnje regulative o informatičkoj sigurnosti/bezbednosti u radu sa tajnim podacima (akt o informacionoj bezbednosti za rad sa tajnim podacima) i umrežavanje sa drugim organima javne vlasti uz odgovarajuće tehnološke i bezbednosne akreditacije opreme, sistema i slično;

- 12) omogućavanju sprovođenja unutrašnje kontrole, nadzora od strane Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, inspeksijskog nadzora od strane Ministarstva pravde, kao i organizacija i država sa kojima postoje međunarodni sporazumi o razmeni tajnih podataka.

Ko može biti rukovalac tajnim podacima - rukovalac tajnim podatkom (čl. 2. tačka 10. ZTP) je fizičko lice ili organizaciona jedinica organa javne vlasti, koji preduzima mere zaštite tajnih podataka u skladu sa odredbama čl. 34. Zakona o tajnosti podataka Model Odluke o određivanju rukovaoca i Rukovalac tajnim podacima – infolist.

Lice koje je ovlašćeno kao rukovalac tajnim podacima, ne može istovremeno biti i lice koje je ovlašćeno da obavlja i poslove unutrašnje kontrole. Preporuka za određivanje rukovaoca tajnim podacima:

- U ministarstvima određuju se sekretarijati (eventualno kabineti ministra).
- U jedinicama lokalne samouprave određuju se organizacione jedinice koje su zadužene na poslovima planiranja odbrane (eventualno sekretarijati organizacionih jedinica).
- U sudovima određuju se sekretari sudova.
- U tužilaštvima određuju se lica na osnovu odluke glavnog tužioca.
- U javnim preduzećima određuju se organizacione jedinice koje su zadužene na poslovima planiranja odbrane.

Odluka o određivanju rukovaoca tajnim podacima ne podrazumeva istovremeno i ovlašćenje za kreiranje tajnih podataka.

Rukovodilac organa javne vlasti na osnovu funkcije koju obavlja ima obavezu vršenja dužnosti rukovaoca tajnim podacima do stupanja na snagu Odluke o određivanju rukovaoca tajnim podacima.

U organima javne vlasti čija organizaciona struktura podrazumeva manji broj zaposlnih lica rukovodilac organa javne vlasti istovremeno obavlja i funkciju rukovaoca tajnim podacima.

* Detaljnije pogledati skriptu Sistem zaštite tajnih podataka
([https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf))

PLAN ZAŠTITE TAJNIH PODATAKA U ORGANU JAVNE VLASTI

Plan zaštite tajnih podataka u organu javne vlasti je ključni dokument organizacione bezbednosti koji definiše sve mere i postupke zaštite tajnih podataka koje organ poseduje ili obrađuje. Kao takav, on je presudan za očuvanje integriteta informacija i nacionalne bezbednosti. Plan ima za cilj da osigura da se tajni podaci obrađuju, čuvaju, prenose i uništavaju u skladu sa najvišim standardima bezbednosti. On je osnovni stub organizacione bezbednosti u svakom organu javne vlasti. Omogućava pravilno upravljanje tajnim podacima i osigurava njihovu zaštitu, što je od ključnog značaja za očuvanje nacionalne bezbednosti.

OSNOVNI ELEMENTI PLANA UKLJUČUJU:

1. **Određivanje odgovornih lica:** U planu se definišu osobe koje su odgovorne za određivanje tajnih podataka, rukovalac tajnih podataka, kao i lice odgovorno za vršenje unutrašnje kontrole. Takođe, ova lica su odgovorna i za nadzor nad postupcima zaštite tajnih podataka i primenjivanje mera u skladu sa izmenama u zakonodavstvu i tehnologiji.
2. **Procedure:** Plan uključuje procedure za pravilno određivanje stepena tajnosti podataka u skladu sa zakonom (interno, poverljivo, strogo poverljivo, državna tajna), kao i određivanje načina obrade, čuvanja i uništavanja tajnih podataka, i bezbednosne mere koje se preduzimaju pri svakom koraku.
3. **Procena rizika za rad sa tajnim podacima:** U okviru izrade i redovnog ažuriranja plana zaštite tajnih podataka, organ javne vlasti mora redovno vršiti procenu rizika koji ugrožavaju bezbednost tajnih podataka. Procena rizika uključuje sve potencijalne pretnje, kao što su napadi na informacione sisteme, zloupotreba pristupa ili loša primena mera zaštite, kao i procenu njihovog uticaja na bezbednost i integritet podataka.
4. **Mere fizičke, tehničke i organizacione zaštite:** Opisuju se metode koje se primenjuju za bezbednost prostora u kojima se čuvaju tajni podaci, kao i zaštita IKT sistema koji obrađuju tajne podatke. Ovo uključuje fizičke barijere, kao što su ograde i pristupne kontrole, kao i tehnološke mere, kao što su kriptovanje podataka, dvostruka autentifikacija i bezbednosni protokoli za komunikaciju.
5. **Akreditacija IKT sistema:** IKT sistemi koji obrađuju tajne podatke moraju biti akreditovani od strane Ministarstva odbrane u vezi sa tehnološkim aspektima i krypto opremom. Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka vrši bezbednosnu akreditaciju tih IKT sistema kako bi se osiguralo da su u skladu sa najvišim bezbednosnim standardima.
6. **Obuka i svest:** Plan predviđa obuku svih zaposlenih koji imaju pristup tajnim podacima, kako bi bili upoznati sa svojim obavezama u vezi sa zaštitom tajnih podataka, kao i sa najnovijim pretnjama i metodama

odbrane. Obuka se redovno ažurira kako bi odražavala nove izazove u oblasti bezbednosti informacija.

7. **Sankcije za kršenje zaštite:** Planiranje sankcija u slučaju neovlašćenog pristupa ili otkrivanja tajnih podataka. Sankcije se odnose na kršenja pravila rada sa tajnim podacima, bilo da se radi o fizičkim prostorima ili IT sistemima.
8. **Plan postupanja u vandrednim situacijama:** Obuhvata procedure i mere koje treba preduzeti u slučaju napada, zloupotrebe ili drugij vandrednih situacija koje ugrožavaju bezbednost podataka.
9. **Praćenje stanja sertifikata:** Obuhvata praćenje izdatih sertifikata za fizička i pravna lica, uključujući proveru valjanosti sertifikata u kontekstu njihovog pristupa tajnim podacima.
10. **Rad sa pravnim licima:** Uprava i saradnja sa pravnim licima kod poverljivih nabavki, posebno u oblasti industrijske bezbednosti, koji uključuju bezbednost informacija i tehnologija u proizvodnim i servisnim procesima.
11. **Evidencije:** Organ javne vlasti mora voditi evidencije o određenim stepenima tajnosti, pristupu tajnim podacima, obuci zaposlenih, incidentima vezanim za bezbednost, revizijama bezbednosnih mera i uništavanju tajnih podataka.
12. **Ažuriranje plana:** Napomena je da se doneti plan zaštite tajnih podataka mora redovno ažurirati u skladu sa izmenama i dopunama propisa, tehnoloških standarda, naučenih lekcija u radu sa tajnim podacima i novonastalim pretnjama i rizicima za rad sa tajnim podacima.

Obaveze koje proizilaze iz Plana:

1. **Usaglašenost sa standardima bezbednosti :** Obaveza organa da se usaglasa sa nacionalnim i međunarodnim standardima u oblasti informacione bezbednosti, posebno u oblasti bezbednosti IT sistema koji obrađuje tajne podatke.
2. **Horizontalna i vertikalna koordinacija :** Planiranje i primena mera zaštite tajnih podataka podrazumeva saradnju između različitih nivoa rukovođenja i sektora unutar organa javne vlasti. Horizontalna koordinacija obuhvata razmenu informacija i uniformnu primenu mera bezbednosti među različitim sektorima, dok vertikalna koordinacija osigurava jasnu podršku i nadzor rukovođenja.
3. **Obavezna obuka :** Redovna obuka zaposlenih koji imaju pristup tajnim podacima, kako bi se osiguralo da su svi usklađeni sa najnovijim merama i procedurama. Kontinuirana komunikacija između organa javne vlasti i svih učesnika u procesu zaštite tajnih podataka je od izuzetnog značaja. Obuka svih zaposlenih treba uključivati ne samo pravljenje i primenu plana, već i razumevanje svih aspekata rizika i koordinacije u okviru organa javne vlasti.

4. **Sistem monitoringa i revizije :** Sistem za praćenje i reviziju koji osigurava da se sve mere zaštite primenjuju na adekvatan način. Revizija i ažuriranje plana u skladu sa novim pretnjama, tehnološkim napredcima i promenama u zakonodavstvu.

Plan zaštite tajnih podataka nije direktno propisan Zakonom o tajnosti podataka, ali se on se smatra implicitno obaveznim kao deo kompletnog sistema zaštite tajnih podataka, koji objedinjuje sve mere i procedure zaštite tajnih podataka u organu javne vlasti i koji mora biti u skladu sa važećim zakonima i propisima, kako o tajnosti podataka, tako i o informacionoj bezbednosti i kancelarijskim poslovanjem, kao i odgovarajućim sektorskim (resornim) propisima u skladu sa nadležnostima i poslovima koje obavlja organ javne vlasti.

Integrisani model upravljanja rizicima u sistemu zaštite tajnih podataka

Sistem zaštite tajnih podataka predstavlja složen i međusobno povezan skup organizacionih, tehničkih i normativnih mera, čija efikasnost zavisi od uravnotežene primene svih njegovih komponenti. Polazeći od te činjenice, ovaj materijal objedinjuje pregled ključnih elemenata sistema, njihovih osnovnih ciljeva i rizika koji nastaju u slučaju njihove neprimene. Na toj osnovi izvršena je procena rizika primenom matrice verovatnoće i uticaja, čime se omogućava jasno identifikovanje kritičnih tačaka i rangiranje prioriteta u zaštiti tajnih podataka.

U drugom koraku, rezultati procene rizika prevedeni su u strukturiran plan mera, koji obezbeđuje postepeno i logično unapređenje sistema — od adresiranja najkritičnijih ranjivosti do uređenja normativnih i ugovornih aspekata. Ovako postavljen pristup omogućava racionalno usmeravanje resursa, jačanje otpornosti sistema na insajderske i spoljne pretnje, kao i uspostavljanje kontinuiranog i održivog mehanizma kontrole i unapređenja zaštite tajnih podataka.

Kompaktna tabela koja poredi sve komponente sistema zaštite tajnih podataka, njihov osnovni cilj i rizike u slučaju neprimene:

Komponenta sistema	Osnovni cilj	Rizik ako se ne primenjuje
Registarski sistem	Uređeno i kontrolisano rukovanje tajnim podacima kroz evidenciju i akreditaciju	Haotično upravljanje, gubitak podataka ili njihovo neovlašćeno otkrivanje
Personalna bezbednost	Procena pouzdanosti lica koja imaju pristup tajnim podacima	Insajderske pretnje i zloupotreba ovlašćenog pristupa
Administrativna bezbednost	Pravilna određivanje i označavanje tajnosti, kao i prestanak tajnosti	Pogrešno označavanje podataka i nekontrolisano širenje informacija

Komponenta sistema	Osnovni cilj	Rizik ako se ne primenjuje
Fizička bezbednost	Kontrola prostora i primena fizičkih zaštitnih mera	Neovlašćen fizički pristup, krađa ili uništenje podataka
Informaciona bezbednost	Zaštita IKT sistema, kao i integriteta, poverljivosti i dostupnosti podataka	Sajber napadi, gubitak integriteta i dostupnosti informacija
Industrijska bezbednost	Zaštita tajnih podataka kod izvođača i podizvođača	Curenje poverljivih informacija kroz ugovorne odnose
Kontrola i nadzor	Kontinuirana provera primene mera i sistem izveštavanja	Formalna primena bez suštinske kontrole i postojanje skrivenih propusta

Ovako uređena tabela omogućava da se na prvi pogled sagleda doprinos svake komponente sistemu u celini, kao i ključni rizici koji nastaju u slučaju njihovog zanemarivanja.

Matrica rizika (verovatnoća × uticaj) za komponente sistema zaštite tajnih podataka

Verovatnoća nastanka rizika procenjuje se na osnovu učestalosti pojavljivanja događaja u relevantnom organizacionom i bezbednosnom kontekstu:

- **Visoka verovatnoća** – događaj se očekuje više puta u toku jedne godine.
- **Srednja verovatnoća** – događaj se može pojaviti u intervalu od jedne do tri godine.
- **Niska verovatnoća** – događaj je moguć, ali se očekuje retko (u intervalu dužem od pet godina).

Ovako definisani kriterijumi omogućavaju ujednačeno i objektivnije vrednovanje rizika unutar sistema.

Komponenta sistema	Verovatnoća	Uticaj	Nivo rizika	Prioritet delovanja
Personalna bezbednost	Visoka	Visok	Kritičan	Najviši
Informaciona bezbednost	Visoka	Visok	Kritičan	Najviši
Registarski sistem	Srednja	Visok	Visok	Visok
Fizička bezbednost	Srednja	Visok	Visok	Visok
Kontrola i nadzor	Srednja	Visok	Visok	Visok
Administrativna bezbednost	Srednja	Srednji	Srednji	Srednji
Industrijska bezbednost	Niska–srednja	Srednji	Srednji	Srednji

Objašnjenje:

- **Kritični rizici:** *personalna i informaciona bezbednost* — insajderske pretnje i sajber napadi imaju istovremeno visoku verovatnoću nastanka i izuzetno visok uticaj na sistem, što ih pozicionira kao prioritet broj jedan.
- **Visoki rizici:** *registarski sistem, fizička bezbednost i kontrola i nadzor* — propusti u ovim komponentama mogu proizvesti ozbiljne posledice po integritet sistema, iako je njihova verovatnoća po pravilu niža nego kod kritičnih rizika.
- **Srednji rizici:** *administrativna i industrijska bezbednost* — iako značajne, ove komponente imaju relativno ograničeniji domet posledica ili se propusti češće otkrivaju kroz druge kontrolne mehanizme.

Strukturisana matrica omogućava jasno prioritizovanje resursa, usmeravanje nadzornih aktivnosti i racionalno planiranje mera unapređenja sistema zaštite tajnih podataka.

Iako su rizici u matrici prikazani pojedinačno, u praksi postoji izražena međuzavisnost komponenti sistema. Propust u jednoj oblasti može inicirati lanac posledica u drugim segmentima zaštite.

Na primer, nedovoljno razvijen sistem **kontrole i nadzora** može dovesti do toga da se nebezbedno ponašanje zaposlenog ne uoči blagovremeno (**personalna bezbednost**), što dalje može rezultirati neovlašćenim pristupom ili curenjem podataka usled nedovoljno zaštićenih IKT sistema (**informaciona bezbednost**).

Ova povezanost potvrđuje da se mere moraju sprovoditi integrisano, a ne izolovano.

Plan prioriteta mera za unapređenje sistema zaštite tajnih podataka (*zasnovan na matrici rizika: verovatnoća × uticaj*)

Plan je strukturiran po nivoima rizika, tako da se najpre adresiraju kritične ranjivosti sistema, a zatim se mere postepeno proširuju na visoke i srednje rizike.

Iako je u planu mera administrativna bezbednost svrstana u srednji prioritet u pogledu implementacije, ona predstavlja **sistemske preduslov za funkcionisanje svih ostalih komponenti**.

Bez jasno definisanog sistema klasifikacije i upravljanja podacima:

- nije moguće adekvatno odrediti nivo pristupa (personalna bezbednost),
- nije moguće primeniti odgovarajuće tehničke mere (informaciona bezbednost),
- niti definisati uslove fizičke i industrijske zaštite.

Iz tog razloga, administrativna bezbednost mora se uspostavljati **paralelno sa kritičnim prioritetima**, kao osnova za dosledno funkcionisanje sistema.

Za efikasno praćenje primene mera, neophodno je uvesti merljive indikatore učinka:

- **Personalna bezbednost**
 - Indikator: 100% lica sa pristupom tajnim podacima poseduje važeći bezbednosni sertifikat.
 - Indikator: realizovane obuke i provereno znanje (testiranje zaposlenih).
- **Informaciona bezbednost**
 - Indikator: svi IKT sistemi akreditovani i dokumentovani.
 - Indikator: vreme reagovanja na incidente u skladu sa definisanim standardima.
- **Kontrola i nadzor**
 - Indikator: broj sprovedenih kontrola i procenat uočenih nepravilnosti koje su otklonjene u roku.

Ovi indikatori omogućavaju objektivnu procenu uspešnosti primene mera i kontinuirano unapređenje sistema.

Kritični prioriteti (sprovести bez odlaganja)

Personalna bezbednost

- Upostaviti i dosledno primenjivati stroge procedure provere lica (*background check*, izdavanje bezbednosnih sertifikata).
- Uvesti kontinuirano praćenje ponašanja zaposlenih, uz funkcionalan sistem za prijavu sumnjivih aktivnosti.
- Organizovati redovne obuke o insajderskim pretnjama i bezbednosnoj kulturi.

Informaciona bezbednost

- Sprovести akreditaciju IKT sistema i kriptografske opreme.
- Uvesti višeslojnu zaštitu: dvofaktorsku autentifikaciju, kriptovanje podataka i monitoring mrežnog saobraćaja.
- Upostaviti i testirati Plan reagovanja na sajber incidente (*Incident Response Plan*).

Visoki prioriteti (sprovести u kratkom roku)

Registarski sistem

- Uspostaviti jedinstvenu i centralizovanu evidenciju za rukovanje tajnim podacima.
- Uvesti standardizovane procedure za prijem, evidentiranje, korišćenje i uništavanje podataka.

Fizička bezbednost

- Uspostaviti kontrolu pristupa prostorijama (identifikacione kartice, biometrijski sistemi).
- Obezbediti video-nadzor i jasno definisane sigurnosne zone sa fizičkim barijerama.

Kontrola i nadzor

- Uspostaviti funkcionalnu unutrašnju kontrolu u organima javne vlasti.
- Obezbediti redovno izveštavanje i spoljni inspekcijski nadzor od strane nadležnih institucija.

Srednji prioriteti (sprovesti u srednjem roku)

Administrativna bezbednost

- Urediti jasan i dosledan sistem određivanja, označavanja i načina prestanka tajnosti podataka.
- Uvesti uniformne oznake i standardizovane procedure za upravljanje službenim dokumentima.

Industrijska bezbednost

Pored ugovornih obaveza i nadzora, industrijska bezbednost mora obuhvatiti i **prethodnu bezbednosnu proveru izvođača i podizvođača (due diligence) i pribavljajanje odgovarajućih sertifikata za pristup tajnim podacima za fizička i pravna lica**. To podrazumeva procenu:

- tehničkih i organizacionih kapaciteta za zaštitu tajnih podataka,
- kadrovske pouzdanosti,
- postojećih bezbednosnih politika i sertifikata.

Bez ovakve provere, ugovorne klauzule ostaju formalne i ne obezbeđuju stvarnu zaštitu podataka u lancu snabdevanja.

Pored toga, potrebno je:

- Obezbediti da svi ugovori sa izvođačima sadrže obavezujuće klauzule o zaštiti tajnih podataka.
- Uspostaviti sistematičan nadzor nad podizvođačima i postupcima poverljivih nabavki.

Ovako definisan plan jasno utvrđuje redosled delovanja:

1. **Prvo** se stabilizuju najosetljivije tačke sistema — personalna i informaciona bezbednost.
2. **Zatim** se jačaju sistemski mehanizmi kontrole — registarski sistem, fizička zaštita i nadzor.
3. **Na kraju** se uređuju normativni i ugovorni aspekti — administrativna i industrijska bezbednost.

Takav pristup omogućava racionalno usmeravanje resursa, maksimizaciju efekata mera i postepeno, ali sveobuhvatno jačanje sistema zaštite tajnih podataka.

Integrirani model upravljanja rizicima u sistemu zaštite tajnih podataka nije samo normativni okvir, već predstavlja operativni instrument koji omogućava kontinuirano unapređenje i jačanje otpornosti celog sistema. Njegova vrednost leži u tome što povezuje sve komponente zaštite u jednu funkcionalnu celinu, obezbeđuje merljive indikatore učinka i omogućava blagovremeno otkrivanje i otklanjanje slabosti. Na taj način, sistem zaštite tajnih podataka postaje dinamičan i održiv mehanizam, sposoban da se prilagođava novim pretnjama i izazovima, istovremeno štiteći nacionalne interese i institucionalni integritet.

NAPOMENA : SVE MODELE OBRAZACA, ODLUKA I EVIDENCIJA KOJE SU SASTAVNI DEO PLANA ZAŠTITE TAJNIH PODATAKA MOŽETE PRONAĆI NA SAJTU KANCELARIJE SAVETA ZA NACIONALNU BEZBEDNOST I ZAŠTITU TAJNIH PODATAKA

<https://nsa.gov.rs/tekst/577/obraci.php>

REGISTARSKI SISTEM

Rukovanje tajnim podacima je predviđeno samo u uređenom sistemu, koji mora biti uspostavljen u skladu sa propisima i standardima iz oblasti zaštite tajnih podataka. Tako uređen i akreditovan sistem predstavlja registarski sistem.

Osnovne funkcije registarskog sistema su prijem, evidentiranje, rukovanje, distribucija i uništavanje tajnih podataka. Navedene funkcije se uspostavljaju unutar jedinstvenog sistema registra, pri čemu se održava kompartmentalizacija tajnih podataka, ili se uspostavlja sistem odvojenih podregistara i pristupnih tačaka.

Registri, podregistri i pristupne tačke deluju kao odgovorne unutrašnje celine organa javne vlasti za prijem i otpremu tajnih podataka, vođenje evidencija o svim tajnim podacima iz njihove nadležnosti, pravilno rukovanje i čuvanje tajnih podataka iz njihove nadležnosti i distribuciju tajnih podataka unutar sistema organa javne vlasti.

Svaki organ javne vlasti, prema potrebi, treba da uspostavi registar, podregistar ili pristupnu tačku za klasifikovane podatke. Oni se mogu uspostaviti na nivou ministarstva, uprava, kancelarija, agencija i ostalih organa javne vlasti. Registarski sistem se može uspostaviti za tajne podatke koji su u papirnoj formi, kao i za podatke u elektronskom obliku, koji su zapisani na bilo kom mediju.

Uspostavljanje registarskog sistema ima za cilj da osigura potpunu kontrolu nad tajnim podatkom i za njegovo uspostavljanje neophodno je obezbediti minimalne uslove:

- adekvatan prostor koji ispunjava sve zahteve za restriktivni pristup tajnim podacima;
- uspostavljanje funkcija ovlašćenih lica i određivanje lica odgovornih za rukovanje i zaštitu tajnih podataka – rukovaoca tajnim podacima i rukovaoca registra tajnih podataka;
- propisivanje politike zaštite tajnih podataka i procedura za postupanje sa tajnim podacima;
- uspostavljanje sistema edukacija zaposlenih za rad sa tajnim podacima u registarskom sistemu;
- organizovanje sistema nadzora i kontrole rada registarskog sistema;
- izvršen stručni nadzor od Kancelarije Saveta;

Načelna organizacija registarskog sistema treba da omogućí zaštitu tajnih podataka, u skladu sa minimalnim uslovima i standardima koji moraju biti ispunjeni, u odnosu na stepen tajnosti koji je određen radi zaštite tajnog podatka u svim magistralama sistema. Takođe, sistem treba da omogućí neometan pristup tajnim podacima, korisnicima koji su ovlašćeni da pristupe i ostvare uvid u tajni podatak, na osnovu principa „POTREBNO DA ZNA“.

Uspostavljanjem osnovnih funkcija i propisivanjem politike zaštite tajnih podataka i procedura za postupanje sa tajnim podacima, organi koji uspostavljaju registarski sistem treba da regulišu:

- određivanje najvišeg stepena tajnosti tajnih podataka koji nastaju u radu organa javne vlasti, odnosno koje organa javne vlasti razmenjuje sa ostalim organima u državi;
- izradu analize rizika, odnosno procenu ugroženosti tajnih podataka u organu javne vlasti;
- donošenje odluka o određivanju posebnih administrativnih i bezbednosnih zona, za rad sa tajnim podacima, u okviru zone razmeštaja organa javne vlasti;
- donošenje odluke o ovlašćenim licima za rad u navedenim zonama;
- propisivanje mera obezbeđenja administrativne i bezbednosne zone;
- uspostavljanje i akreditacija sistema fizičko-tehničke zaštite tajnih podataka u registarskom sistemu, u skladu sa izrađenom analizom rizika i propisanim merama obezbeđenja;
- plan zaštite tajnih podataka u registarskom sistemu;
- plan zaštite tajnih podataka u registarskom sistemu u vanrednim i hitnim slučajevima, odnosno slučajevima narušavanja bezbednosti i kompromitovanja tajnih podataka;
- uspostavljanje sistema kriptozastite za zaštitu tajnih podataka koji se razmenjuju elektronskim putem;
- sistem evidentiranja postupaka i izvršenih procedura za rad i korišćenje registarskog sistema;
- sistem ostvarivanja pristupa i uvida u tajne podatke koji se čuvaju u registarskom sistemu, za ovlašćene korisnike;
- sistem kontrole i nadzora nad organizacionim i uspostavljenim merama zaštite tajnih podataka;
- program obuke ovlašćenih lica i zaposlenih u organu javne vlasti za rad u registrima.

Pravilno uspostavljanje registarskog sistema omogućava smanjenje rizika od neovlašćenog pristupa tajnim podacima i kompromitovanje tajnih podataka, kao i obezbeđivanje sprečavanja i otkrivanja neovlašćenih radnji koje imaju cilj narušavanje bezbednosti tajnih podataka.

EVIDENCIJE ZA RAD SA TAJNIM PODACIMA

- Evidencija rešenja i sertifikata stepena tajnosti "POVERLjIVO", "STROGO POVERLjIVO" i "DRŽAVNA TAJNA", za lica koja u organu javne vlasti obavljaju funkciju ili su zaposlena, odnosno za lica koja obavljaju poslove, u skladu sa zakonom kojim se uređuje tajnost podataka.
- Lista ovlašćenih lica za pristup tajnim podacima u organu javne vlasti
- Evidencija tajnih podataka u organu javne vlasti (po stepenu tajnosti)

- Evidencija kopiranja i umnožavanja tajnih podataka
- Evidencija nosača tajnih podataka
- Evidencija ostvarivanja uvida u tajne podatke
- Evidencija uništenih tajnih podataka
- Evidencija pečata i pomoćnih štambilja
- Evidencija izdatih bezbednosnih propusnica za ulazak u bezbednosnu i administrativnu zonu, odnosno registar tajnih podataka
- Evidencija ključeva za pristup tajnim podacima u organu javne vlasti
- Evidencija zamene šifara za pristup tajnim podacima u organu javne vlasti
- Evidencija ulazaka u registar tajnih podataka
- Evidencija uvežbavanja postupanja u slučaju narušavanja bezbednosti tajnih podataka, vanrednim i hitnim slučajevima
- Evidencija narušavanja bezbednosti ili kompromitovanja tajnih podataka
- Evidencija kontrole fizičko-tehničkih mera zaštite tajnih podataka
- Evidencija inspekcija

* Detaljnije pogledati skriptu Sistem zaštite tajnih podataka

[\(\[https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\\).pdf\]\(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf\)\)](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)

PERSONALNA BEZBEDNOST

Mere i aktivnosti koje se sprovode u domenu personalne bezbednosti imaju veoma važnu ulogu u procesu zaštite tajnih podataka.

One obuhvataju niz procedura čiji je osnovni cilj da se utvrdi da li neko lice može biti ovlašćeno da dobije pristup tajnim podacima, a da pri tome ne predstavlja neprihvatljiv rizik za nacionalnu bezbednost.

Lica čije dužnosti predviđaju pristup tajnim podacima prethodno moraju biti podvrgnuta odgovarajućoj bezbednosnoj proverbi pre nego što im se izda određeni bezbednosni sretifikat/dozvola koji će važiti tokom odobrenog trajanja tog pristupa.

Posedovanje bezbednosnog sertifikata je prvi korak i nužan uslov za pristup tajnim podacima. Uslovi za izdavanje sertifikata utvrđuju se kroz bezbednosnu proveru koju vrše nadležne službe, na zahtev organa javne vlasti, a preko Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.

Bezbednosnom proverom vrši se procena bezbednosnog rizika naročito od pristupa i korišćenja tajnih podataka. U okviru bezbednosne provere nadležni organ sa aspekta bezbednosti ocenjuje navode u popunjenom bezbednosnom upitniku.

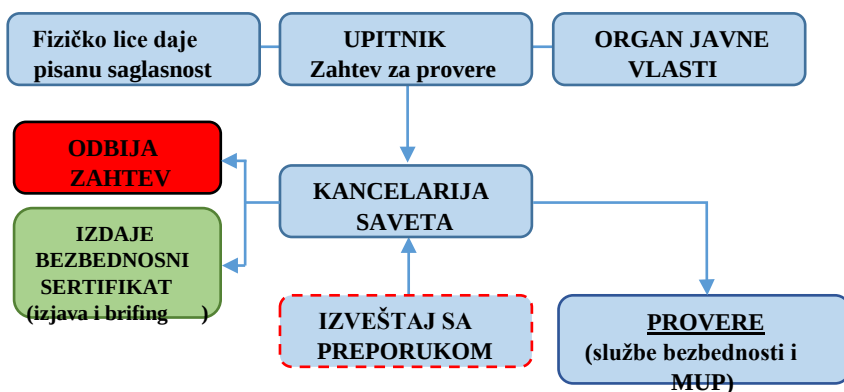
Nadležni organ u vezi da navodima iz bezbednosnog upitnika prikuplja lične i druge podatke od lica na koje se ti podaci odnose, od drugih organa javne vlasti, organizacija i registara, evidencija, datoteka i zbirki podataka koje se vode na osnovu zakona.

Bezbednosni sertifikat je dokument koji potvrđuje da lice ima pravo pristupa i korišćenja tajnih podataka odgovarajućeg stepena tajnosti, a u skladu sa principom „Potrebno da zna“. Pre izdavanja sertifikata, odnosno dozvole, lice kome se izdaje sertifikat dužno je da potpiše izjavu kojom potvrđuje da će postupati sa tajnim podacima u skladu sa zakonom. Ako lice ne potpiše izjavu i ne preuzme sertifikat za pristup tajnim podacima odnosno dozvolu, postupak izdavanja se obustavlja.

POSEDOVANJE REŠENJA BEZ IZDATOG SERTIFIKATA NE ZNAČI MOGUĆNOST PRISTUPU TAJNOM PODATKU. NE PREUZIMANJE SERTIFIKATA PODRAZUMEVA UGOŽAVANJE NACIONALNE BEZBEDNOSTI REPUBLIKE SRBIJE, ŠTO UJEDNO MOŽE PREDSTAVLJATI I BEZBEDNOSNU SMETNJU PRILIKOM NOVE PROVERE.

Podizanje bezbednosne kulture i svesti korisnika tajnih podataka sprovodi se kroz kontinuiranu obuku iz oblasti zaštite i rada sa tajnim podacima, koja se sprovodi na svim nivoima, kao i kroz redovne brifinge i debriefinge o obavezama koje proizilaze iz sticanja bezbednosnog sertifikata.

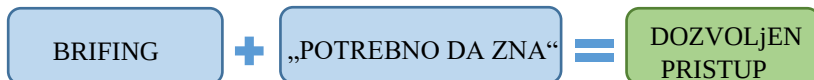
PROCES IZDAVANJA SERTIFIKATA



USLOVI ZA PRISTUP TAJNOM PODATKU



POVERLJIVO I VIŠE



INTERNO

Bezbednosna kultura i svest - bezbednosna aktivnost koja izražava spremnost delovanja i ponašanja u skladu sa stečenim znanjima i veštinama, kao i u skladu sa prihvaćenim vrednosnim stavovima. Ogleda se u prepoznavanju opasnosti, reagovanju na njih izbegavanjem opasnosti, otklanjanjem opasnosti ili upućivanjem na one subjekte koji će profesionalno reagovati i sačuvati ugrožene vrednosti. Znanje i stav koji članovi organizacije imaju u pogledu zaštite određenih vrednosti – nacionalne bezbednosti, odbrane, unutrašnjih i spoljnih poslova, ljudskih sloboda i prava, kao i fizičke i intelektualne imovine, a posebno informacija i podataka kojima raspolaže organizacija (organ javne vlasti, pravno lice ili kompanija).

Informaciona kultura i svest - praksa osiguranja informacija i upravljanja rizicima vezanim za upotrebu, obradu, skladištenje, prenos i arhiviranje informacija. Informaciona kultura i svest uključuje zaštitu integriteta, dostupnosti, autentičnosti, nepovršenosti i poverljivosti korisnika. Obuhvata i digitalne zaštite i fizičke tehnike. Usvajanje adekvatnog ponašanja da se pronađu informacije, koristeći pritom bilo koji način ili medijum, koji na najbolji mogući način zadovoljava potrebe za informacijama, a koje vode mudrom i etičkom korišćenju informacija u društvu (digitalna pismenost?).

Informaciona bezbednosna kultura i svest - deo u razvoju informacione bezbednosti koja se fokusira na prikupljanje saznanja i iskustava u vezi sa potencijalnim rizicima i pretnjama koje se brzo razvijaju, u vezi sa ljudskim ponašanjem, kako korisnika IKT sistema, tako i potencijalnih napadača. 1 INFOLIST Manifestije se u okviru organizacije kroz aspekte bezbednosti koji se odnose na: 1) vrednosti; 2) ponašanje; 3) stavove; 4) akcije; 5) aktivnosti rukovodstva (mendžmenta); i 6) fizičko okruženje.

Organizaciona kultura i svest - sistem zajedničkih značenja i simbola. • Model osnovnih pretpostavki, vrednosti i normi, koje je data grupa razvila ili otkrila učeći kako da rešava probleme eksterne adaptacije i intarne integracije i koji funkcionišu dovoljno dobro da bi bili preneti novim članovima organizacije kao ispravan način mišljenja i osećanja u vezi sa tim problemima. • Obrazac verovanja, vrednosti i naučenih načina postupanja sa iskustvom koji su se razvili kroz organizacionu istoriju i koji se manifestuju kroz materijalne objekte, kao i ponašanje članova organizacije.

Sajber higijena - reč je o bezbednosnoj praksi koja uključuje sve korisnike interneta, i sa internetom povezanih stvari, servisa, aplikacija, i uređaja sa ciljem zaštite sigurnosti i integriteta štićenih podataka i sprečavanja sajber napada. • Odnosi se na prakse koje imaju za cilj sprečavanje infekcije malicioznim sofverom (malware), kao i sajber upade i gubljenje ili korumpiranje podataka i održavanje zdravog sajber okruženja.

Međuinstitucionalna saradnja - Kancelarija Saveta potpisala je više Sporazuma o saradnji koji obuhvataju poslove unapređenja i inovacije znanja i veština u obradi i zaštiti tajnih podataka, kako podataka od interesa za Republiku Srbiju, tako i stranih tajnih podataka, u cilju stručnog usavršavanja u državnim i drugim organima.

Sporazumi o međuinstitucionalnoj saradnji potpisani su sa:

1. Direktorat civilnog vazduhoplovstva Republike Srbije, Skadarska 23, 11000 Beograd,
2. Ministarstvo finansija - Uprava za sprečavanje pranja novca, Resavska 24, 11167 Beograd,
3. Državna revizorska institucija, Makenzijeve 41, 11111 Beograd,
4. Privredna komora Srbije, Resavska 13 - 15, 11000 Beograd,
5. Akreditaciono telo Srbije, Vlajkovićeve 3, 11103, Beograd,
6. Univerzitet u Beogradu, Pravni fakultet, Bulevar kralja Aleksandra 67, 11120 Beograd,
7. Univerzitet u Beogradu, Fakultet organizacionih nauka, Jove Ilića 154, 11010 Beograd,
8. Univerzitet u Beogradu, Fakultet bezbednosti, Gospodara Vučića 50, 11118 Beograd,
9. Kriminalističko-policijski univerzitet, Cara Dušana 196, 11080 Beograd,
10. BIA - Akademija za nacionalnu bezbednost, Ulica kraljice Ane bb, 11000 Beograd,

11. Ministarstvo spoljnih poslova - Diplomatska akademija, Kneza Miloša 24-26, 11000 Beograd,
12. Nacionalna akademija za javnu upravu Vlade Republike Srbije, Bulevar Mihajla Pupina 2, 11000 Novi Beograd.

* Detaljnije pogledati skriptu Sistem zaštite tajnih podataka
([https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf))

* Postupak izdavanja bezbednosnog sertifikata
(https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja_BS-skripta.pdf)

FIZIČKA BEZBEDNOST

Fizička bezbednost podrazumeva primenu mera fizičke i tehničke zaštite na pojedinačnim lokacijama, u zgradama ili na otvorenim prostorima u kojima se nalaze ili čuvaju tajni podaci koji zahtevaju zaštitu od gubljenja, neovlašćenog pristupa, kompromitovanja ili otuđenja.

Izbor mera koje će se koristiti za fizičku bezbednost tajnih podataka zavisi od specifičnosti objekta, broja tajnih podataka, stepena tajnosti. Na osnovu ovih parametara radi se opšta procena rizika na osnovu koje se primenjuju mere fizičko-tehničke zaštite. Svrha procene je da se koordinira i optimizuje korišćenje resursa i nadgledaju, kontrolišu i umanje pretnje koje mogu da ugroze bezbednost.

Mere fizičkog i tehničkog obezbeđenja treba da se zasnivaju na principu „**odbrana po dubini**“, Rukovanje i čuvanje tajnih podataka vrši se u **bezbednosnim i administrativnim zonama**.

Prostor ili prostorije u kojima se obrađuju i čuvaju tajni podaci stepena tajnosti „DRŽAVNA TAJNA“, „STROGO POVERLjIVO“, i „POVERLjIVO“ uspostavljene su kao bezbednosne zone prvog i/ili drugog stepena.

Prostor ili prostorije u kojima se obrađuju i čuvaju tajni podaci stepena tajnosti „INTERNO“ uspostavljaju se kao administrativne zone.

Prostorije u kojima se čuvaju, koriste, obrađuju i uništavaju tajni podaci obezbeđuju se **protivprovalnim i protivpožarnim sistemom**. Jedna od mera je i uspostavljanje efikasne **kontrole pristupa**.

Prostor oko prostorija u kojima se čuvaju, koriste, obrađuju ili uništavaju tajni podaci, kao i put do njih, po pravilu, se obezbeđuju **video-nadzorom**.

Prostorije u kojima se postavljaju telefonske centrale i druga telekomunikaciona oprema za objedinjavanje celokupnog informacionotelekomunikacionog saobraćaja, kao i prostorije u kojima se postavljaju centralni serveri informacionih sistema, po pravilu, su bez prozora. Ako prostorije imaju prozore, radi preduzimanja mera odgovarajuće tehničke zaštite, ugrađuju se **sredstva za protivprovalnu zaštitu (detektori pokreta i loma stakla)**, **sigurnosne metalne rešetke** čiji položaj onemogućava otvaranje prozora, kao i **specijalna stakla** koja onemogućavaju pogled u unutrašnjost prostorije.

Bezbednosno tehnička oprema, odnosno odgovarajuća sredstva tehničke zaštite u kojoj se čuvaju tajni podaci su: **protivpožarna metalna kasa sa ugrađenom bravom** za stepen tajnosti „DRŽAVNA TAJNA”, „STROGO POVERLjIVO” i „POVERLjIVO” i/ili **kancelarijski ili metalni ormar** za stepen tajnosti „INTERNO”. Kase ili prostorije u kojoj se ta kasa nalazi, opremljene su sistemom javljanja i moraju ispunjavati odgovarajuće SRPS/EN tehničke standarde.

* Detaljnije pogledati skripte Sistem zaštite tajnih podataka

[https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)

* Priručnik Osnove obrade i zaštite podataka

https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf

ADMINISTRATIVNA BEZBEDNOST

Administrativna bezbednost predstavlja skup mera, politika, procedura i praksi koje su usmerene na očuvanje bezbednosti informacija, resursa i operacija unutar organizacije ili sistema. Ova oblast se odnosi na upravljanje rizicima, zaštitu podataka i informacija, upravljanje pristupom, obuku zaposlenih i slične aktivnosti koje imaju za cilj očuvanje poverljivosti, integriteta i dostupnosti informacija.

Administrativna bezbednost tajnih podataka preduzima se u cilju obezbeđivanja njihove efikasne pravne i potpune zaštite pri rukovanju istim, kao i smanjenja ili otklanjanja mogućih rizika od neovlašćenog pristupa i otkrivanja neovlašćenim licima.

Administrativna bezbednost tajnih podataka uspostavlja se od trenutka donošenja odluke o određivanju tajnosti podatka i traje do trenutka njegovog fizičkog uništenja ili skidanja oznake tajnosti.

Podaci koji podležu označavanju stepena tajnosti i koji su zaštićeni jednim od zakonom utvrđenih stepena tajnosti su iz sledećih oblasti: zaštita teritorijalnog integriteta i suverenosti Republike Srbije, zaštita ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalna i javna bezbednost, odbrana, unutrašnji i spoljni poslovi, odnosno aktivnosti bezbednosnih i obaveštajnih službi, ekonomski interesi i međunarodni položaj Republike Srbije i saradnja sa drugim državama i međunarodnim subjektima.

Tajni podatak se određuje i označava stepenom tajnosti u zavisnosti od procene ozbiljnosti nastanka moguće štete po interese Republike Srbije, u slučaju njegovog otkrivanja neovlašćenom licu, njegove zloupotrebe ili uništavanja.

Tajni podatak može da kreira samo organ javne vlasti, odnosno ovlašćeno lice u organu javne vlasti koje ima odgovarajući bezbednosni sertifikat za pristup tajnim podacima i koje prema svojim dužnostima i zadacima treba da kreira tajne podatke, tj. da rukuje tim podacima.

Tajnim podatkom ne smatra se podatak koji je označen kao tajna radi prikrivanja krivičnog dela, prekoračenja ovlašćenja ili zloupotrebe službenog položaja ili drugog nezakonitog akta ili postupanja organa javne vlasti.

Lica koja rukuju tajnim podacima (kreatori i korisnici), u skladu sa Zakonom o tajnosti podataka, preduzimaju mere i radnje za administrativnu bezbednost, kad god postoji potreba za rukovanjem i čuvanjem tajnih podataka.

Mere i aktivnosti za administrativnu bezbednost tajnih podataka preduzimaju organi javne vlasti (državni organi, javne ustanove i službe, organi jedinica lokalne samouprave) i druga pravna i fizička lica, u cilju obezbeđenja zaštite i zakonitog

postupanja sa tajnim podacima kao što su: • pravilno utvrđivanje i označavanje stepena tajnosti podataka;

- prijem i evidentiranje u knjige evidencije;
- obezbeđivanje pravilnog čuvanja i rukovanja;
- pravilna distribucija, priprema kopija, prevoda i izvoda iz tajnog podatka i realizacija kontrole distribucije do krajnjih korisnika po principu „POTREBNO DA ZNA“;
- sprečavanje svakog pokušaja neovlašćenog pristupa i rukovanja od strane neovlašćenih lica;
- pravilan odabir arhivske građe, kao i pravilno izdvajanje i uništavanje odabrane nepotrebne arhivske građe.

Pravilnom primenom administrativnih bezbednosnih mera i aktivnosti u velikoj meri se omogućava smanjenje rizika od neovlašćenog pristupa tajnim podacima, kao i lakše otkrivanje narušavanja bezbednosti tajnih podataka.

*

Detaljnije pogledati skriptu Sistem zaštite tajnih podataka

[https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)

INFORMACIONA BEZBEDNOST

Informaciona bezbednost tajnih podataka obuhvata integrisani skup međuzavisnih mera i aktivnosti usmerenih na zaštitu tajnih podataka koje se obrađuju u IKT sistemima (IKT- informaciono komunikacione tehnologije). Procesom bezbednosne akreditacije IKT sistema utvrđuje se da li je sistem postigao adekvatan nivo zaštite tajnih podataka.

Bezbednosna verifikacija IKT sistema obezbeđuje:

- potvrdu da li su planirane mere bezbednosti IKT sistema pravilno sprovedene;
- potvrdu da je odgovarajućim testiranjem postignut zahtevani nivo bezbednosti;
- dokumentovanje rezultata verifikacije bezbednosne implementacije IKT sistema; Ovo potvrđuje da su ispoštovani minimalni bezbednosni standardi IKT sistema za obradu, čuvanje i razmenu tajnih podataka.

Procenom mogućeg narušavanja bezbednosti tajnih podataka i bezbednosti IKT sistema, odnosno procenom bezbednosnog rizika, utvrđuje se verovatnoća da će određena ranjivost tog sistema biti iskorišćena i dovesti do narušavanja bezbednosti sistema.

Procena bezbednosnog rizika služi za utvrđivanje bezbednosnih rizika, tj. pretnji i ranjivosti IKT sistema, utvrđivanje njihove veličine, kako bi se identifikovale oblasti u kojima je potrebna zaštita tajnih podataka u IKT sistemu.

Primenom mera bezbednosti radi zaštite IKT sistema postižu se sledeći efekti:

- identifikacija osoba koje pristupaju sistemu;
- kontrola i evidencija pristupa na osnovu datog prava pristupa iz definisane baze podataka;
- obezbeđivanje pouzdanog načina da se ukaže na stepen tajnosti;
- identifikacija korisnika i pouzdana evidencija odštampanog, kopiranog, modifikovanog ili izbrisnog tajnog podatka;
- zaštita važnih tehničkih i programskih elemenata i funkcionalnost sistema;
- kontrola i upravljanje rukovanjem i prenosom nosača podataka na kojima se čuvaju tajni podaci;
- planiranje, konfigurisanje, upravljanje i kontrola mrežnih uređaja.

Ove mere zajedno čine osnovu za zaštitu IKT sistema od različitih pretnji, ali je važno kontinuirano pratiti nove trendove i tehnologije kako bi se osiguralo da su sistemi uvek zaštićeni od najnovijih pretnji.

Kriptografska zaštita IKT sistema u kojima se obrađuju tajni podaci je deo informacione bezbednosti. Primenom kriptografskih sredstava i metoda obezbeđuje se siguran i zaštićen prenos tajnih podataka u IKT sistemima između dve tačke kroz nekontrolisani prostor. Time se značajno povećava bezbednost tajnih podataka i smanjuje mogućnost njihovog kompromitovanja i nanošenja štete.

Kriptografske metode i sredstva primenjuju se sa ciljem očuvanja autentičnosti, integriteta i dostupnosti tajnih podataka. Prilikom prenosa tajnih podataka, svaki IKT sistem koji obrađuje tajne podatke stepena tajnosti „POVERLJIVO“ i više treba da bude zaštićen od kompromitujućeg elektromagnetnog zračenja (KEMZ).

Prema rezultatima merenja sprovedenih uz pomoć odgovarajuće opreme za zoniranje objekata i merenja elektromagnetnog zračenja određuju se bezbednosne zone u objektima u kojima se obrađuju tajni podaci. U stvari, to znači određivanje prostorija prema stepenu zaštite od elektromagnetnog zračenja.

Na osnovu rezultata koji su dobijeni merenjima, preduzimaju se određene bezbednosne mere za smanjenje elektromagnetnog zračenja van kontrolisanog prostora ustanove, čime se izbegava mogućnost oticanja tajnih podataka putem kompromitujućeg elektromagnetnog zračenja opreme.

U oblasti emisije bezbednosti, merenja elektromagnetnog zračenja vrše se na opremi koja će se koristiti za obradu tajnih podataka. Na osnovu dobijenih rezultata utvrđuje se vrsta opreme koja će se koristiti u odgovarajućim zonama bezbednosti. Ova vrsta bezbednosnih mera je neophodna, jer se suočavamo sa velikim rizikom od kompromitovanja tajnih podataka koje emituje IKT oprema.

* Detaljnije pogledati skriptu Sistem zaštite tajnih podataka
([https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf))

* Priručnik Osnove obrade i zaštite podataka
(https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf)

INDUSTRIJSKA BEZBEDNOST

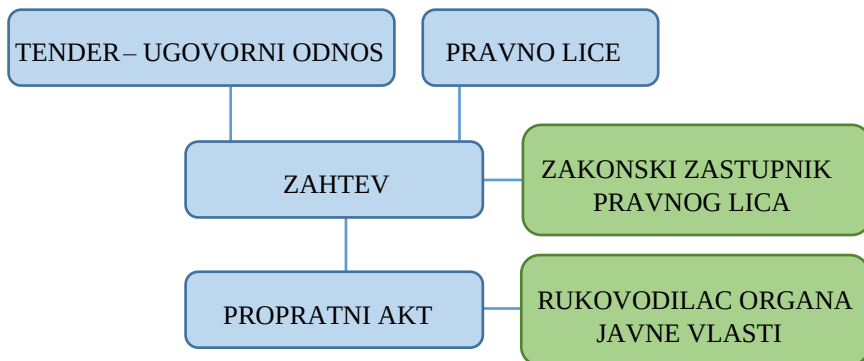
Industrijska bezbednost predstavlja primenu mera radi obezbeđenja zaštite tajnih podataka od strane izvođača ili podizvođača u pregovorima koji prethode zaključivanju ugovora i tokom celog veka trajanja tajnih/poverljivih ugovora. Izvršenje poverljivog ugovora podrazumeva sve radnje preduzete nakon njegovog zaključenja do izvršenja ugovornih obaveza, odnosno do prestanka njegovog važenja.

Mere i aktivnosti koje treba preduzeti u radu sa tajnim podacima iz domena industrijske bezbednosti zavise od stepena tajnosti, procene pretnje po bezbednost tajnih podataka i količine i prirode/oblika dokumenta u kome je sadržan tajni podatak. Posebne mere zaštite tajnih podataka, propisane odgovarajućom uredbom iz oblasti industrijske bezbednosti, odnose se na način i postupak utvrđivanja ispunjenosti organizacionih i tehničkih uslova za čuvanje tajnih podataka koji su dostavljeni pravnom ili fizičkom licu po osnovu ugovornog odnosa.

Radi zaštite tajnih podataka prilikom realizacije poverljivih ugovora, neophodno je da učesnici u realizaciji ugovora prethodno obezbede posedovanje odgovarajućih bezbednosnih sertifikata za pravno lice i za fizička lica. Posedovanje rešenja bez izdatog sertifikata ne znači posedovanje mogućnosti pristupa tajnom podatku. Neophodne bezbednosne sertifikate za pravna i fizička lica izdaje Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, po zahtevu organa javne vlasti, nakon prethodno sprovedenih bezbednosnih provera za pravna i fizička lica, imajući u vidu ispunjenost uslova za izdavanje sertifikata propisanih čl. 49. Zakona o tajnosti podataka kao i utvrđivanje odsustva/postojanje bezbednosnog rizika za pravno i fizičko lice. Sertifikovanje pravnih lica omogućava njihov nesmetan pristup tajnim podacima Republike Srbije i učešće na raspisanim tenderima u državama sa kojima

Republika Srbija ima zaključene i ratifikovane međunarodne sporazume o razmeni i uzajamnoj zaštiti tajnih podataka.

PODNOŠENJE ZAHTEVA ZA SERTIFIKACIJU PRAVNIH LICA



* Detaljnije pogledati skriptu Sistem zaštite tajnih podataka
([https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta\).pdf](https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf))

* Postupak izdavanja bezbednosnog sertifikata
(https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja_BS-skripta.pdf)

UNUTRAŠNJA KONTROLA

Unutrašnja kontrola osmišljena je sa ciljem da obezbedi:

- usaglašenost sa zakonskim i institucionalnim zahtevima;
- realizaciju koncepta „zaštite nacionalne bezbednosti“ ;
- postizanje visokih standarda kvaliteta korporativnog upravljanja;
- adekvatno ponašanje zaposlenih;
- odgovornost u radu s tajnim podacima; • dobre sisteme zaštite tajnih podataka.

Unutrašnja kontrola predstavlja proveru zakonitosti i pravilnosti postupanja unutar organa javne vlasti u slučajevima kada se ukazuje na zloupotrebe i prekoračenje ovlašćenja, odnosno na kršenje procedura rada sa tajnim podacima, a time i na ugrožavanje organizacione i nacionalne bezbednosti.

CILJEVI UNUTRAŠNJE KONTROLE

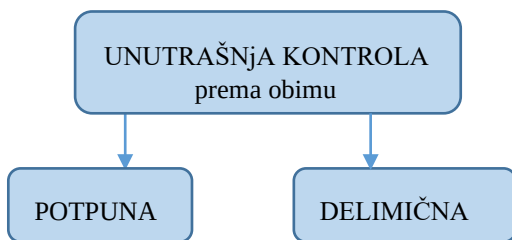
- **PRAĆENJE POTPUNE IMPLEMENTACIJE ZAKONA O TAJNOSTI PODATAKA**
- **POUZDANO IZVEŠTAVANJE RUKOVODIOCA JAVNE VLASTI**

RAD UNUTRAŠNJE KONTROLE

Unutrašnja kontrola koja se sprovodi nad radom sa tajnim podacima ne sastoji se samo u kontroli zakonitosti, već i u kontroli celishodnosti rada, kontroli obučenosti, opremljenosti i pripremljenosti zaposlenih, rukovaoca tajnim podacima, postupanja sa IKT sistemima za rad sa tajnim podacima, odgovornog trošenja namenskih sredstava, blagovremenosti, potpunosti i tačnosti informisanja rukovodstva, kao i obaveza u oblasti slobodnog pristupa informacijama od javnog značaja.

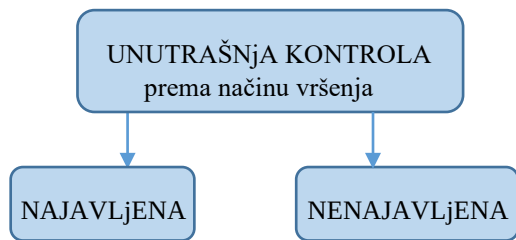
Unutrašnju kontrolu u organu javne vlasti može obavljati i unutrašnja organizaciona jedinica u organu javne vlasti, koja je za te poslove određena aktom o unutrašnjem uređenju i sistematizaciji radnih mesta u organu javne vlasti, a neposrednu kontrolu može obavljati zaposleni u toj unutrašnjoj organizacionoj jedinici pod uslovom da ima odgovarajući sertifikat za pristup tajnim podacima. Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka vrši obuku lica ovlašćenih za poslove unutrašnje kontrole.

VRSTE UNUTRAŠNJE KONTROLE



Potpunom kontrolom vrši se primena svih propisanih mera za zaštitu tajnih podataka, a delimičnom kontrolom jedne ili više mera.

Najavljena unutrašnja kontrola vrši se na osnovu godišnjeg plana rada organa javne vlasti, a nenajavljena na osnovu odluke koju donosi rukovodilac organa javne vlasti.



Nakon izvršene unutrašnje kontrole ovlašćeno lice sačinjava zapisnik i najkasnije u roku od tri dana podnosi rukovodiocu organa izveštaj o unutrašnjoj kontroli zajedno sa zapisnikom.

UNUTRAŠNJA KONTROLA JE VAŽNA ZBOG:

- utvrđivanja usklađenosti sa važećim zakonima i propisima;
- propisnog izvršenja poslova i nadležnosti organa javne vlasti;
- relevantnog i pouzdanog izveštavanja o radu sa tajnim podacima u organu javne vlasti;
- nepristrasnih analiza bezbednosnih incidenata i važećih procedura;
- predlaganja mera za unapređenje stanja bezbednosti tajnih podataka.

Немојте само да “штиклирате” документа



Немојте само пролазити кроз захтеве.

Ко може обављати унутрашњу контролу? – **унутрашњу контролу** у органу јавне власти може обављати и унутрашња организациона јединица у органу јавне власти, која је за те послове одређена актом о унутрашњем уређењу и систематизацији радних места, а непосредну контролу може обављати запослени у тој унутрашњој организационој јединици под условом да има одговарајући сертификат за приступ тајним подацима.

Сматрамо да у органу јавне власти ако нема успостављен систем унутрашње контроле у смислу члана 84. став 2. (Министарство одбране, Министарство унутрашњих послова, Министарство спољних послова, Безбедносноинформативна агенција и слично) потребно је проширити надлежности интерне ревизије или FUK-а (Финансијско Управљање Контроле) у сегменту безбедности информација - унутрашње контроле за рад са тајним подацима. Наравно, да би се успоставила унутрашња контрола потребно је отпочети процес implementације Закона о тајности података, одредити руковођа тајних података и doneti све потребне одлуке.

Руководилац тајним подацима никako не може бити и унутрашња контрола.

Указујемо да је руководиоца органа јавне власти уједно и унутрашња контрола док не успостави систем унутрашње контроле.

Сва лица укључена у процес рада са тајним подацима било да обављају послове руковођаца или унутрашње контроле или да су само корисници тајних података у органу јавне власти морају поседовати одговарајући сертификат и проћи едукације за рад са тајним подацима

* Детаљније погледати скрипту Систем заштите тајних података

(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta.pdf)

* Priručnik unutrašnja kontrola nad radom sa tajnim podacima
(https://nsa.gov.rs/extfile/sr/1761/Unutrasnja_kontrola_nad_radom_sa_tajnim_podacima.pdf)

STRUČNI NADZOR

Na osnovu čl. 86 Zakona o tajnosti podataka Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka ima u nadležnosti određene poslove sprovođenja i kontrole primene ovog zakona i nadzor nad sprovođenjem zakona.

Stručni nadzor se vrši na zahtev/molbu organa javne vlasti koji se pisanim putem upućuje Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.

Nastao je kao rezultat potrebe organa javne vlasti da verifikuju svoje rezultate u implementaciji Zakona o tajnosti podataka.

On logički i metodološki treba da sledi nakon pune implementacije Zakona o tajnosti i nakon izvršene unutrašnje kontrole.

Ne predstavlja inspeksijski nadzor – inspeksijski nadzor je u celini u nadležnosti Ministarstva pravde.

Stručni nadzor Kancelarije Saveta ima za cilj da utvrdi da li je i u kojoj meri u organu javne vlasti implementiran Zakon o tajnosti podataka, da li su u organu javne vlasti na adekvatan način primenjene opšte i posebne mere zaštite tajnih podataka kao i da da odgovarajuće preporuke za unapređenje stanja zaštite tajnih podataka u organu javne vlasti

Prilikom vršenja stručnog nadzora ceni se funkcionisanje celokupnog sistema zaštite tajnih podataka u organu javne vlasti sa naglaskom na:

Status implementacije zakona u organu javne vlasti – (podrazumeva između ostalog i donošenje Odluke o određivanju rukovaoca, Odluke o određivanju TP, Odluke o određivanju unutrašnje kontrole i Liste potrebno da zna, a na osnovu godišnjeg Izveštaja), Personal za rukovanje podacima,Infrastrukturu za smeštaj i čuvanje podataka,Tehničke sisteme za zaštitu i obradu podataka,Regulativu za zaštitu podataka

Nakon sprovedenog nadzora, utvrđuje se činjenično stanje i donosi opšti zaključak o izvršenom stručnom nadzoru po segmentima, sa kojim se upoznaju lica u organu javne vlasti i pozivaju se da (dok traje nadzor) daju odgovarajuće komentare ukoliko ih imaju. Na osnovu čeka liste i komentara sastavlja se Izveštaj o izvršenom nadzoru koji se dostavlja organu javne vlasti uz poziv da se primećeni nedostaci otklone.

Napominjemo da organ javne vlasti ne može samostalno utvrđivati da li ispunjava zakonom predviđene uslove za rad sa tajnim podacima, odnosno to je težišni zadatak Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka koji se i realizuje vršenjem stručnog nadzora i kontrole u smislu člana 86 Zakona o tajnosti podataka.

PRIMERI LOŠE PRAKSE SISTEMA RADA SA TAJNIM PODACIMA

1. Pristup tajnim podacima bez institucionalnog okvira i organizacione bezbednosti -krivično delo iz člana 98. Zakona o tajnosti podataka
2. Tretiranje tajnih podataka i dokumenata kao otvorenih i ličnih podataka - krivično delo iz člana 98. Zakona o tajnosti podataka
3. Zaposleni bez sertifikata pristupaju tajnim podacima - krivično delo iz člana 98. Zakona o tajnosti podataka
4. Lica bez ovlašćenja starešine organa javne vlasti kreiraju tajne podatke - prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka
5. Nepostojanje procedura implementacije Zakona o tajnosti podataka - prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka
6. Rad sa tajnim podacima na informacionim sistemima koji su priključeni na internet- prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka
7. Neuspostavljanje prostora (bezbednosnih zona) za čuvanje tajnih podataka i nenabavljanje odgovarajuće opreme - prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka
8. Sprovođenje poverljivih nabavki bez utvrđene procedure rada sa tajnim podacima i ustupanje tajnih podataka pravnim licima bez odgovarajućeg sertifikata (bezbednosne akreditacije prostora i zaposlenih) - krivično delo iz člana 98. Zakona o tajnosti podataka; prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka
9. Objavljivanje tajnih podataka u medijima bez procedure skidanja oznake tajnosti- krivično delo iz člana 98. Zakona o tajnosti podataka
10. Nepostojanje funkcionalnog rukovaoca tajnih podataka i sistema unutrašnje kontrole rada sa tajnim podacima u organu javne vlasti - prekršaj iz člana 99. tačka

16. Zakona o tajnosti podataka; prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka (vezuje se za član 32. stav 1. tačka 5. Zakona o tajnosti podataka)
11. Nepropisno označavanje tajnih podataka, bez odgovarajuće odluke i bez kriterijuma za određivanje tajnosti – prekršaj iz člana 99. tačka 3. Zakona o tajnosti podataka
12. Neuspostavljanje sistema edukacija u radu sa tajnim podacima na nivou organa javne vlasti - prekršaj iz člana 100. Zakona o tajnosti podataka
13. Nesistematizovanje radnih mesta koja imaju pristup tajnim podacima u organu javne vlasti - prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka
14. Prosleđivanje tajnih podataka drugim organima javne vlasti bez odgovarajuće procedure „POTREBNO PODELITI SA“ i bez kurirske dostave
- prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka (vezuje se za član 32. stav 1. tačka 3. Zakona o tajnosti podataka)
15. Razgovor o tajnim podacima sa licima koja nisu sertifikovana i izvan odgovarajuće bezbednosne zone (npr. u restoranu, na ulici, u hodniku ili toaletu...) - krivično delo iz člana 98. Zakona o tajnosti podataka
16. Uvođenje stranih državljana u administrativne ili bezbednosne zone bez odluke starešine organa javne vlasti - krivično delo iz člana 98. Zakona o tajnosti podataka
17. Ustupanje tajnih podataka nepozvanim licima, bez odgovarajuće procedure i odluka – krivično delo iz člana 98. Zakona o tajnosti podataka
18. Unošenje mobilnih telefona, laptopova, usb-ova i slično u bezbednosne zone bez procedure i odobrenja - prekršaj iz člana 99. tačka 11. Zakona o tajnosti podataka

PRIMERI LOŠE PRAKSE PORED KRIVIČNOG DELA I PREKRŠAJA PREDSTAVLJAJU I UGROŽAVANJE NACIONALNE BEZBEDNOSTI REPUBLIKE SRBIJE.

GODIŠNJI IZVEŠTAJ O RADU SA TAJNIM PODACIMA U REPUBLICI SRBIJI

Godišnji izveštaj o radu sa tajnim podacima u Republici Srbiji neophodno je da sadrži sledeće:

1. Status implementacije Zakona o tajnosti podataka u vašoj organizaciji; videti više - https://nsa.gov.rs/extfile/sr/1791/Neophodni_koraci-Implementacija_ZTP_u_organu_JV_.pdf
2. Broj kreiranih tajnih podataka u organu javne vlasti u izveštajnom periodu, po stepenima tajnosti;
3. Aktivnosti vašeg organa u skladu sa članom 94. stav 2. i 3. Zakona o tajnosti podataka - izveštaj koji sadrži brojčane pokazatelje o razmeni tajnih podataka sa stranom državom ili međunarodnom organizacijom.

Organi javne vlasti u svom izveštaju treba da navedu u kojoj je fazi implementacija Zakona o tajnosti podataka u njihovom organu, odnosno koji su koraci preduzeti kako bi se zakon implementirao. To se prvenstveno odnosi na dostavljanje podataka o uređenim internim normativnim i bezbednosnim procedurama (između ostalog, donete odluke o određivanju rukovaoca tajnim podacima, odluke o određivanju stepena tajnosti dokumenata kao i sačinjene liste „POTREBNO DA ZNA“), shodno pozitivnom zakonodavstvu kojim je uređen rad sa tajnim podacima u Republici Srbiji. Takođe, potrebno je navesti da li je formirana unutrašnja organizaciona jedinica za vršenje unutrašnje kontrole u organu javne vlasti, te da li su vršene unutrašnje kontrole.

Ukoliko u vašem organu nije implementiran zakon, nije rađeno sa tajnim podacima odnosno nije vršena razmena tajnih podataka, potrebno je da to navedete u vašem dopisu. Takođe, ukoliko smatrate da postoji potreba da se u budućnosti radi sa tajnim podacima u vašem organu, potrebno je da odredite kontakt osobu kako bi vam Kancelarija Saveta pružila neophodnu stručnu pomoć u implementaciji zakona i podzakonskih akata koji regulišu oblast zaštite tajnih podataka u Republici Srbiji.

Zbog potrebe da se adekvatno prati rad sa tajnim podacima u Republici Srbiji, u skladu sa zakonom, potrebno je da svaki organ javne vlasti dostavi broj tajnih podataka koje je kreiran u organu, odnosno da se iskaže broj dokumenata na koji

je stavljena oznaka tajnosti, po stepenima tajnosti. Ukoliko organ javne vlasti nije kreirao tajne podatke, dovoljno je da se to konstatuje u izveštaju.

Implementacija Zakona i uspostavljanje jedinstvenog sistema rada sa tajnim podacima na nacionalnom nivou, preduslov je za rad sa stranim tajnim podacima.

KO JE U OBAVEZI DA DOSTAVI GODIŠNJI IZVEŠTAJ

Shodno Zakonu o tajnosti podataka Godišnji izveštaj o radu sa tajnim podacima su u obavezi da dostave svi organi javne vlasti, organi teritorijalne autonomije, organi jedinice lokalne samouprave, organizacija kojoj je povereno vršenje javnih ovlašćenja, kao i pravno lice koje osniva državni organ ili se finansira u celini, odnosno u pretežnom delu iz budžeta, a koja učestvuju u izradi i realizaciji Plana odbrane Republike Srbije.

„Nepoštovanje i neimplementacija Zakona o tajnosti podataka predstavlja kršenje nacionalne bezbednosti i nanošenje štete interesima Republike Srbije“

POJMOVNIK O RADU SA TAJNIM PODACIMA

1. **Administrativna bezbednost** je adekvatna i efikasna klasifikacija i zaštita zvaničnih informacija koje zahtevaju zaštitu u interesu nacionalne bezbednosti kao i njihova deklasifikacija kada više ne zahtevaju zaštitu.
2. **Administrativna zona** je prostor ili prostorija u kojoj se obrađuju i čuvaju tajni podaci stepena tajnosti „INTERNO”.
3. **Akreditacija ikt sistema** podrazumeva da IKT sistemi koji obrađuju tajne podatke moraju biti akreditovani od strane Ministarstva odbrane u vezi sa tehnološkim aspektima i krypto opremom. Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka vrši bezbednosnu akreditaciju tih IKT sistema kako bi se osiguralo da su u skladu sa najvišim bezbednosnim standardima
4. **Aktiviranje containment mera:** Ove mere podrazumevaju brzu reakciju kako bi se incident izolovao i sprečilo dalje širenje oštećenja.
5. **Alarmni uređaji** su uređaji koji služe za obezbeđivanje objekta i predmeta, tako što zvučnim ili svetlosnim signalom upozoravaju na nedozvoljenu aktivnost. Mogu biti mehanički, električni i elektronski.
6. **Apsolutne smetnje** (neposredni razlog za uskraćivanje sertifikata) - Ovo su zdravstveni problemi koji automatski diskvalifikuju osobu, jer predstavljaju trajan ili težak rizik po bezbednost.
7. **Arhivska građa** jeste celina dokumenata ili zapisa nastalih ili primljenih delovanjem i radom subjekata u izvornom ili reprodukovanom obliku dokumenta, bez obzira na formu i format beleženja, kao i propisane evidencije o njemu.
8. **Autentičnost** je svojstvo koje znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarirano da je tu radnju izvršio.
9. **Autentifikacija** – proces verifikacije identiteta korisnika, sistema ili uređaja pre odobravanja pristupa tajnim podacima.
10. **Autorizacija** – proces određivanja prava i privilegija korisnika nakon uspešne autentifikacije.
11. **Accountability („odgovornost i praćenje postupanja“)** – svako lice koje rukuje tajnim podacima mora biti u potpunosti odgovorno za svoje postupke u vezi sa tim podacima, a organ je u obavezi da obezbedi sistem nadzora, praćenja i evidentiranja aktivnosti.
12. **Bezbednosna akreditacija** - obuhvata fizičku i administrativnu zaštitu podataka, kao što su kontrola pristupa, obuka zaposlenih i primena mera zaštite. Sprovodi je Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka i druge institucije, u zavisnosti od vrste sistema.
13. **Bezbednosna zona I stepena** je prostor ili prostorija u kojoj se obrađuju i čuvaju tajni podaci stepena tajnosti „DRŽAVNA TAJNA”, „STROGO POVERLjIVO” i „POVERLjIVO”. Samim ulaskom u ovu zonu smatra se da je ostvaren pristup tajnim podacima.

14. **Bezbednosna zona II stepena** je prostor ili prostorija u kojoj se obrađuju i čuvaju tajni podaci stepena tajnosti „DRŽAVNA TAJNA”, „STROGO POVERLJIVO” i „POVERLJIVO”.
15. **Bezbednosna kultura** je bezbednosna aktivnost koja izražava spremnost delovanja i ponašanja u skladu sa stečenim znanjima i veštinama, kao i u skladu sa prihvaćenim vrednosnim stavovima. Ogleda se u prepoznavanju opasnosti, reagovanju na njih izbegavanjem opasnosti, otklanjanjem opasnosti ili upućivanjem na one subjekte koji će profesionalno reagovati i sačuvati ugrožene vrednosti.
16. **Bezbednosna provera** je postupak koji pre izdavanja sertifikata za pristup tajnim podacima sprovodi nadležni organ, u cilju prikupljanja podataka o mogućim bezbednosnim rizicima i smetnjama u pogledu pouzdanosti za pristup tajnim podacima.
17. **Bezbednosna svest** podrazumeva znanje i stav koji članovi organizacije imaju u pogledu zaštite određenih vrednosti – nacionalne bezbednosti, odbrane, unutrašnjih i spoljnih poslova, ljudskih sloboda i prava, kao i fizičke i intelektualne imovine, a posebno informacija i podataka kojima raspolaže organizacija (organ javne vlasti, pravno lice ili kompanija).
18. **Bezbednosna smetnja** predstavlja činjenicu koja onemogućava izdavanje sertifikata.
19. **Bezbednosne procedure** su propisana pravila za postupanje lica u radu sa tajnim podacima.
20. **Bezbednosni brifing** predstavlja upoznavanje sa propisima kojima se uređuje tajnost podataka i posledicama neovlašćenog pristupa i korišćenja tajnih podataka.
21. **Bezbednosni incident** dešava se kada postoji stvarni ili potencijalni rizik za štićene podatke i dalje kategorisan kao krivično delo ili prekršaj.
22. **Bezbednosni rizik** je stvarna mogućnost narušavanja bezbednosti tajnih podataka.
23. **Bezbednosni upitnik** je sastavni deo dokumentacije u postupku izdavanja sertifikata za pristup tajnim podacima.
24. **Bezbednost** označava stanje nekog subjekta (pojedince, grupe ljudi, zajednice, institucije) koje karakteriše odsustvo nevolja, briga, nesreća, opasnosti i drugih zla.
25. **Blokada pristupa:** Za sprečavanje daljih oštećenja, neophodno je ograničiti pristup ugroženim podacima i preduzeti tehničke mere kao što su lock-out i povlačenje dokumenata.
26. **Vodič za postupanje u slučaju incidenta sa tajnim podacima** predstavlja ključni instrument za adekvatno upravljanje situacijama koje ugrožavaju bezbednost i integritet zaštićenih podataka u okviru organa javne vlasti i pravnih lica.
27. **Gubitak poverenja** - Nedostatak adekvatne zaštite tajnih podataka može dovesti do značajnog gubitka poverenja u organe javne vlasti.

28. **Data Breach/Kompromitacija podataka** je bezbednosni incident u kome se osetljivi, zaštićeni ili poverljivi podaci kopiraju, prenose, gledaju, krađu ili koriste od strane pojedinca koji je neovlašćen za pristup tim podacima.
29. **Debrifing** podrazumeva upoznavanje sa propisima i obavezama po prestanku potrebe za pristupom tajnim podacima po različitim osnovama.
30. **Direktiva 488/2001/EC Evropskog parlamenta i Saveta** odnosi se na zaštitu klasifikovanih informacija koje se stvaraju i obrađuju u Evropskoj uniji, i predstavlja pravni okvir za regulisanje bezbednosti i razmene klasifikovanih podataka između država članica i institucija EU. Ova direktiva postavlja standarde koji se odnose na obradu klasifikovanih informacija u državama članicama, kao i na postupke vezane za bezbednost, komunikaciju i razmenu tih informacija. Direktiva propisuje pravila za pristup klasifikovanim informacijama, što podrazumeva da osobe koje imaju pristup klasifikovanim podacima moraju proći bezbednosne provere.
31. **Digitalni potpis** – kriptografski mehanizam koji obezbeđuje autentičnost, integritet i neporecivost digitalnog dokumenta.
32. **Dokument** je svaki nosač podatka (papir, magnetni ili optički medij, disketa, USB memorija, smart kartica, kompakt disk, mikrofilm, video i audio zapis i dr.), na kome je zapisan ili memorisan tajni podatak.
33. **Donošenje formalne odluke o tajnosti** - Organ javne vlasti je u obavezi da donese generičnu ili pojedinačnu pismenu odluku o određivanju stepena tajnosti podataka, uz procenu uticaja i potencijalne štete po interese Republike Srbije u slučaju otkrivanja, zloupotrebe ili uništenja podataka. Tajnost podatka, pod uslovima i na način utvrđen zakonom o tajnosti podataka, određuje ovlašćeno lice.
34. **Dostavnica** je potvrda o tome da je lično ili posredno dostavljanje izvršeno koja sadrži lično ime i adresu lica i podatke kojima se identifikuje uručeno pismo.
35. **Evidencije** podrazumevaju da organ javne vlasti mora voditi evidencije o određenim stepenima tajnosti, pristupu tajnim podacima, obuci zaposlenih, incidentima vezanim za bezbednost, revizijama bezbednosnih mera i uništavanju tajnih podataka.
36. **Evidenciju korisnika tajnih podataka** je evidencija koju vodi rukovalac tajnim podacima u organu javne vlasti.
37. **Etički aspekti bezbednosnih provera medicinskih podataka** uključuju zaštitu privatnosti, izbegavanje diskriminacije, osiguranje informisanog pristanka, jasne i pravедne ciljeve, kao i minimizaciju intervencije.
38. **Žalba** je pravno sredstvo u upravnom postupku koje se može izjaviti protiv upravnog akta tj. protiv prvostepenog rešenja.
39. **Zavisnost od informaciono-komunikacionih tehnologija (IT)** - podrazumeva prekomernu upotrebu digitalnih alata, kao što su mobilni telefoni, računari, društvene mreže ili video igre, koja može dovesti do 16 poremećaja koncentracije, smanjene produktivnosti ili čak psiholoških problema.

40. **Zavisnost od kocke (pataljije)** - može biti problem koji utiče na pojedinca u različitim aspektima života, uključujući i njegov radni učinak i ponašanje u situacijama koje zahtevaju visok nivo odgovornosti i pažnje, kao što je rad sa klasifikovanim informacijama.
41. **Zavisnost od seksa ili seksualna zavisnost**, koja se karakteriše prekomernom i nekontrolisanom potrebom za seksualnim aktivnostima koja može biti psihološki i fizički štetna, može se razmatrati kao faktor u bezbednosnim proverama za pristup klasifikovanim informacijama, ali kao i kod drugih zavisnosti, njen uticaj zavisi od ozbiljnosti i posledica koje ona ima na pojedinca.
42. **Zaštita podataka** je skup različitih tehnoloških metoda kojima se digitalni podaci štite tokom procesa digitalnog prenosa podataka ili digitalne komunikacije.
43. **Zloupotreba informacija** - Neovlašćeni pristup tajnim podacima može dovesti do izvoza osetljivih informacija i korišćenja od strane stranaka koje imaju neprijateljske namere prema Srbiji.
44. **Zloupotreba tajnih podataka** - Lice koje zloupotrebi tajne podatke, bilo da ih deli, prodaje ili na neki drugi način koristi protiv nacionalne bezbednosti, može biti osuđeno na kazne zatvora.
45. **Zoniranje** - predstavlja sistematsku podelu prostoriya u zone različitih nivoa bezbednosti u skladu sa Zakonom o tajnosti podataka, Uredbom o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima i Uredbom o posebnim merama fizičko-tehničke zaštite tajnih podataka.
46. **Identifikacija kategorija podataka** - Podaci se analiziraju kako bi se utvrdilo da li ispunjavaju uslove za označavanje kao tajni, uključujući propisima predviđene kategorije podataka, kao i procenu mogućeg uticaja na nacionalnu bezbednost, javni interes, teritorijalni integritet i ekonomske interese. U ovom koraku se takođe razmatra i opšti značaj podataka, kao i posledice koje bi njihovo otkrivanje moglo imati na rad organa javne vlasti.
47. **Izjava** čini sastavni deo dokumentacije na osnovu koje je izdat sertifikat za pristup tajnim podacima, odnosno dozvola.
48. **Industrijska bezbednost** predstavlja primenu mera radi obezbeđenja zaštite tajnih podataka, od strane izvođača ili podizvođača, u pregovorima koji prethode zaključivanju ugovora i tokom celog veka trajanja tajnih/poverljivih ugovora.
49. **Insajder** (eng. insider - "neko unutra") je naziv za osobu koja je pripadnik neke društvene grupe zbog čega raspolaže određenim saznanjima nedostupnim široj javnosti.
50. **Integritet** znači očuvanost izvornog sadržaja i kompletnosti podataka;
51. **Interna kontrola** predstavlja mere pažnje usmerene na sprečavanje grešaka, prekomernih troškova i prevare, proverava i obezbeđuje pouzdanost informacija.
52. **Informanti** su lica koja slučajno i prigodno saznaju za planirana ili izvršena krivična dela i njihove učinioce.

53. **Informatori** (pouzdanik, vigilan i agent provokator) su osobe spremne da duže vreme policiji pružaju kriminalistički i krivično pravne relevantne informacije, pri čemu se njihov identitet čuva u tajnosti.
54. **Informaciona bezbednost** predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem ikt sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.
55. **Informaciona bezbednost tajnih podataka** obuhvata integrisani skup međuzavisnih mera i aktivnosti usmerenih na zaštitu tajnih informacija koje se obrađuju u komunikaciono-informacionim sistemima – KIS.
56. **Informaciona garancija** predstavlja garanciju od strane organa javne vlasti ili pravnog lica da će adekvatno štititi podatke od neovlašćenog pristupa, korišćenja, deljenja ili zloupotrebe uz poštovanje propisa i standarda za zaštitu podataka.
57. **ISO/IEC 27001** je međunarodni standard za upravljanje bezbednošću informacija. Detaljno opisuje zahteve za uspostavljanje, implementaciju, održavanje i kontinuirano poboljšanje sistema upravljanja bezbednošću informacija (ISMS) – čiji je cilj da pomogne organizacijama da učine bezbednijom informacionu imovinu koju drže.
58. **Javni podaci** su koncept u kome određeni podaci treba da budu slobodno dostupni svima na korišćenje i ponovnu upotrebu, bez autorskih ili bilo kakvih drugih ograničenja.
59. **Kemz (Kompromitacija elektromagnetnim zračenjem)**- predstavlja širi koncept koji obuhvata tehničke i organizacione mere za sprečavanje curenja podataka putem elektromagnetnih emisija.
60. **Klasifikacija incidenata** - U skladu sa odredbama Zakona o tajnosti podataka („Sl. glasnik RS“, br. 72/2009), incidenti u sistemu zaštite tajnih podataka klasifikuju se prema stepenu rizika po zaštićene interese i vrsti povrede zakona. U najširem smislu, svaka kompromitacija štićenih podataka podrazumeva neovlašćen pristup, otkrivanje, izmenu, uništavanje ili gubitak podataka, što predstavlja povredu osnovnih principa zaštite i može dovesti do ozbiljnih posledica po javne organe, pravna lica ili pojedince.
61. **Kompromitacija tajnog podatka** predstavlja umišljajno, nehatno ili nemarno otkrivanje tajnih podataka nepozvanim i neovlašćenim licima.
62. **Kompromitacija štićenih podataka u najširem smislu** (tajnih podataka, ličnih podataka, bankarske tajne, poreske tajne, poslovne i profesionalne tajne) nastaje kada dođe do neovlašćenog otkrivanja, pristupa, izmene, uništenja ili gubitka podataka, čime se ugrožava njihova poverljivost, integritet ili dostupnost. Takvi događaji mogu prouzrokovati ozbiljnu štetu po organ javne vlasti, pravno lice, organizaciju ili pojedinca.
63. **Kontrolna lista u slučaju incidenta** - Organi javne vlasti i pravna lica se ohrabruju da primenjuju unapred definisanu listu za proveru, kao alat za brzo i efikasno reagovanje u slučaju incidenta.

- 64. Kontraobaveštajna zaštita** je poseban vid obaveštajne aktivnosti čiji je cilj zaštita tajnih podataka sopstvene države, zaštita vitalnih državnih organa i institucija, sprečavanje delovanja protivničkih obaveštajnih službi na teritoriji svoje zemlje i drugo.
- 65. Korisnik tajnog podatka** je državljanin Republike Srbije ili pravno lice sa sedištem u Republici Srbiji, kome je izdat sertifikat od strane nadležnog organa, odnosno strano fizičko ili pravno lice kome je na osnovu zaključenog međunarodnog sporazuma izdata bezbednosna dozvola za pristup tajnim podacima, kao i funkcioner organa javne vlasti koji na osnovu ovog zakona ima pravo pristupa i korišćenja tajnih podataka bez izdavanja sertifikata.
- 66. Krivično delo (Krivična odgovornost):** Incident koji je doveo ili mogao doveći do kompromitacije tajnih podataka, uključujući: • neovlašćeno saopštavanje, predaja ili omogućavanje pristupa tajnim podacima, • gubitak, uništenje ili otkrivanje dokumenata koji sadrže tajne podatke, • pribavljanje tajnih podataka bez odobrenja.
- 67. Krivično delo** je bezbednosni incident koji bi razumno mogao da dovede ili jeste doveo do gubitka ili kompromitovanje štićenih podataka i zahteva istragu radi dalje analize i pokretanja krivičnog postupka.
- 68. Kriptografski proizvod** je softver ili uređaj putem koga se vrši kriptozastita.
- 69. Kriptozastita** je primena metoda, mera i postupaka radi transformisanja podataka u oblik koji ih za određeno vreme ili trajno čini nedostupnim neovlašćenim licima.
- 70. Kontinuirani nadzor:** Proces, ne samo stanje.
- 71. Lanac čuvanja (Chain of custody)** – dokumentovan proces praćenja fizičkog ili digitalnog tajnog podatka od trenutka njegovog nastanka do čuvanja, prenosa ili uništenja, radi očuvanja dokazne vrednosti.
- 72. Lista “POTREBNO DA ZNA”** predstavlja međunarodni princip rada sa tajnim podacima koji podrazumeva spisak lica i radnih mesta koji imaju pristup tajnim podacima u okviru organa javne vlasti/ princip dvostrukog ključa pristupu tajnim podacima.
- 73. Lista “POTREBNO PODELITI SA”** predstavlja međunarodni princip rada sa tajnim podacima koji podrazumeva spisak organa javne vlasti koji međusobno razmenjuju tajne podatke.
- 74. Lični podatak** je svaki podatak koji se odnosi na fizičko lice čiji je identitet neposredno ili posredno određen ili odrediv-posebno na osnovu oznake identiteta. Lični podatak je svaka informacija koja se odnosi na fizičko lice koje se u nekom trenutku može identifikovati; to je karakteristična osobina svake pojedinačne osobe.
- 75. Lojalnost** je značenje izvedeno preko sinonima: odanost, vernost, ispravnost, podanička vernost, čestitost, časnost, privrženost, poverljivost, postojanost, nepromenljivost, iskrenost, poštenje.
- 76. Logovanje i nadzor (logging & monitoring)** – kritično za detekciju incidenata.

77. **Mere zaštite IKT sistema** su tehničke i organizacione mere za upravljanje bezbednosnim rizicima IKT sistema.
78. **Mere zaštite** su opšte i posebne mere koje se preduzimaju radi sprečavanja nastanka štete, odnosno mere koje se odnose na ostvarivanje administrativne, informatičko-telekomunikacione, personalne i fizičke bezbednosti tajnih podataka i stranih tajnih podataka.
79. **Multifaktorska autentifikacija (MFA)** – metod autentifikacije koji zahteva dva ili više nezavisnih faktora (npr. lozinka + jednokratni kod).
80. **Nadležnost** predstavlja pravo i dužnost donošenja odluka koje se odnose na upravljanje delegiranim resursima (ljudskim, budžetskim, tehnikom i tajnim podacima) da bi se ostvarili ciljevi nacionalne i organizacione bezbednosti, odnosno sistema zaštite tajnih podataka.
81. **NATO standard S-M (2002) 49** podrazumeva da bezbednosne provere obuhvataju različite aspekte kandidata, uključujući: • Krivičnu istoriju. • Psihološke procene. • Medicinske procene.
82. **NATO RESTRICTED, EU CONFIDENTIAL i sl.** – stepeni tajnosti u međunarodnim sistemima (važno ako se razmenjuju podaci sa NATO-om, EU-om itd.).
83. **Nedopuštena izmena ili uništavanje tajnih podataka**- Lica koja unište, izmene ili na neki način ometaju očuvanje tajnih podataka, kao i lica koja ne preduzmu propisane mere zaštite podataka, mogu biti krivično sankcionisana.
84. **Neovlašćeno otkrivanje tajnih podataka**- Lice koje bez ovlašćenja otkrije tajne podatke ili ih koristi u nezakonite svrhe, može biti krivično gonjeno.
85. **Nepovoljna istorija u radu sa tajnim podacima** – Ranije povrede pravila o zaštiti tajnih podataka ili neodgovorno postupanje sa poverljivim informacijama (poslovna tajna, profesionalna tajna...)
86. **Neporecivost** predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći.
87. **Nepouzdanost vlasničke strukture** – Ako se utvrdi da su vlasnici ili osnivači pravnih lica povezani sa rizičnim subjektima, stranim uticajem ili kriminalnim grupama.
88. **Nepouzdanost i nestabilnost** – Procena da kandidat nije dovoljno odgovoran, finansijski stabilan (dugovi, česte promene radnih mesta), ili da ima druge lične karakteristike koje ga čine podložnim pritisku ili uceni.
89. **Obaveza obaveštavanja** - Sva lica koja na bilo koji način rade sa tajnim podacima imaju neodložnu obavezu da prijave svaki bezbednosni incident ili sumnju na povredu mera zaštite. Obaveštavanje se vrši neposredno nadređenom, ovlašćenom licu za zaštitu tajnih podataka ili rukovodiocu organa. U zavisnosti od težine i prirode incidenta, obaveštavaju se i Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, službe bezbednosti (BIA ili VBA u skladu sa nadležnostima) ili nadležno tužilaštvo.

90. **Obezbeđenje** je planska primena i korišćenje operativno-taktičkih metoda, mera, radnji, sredstva i snaga radi zaštite od ugrožavanja određenih ličnosti, ljudi, masovnih skupova, imovine, otvorenog-zatvorenog prostora, fabričkih hala, magacina ili drugih objekata.
91. **Obrada podataka** je generalno, "prikupljanje i upotreba podataka radi stvaranja smislene informacije".
92. **Obuka i svest (TRAINING & AWARENESS):** Kritičan element personalne bezbednosti.
93. **Ovlašćeno lice za određivanje tajnosti podataka (proizvođač)** podrazumeva da kreator tajnih podataka može biti svako lice koje ima odgovarajući bezbednosni sertifikat i koje prema svojim dužnostima i zadacima treba da kreira, tj. rukuje tajnim podacima - informacijama.
94. **Odgovornost** kada je u pitanju sistem zaštite tajnih podataka i organizaciona bezbednost, predstavlja obavezu da se davaocu ovlašćenja odgovara za ispunjavanje tih ovlašćenja (obaveza postupanja). Odgovornost obuhvata i davanje informacija i obrazloženja za sprovođenje određenih postupaka, aktivnosti ili odluka, kada je u pitanju rad sa tajnim podacima.
95. **Odluka o određivanju rukovaoca tajnim podacima u organu javne vlasti** je odluka kojom se određuje se rukovalac tajnim podacima u organu javne vlasti.
96. **Odluka o određivanju tajnih podataka u Organu javne vlasti** je odluka kojom se određuju se tajni podaci u Organu javne vlasti što uključuje i utvrđivanje stepena i roka tajnosti.
97. **Određivanje tajnih podataka** je postupak kojim se podatak, u skladu sa ovim zakonom, određuje kao tajni i za koji se utvrđuje stepen i rok tajnosti.
98. **Označavanje podataka** - Podaci dobijaju jasnu oznaku koja uključuje stepen tajnosti, način prestanka tajnosti, podatke o ovlašćenom licu, datum označavanja, naziv organa koji je doneo odluku i pravnu osnovu.
99. **Označavanje stepena tajnosti** je označavanje tajnog podatka oznakama: "DRŽAVNA TAJNA", "STROGO POVERLJIVO", "POVERLJIVO" ili "INTERNO".
100. **Organ javne vlasti** je državni organ, organ teritorijalne autonomije, organ jedinice lokalne samouprave, organizacija kojoj je povereno vršenje javnih ovlašćenja, kao i pravno lice koje osniva državni organ ili se finansira u celini, odnosno u pretežnom delu iz budžeta, a koji postupi sa tajnim podacima, odnosno koji ih stvara, pribavlja, čuva, koristi, razmenjuje ili na drugi način obrađuje.
101. **Organizacione mere zaštite** predstavljaju organizaciju zaštite procesa rada i funkcionisanja informaciono-komunikacionog sistema u redovnim okolnostima i vanrednim situacijama.
102. **Organizacioni uslovi** odnose se naročito na organizaciju procesa rada, zaštitu pristupa tajnim podacima, zaštitu od neovlašćenog korišćenja tajnih podataka, određivanje odgovornog lica zaduženog za sprovođenje mera zaštite, kao i utvrđivanje postupka u slučaju vanrednih i hitnih okolnosti.

- 103. Podatak o ličnosti** je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta.
- 104. Patroliranje** je usluga obezbeđenja koju vrše službenici obezbeđenja krećući se u određeno vreme između više međusobno razdvojenih mesta/objekata.
- 105. Perimetar je deo fizičke bezbednosti** koji se mora postaviti oko objekata u kojima se nalazeštićeni podaci, kako bi se sprečilo neovlašćen pristup.
- 106. Personalna bezbednost** predstavlja niz procedura čiji je osnovni cilj da se utvrdi da li neko lice može biti ovlašćeno da dobije pristup tajnim podacima a da pri tome ne predstavlja neprihvatljiv rizik za bezbednost.
- 107. Plan zaštite tajnih podataka** u organu javne vlasti – je osnovni stub organizacione bezbednosti u svakom organu javne vlasti. On omogućava pravilno upravljanje tajnim podacima i osigurava njihovu zaštitu, što je od ključnog značaja za očuvanje nacionalne bezbednosti. Iako sam Plan nije direktno propisan Zakonom o tajnosti podataka, on se smatra implicitno obaveznim kao deo kompletnog sistema zaštite tajnih podataka, koji mora biti u skladu sa važećim zakonima i propisima.
- 108. Plan postupanja u vandrednim situacijama** obuhvata procedure i mere koje treba preduzeti u slučaju napada, zloupotrebe ili drugij vandrednih situacija koje ugrožavaju bezbednost podataka.
- 109. Povreda radne discipline (Disciplinska odgovornost):** Incident koji ne dovodi do kompromitacije tajnih podataka, ali predstavlja nezakonito ili nesavesno postupanje u vršenju službene dužnosti.
- 110. Podatak od interesa za Republiku Srbiju** je svaki podatak ili dokument kojim raspolaže organ javne vlasti, koji se odnosi na teritorijalni integritet i suverenost, zaštitu ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalnu i javnu bezbednost, odbranu, unutrašnje poslove i spoljne poslove.
- 111. Poslovna tajna** je podatak koji može da ima ekonomsku vrednost. Ova vrsta podataka nije opšte poznata niti lako dostupna trećim licima. Bankarska tajna je primer poslovne tajne, ali njena specifičnost jeste da ista prelazi u više kategorija (profesionalna tajna, lični podaci).
- 112. Postupci zbog povreda radne discipline:** Odgovorna lica koja su prekršila procedure mogu biti predmet disciplinskih mera, kao što su opomena, suspenzija ili otkaz.
- 113. Pravne implikacije** - Kada dođe do kršenja procedura označavanja i zaštite tajnih podataka, mogu se pokrenuti i pravni postupci protiv odgovornih lica.
- 114. Pravno lice** ima registrovano sedište na teritoriji Republike Srbije;obavljanje delatnosti u vezi sa interesima iz člana 8. ovog zakona; postojanje odgovarajuće bezbednosne provere; ako nije u postupku likvidacije ili stečaja; nije kažnjavano merom zabrane vršenja delatnosti,

odnosno da mu nije izrečena kazna prestanka pravnog lica ili mere bezbednosti zabrane obavljanja određenih registrovanih delatnosti ili poslova, uredno izmirenje poreskih obaveza i doprinosa;

115. **Pravovremeno, transparentno i sistematizovano postupanje u slučaju incidenta** predstavlja jedan od osnovnih stubova sistema zaštite tajnih podataka. Ovakve procedure moraju biti deo Plana zaštite tajnih podataka, uključujući i evidenciju svih prijavljenih incidenata, analiza uzroka i izveštavanje prema nadležnim institucijama.
116. **Praćenje stanja sertifikata** obuhvata praćenje izdatih sertifikata za fizička i pravna lica, uključujući proveru valjanosti sertifikata u kontekstu njihovog pristupa tajnim podacima.
117. **Prekršaj (Prekršajna odgovornost):** Incident koji nije doveo do kompromitacije tajnih podataka, ali ukazuje na propuste u primeni propisanih mera zaštite.
118. **Prestanak tajnosti:** Proces ukidanja tajnosti (ovde je spomenuta, ali bi mogla imati posebnu definiciju).
119. **Prekršajni postupci:** Ukoliko je došlo do prekršaja u smislu nepravilnog čuvanja ili postupanja sa tajnim podacima, mogu se izreći novčane kazne ili druge mere kao što su upozorenje ili javna opomena.
120. **Princip minimizacije podataka** – relevantan za obradu tajnih podataka.
121. **Provera medicinskih podataka** je ključan aspekt bezbednosne provere jer omogućava procenu da li kandidat ima mentalne, neurološke ili druge zdravstvene smetnje koje mogu uticati na njegovu sposobnost da pouzdano, svesno i odgovorno rukuje tajnim podacima i informacijama.
122. **Provera medicinskih podataka** je ključan aspekt bezbednosne provere jer omogućava procenu da li kandidat ima mentalne, neurološke ili druge zdravstvene smetnje koje mogu uticati na njegovu sposobnost da pouzdano, svesno i odgovorno rukuje tajnim podacima i informacijama. Provera medicinskih podataka je neophodna radi zaštite nacionalne bezbednosti, tajnih podataka i stabilnosti lica koje rade sa tajnim podacima. Neophodno je osigurati da nijedna osoba sa teškim psihofizičkim poremećajima ne dobije pristup tajnim podacima jer bi to moglo dovesti do ozbiljnih bezbednosnih rizika.
123. **Profesionalna tajna** je podatak koji profesionalac u kontaktu sa klijentom sazna o ličnom ili porodičnom životu klijenta, a što ne sme biti dostupno drugim osobama. Profesionalna tajna u sebi sadrži lični podatak, odnosno lične podatke, koji su povezani sa pravilima struke.
124. **Procedura za označavanje i određivanje stepena tajnosti podataka** predstavlja ključni korak u zaštiti osetljivih informacija, dokumenata i podataka, kao i očuvanju interesa Republike Srbije. Ova procedura ima za cilj da obezbedi bezbednost podataka, uz transparentnost i odgovornost organa javne vlasti. Kao tajni podatak može se odrediti podatak od interesa za Republiku Srbiju čijim bi otkrivanjem neovlašćenom licu nastala šteta, ako je potreba zaštite interesa Republike Srbije pretežnija od interesa za slobodan pristup informacijama od javnog značaja.

- 125. Procena okolnosti nastanka bezbednosnog incidenta u radu sa tajnim podacima**, kao i njegova pravna kvalifikacija, jedan je od najvažnijih koraka u obradi i određivanju daljeg postupanja u skladu sa propisima. U zavisnosti od vrste incidenta, različito će se reagovati nadležni organi i primeniti odgovarajući pravni mehanizmi.
- 126. Procena pretnje za bezbednost tajnog podatka (samoprocena)** - po Zakonu o tajnosti podataka predstavlja bezbednosnu procenu koja se primenjuje u radu sa tajnim podacima. Procena pretnje za bezbednost tajnog podatka ili samoprocena nije samo identifikacija nepravilnosti, već i kontinuiran proces unapređenja. Kombinacija redovne procene, obuke, tehnoloških rešenja, unutrašnje kontrole i nadzora osigurava najviši nivo zaštite.
- 127. Procena rizika** je određivanje kvantitativnih i kvalitativnih vrednosti rizika koji se odnose na konkretnu situaciju i priznato pretnje (naziva opasnost).
- 128. Procena uticaja i rizika od incidenta u radu sa tajnim podacima važan** je korak u razumevanju stepena ugrožavanja koji je nastupio. To podrazumeva ne samo procenu nastanka materijalne štete, već i potencijalne posledice po nacionalnu bezbednost, prava lica ili organizaciju. Kada se procenjuje da li je incident mogao imati međunarodne implikacije, važno je uzeti u obzir stepen osetljivosti podataka, kao i mogućnost da se povreda izazove preko granica.
- 129. Rad sa pravnim licima** odnosni se na upravu i saradnju sa pravnim licima kod poverljivih nabavki, posebno u oblasti industrijske bezbednosti, koji uključuju bezbednost informacija i tehnologija u proizvodnim i servisnim procesima.
- 130. Radna tačka za rad sa tajnim podacima** predstavlja funkcionalni određeni deo radnog prostora unutar organa javne vlasti koji je posebno organizovan radi prijema, obrade, pristupa i čuvanja tajnih podataka u organu javne vlasti. Radna tačka ne predstavlja zvanično uspostavljenu administrativnu, odnosno bezbednosnu zonu, već služi kao privremeno rešenje za rad sa tajnim podacima u kontrolisanim i bezbednim uslovima, do uspostavljanja zona u skladu sa Uredbom o posebnim merama fizičkotehničke zaštite tajnih podataka.
- 131. Raspoloživost** je svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;
- 132. Revizija i ažuriranje** - Oznake tajnosti se periodično preispituju i revidiraju kako bi se utvrdilo da li je potrebno zadržati, promeniti ili ukinuti stepen tajnosti, zbog vremenskog ograničenja, prestanka tajnosti utvrđivanjem datuma, nastupanjem određenog događaja i istekom roka.
- 133. Registarski sistem** predstavlja uređen sistem koji mora da bude realizovan u skladu sa propisima i standardima iz oblasti ZTP.
- 134. Relativne smetnje** (procena pojedinačnog slučaja) - Ovo su stanja koja ne moraju automatski voditi diskvalifikaciji, ali mogu predstavljati

bezbednosni rizik u zavisnosti od težine, učestalosti simptoma i načina lečenja.

135. **Rešenje** predstavlja upravni akt nadležnog organa kojim je rešena upravna stvar koja je bila predmet upravnog postupka.
136. **Rizik informaciono-komunikacionog sistema** podrazumeva mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;
137. **Rukovalac tajnim podatkom** je fizičko lice ili organizaciona jedinica organa javne vlasti, koji preduzima mere zaštite tajnih podataka u skladu sa odredbama ovog zakona.
138. **Sabotaža** opisuje namerne radnje kojima se nanosi šteta fizičkoj ili virtualnoj infrastrukturi organizacije, uključujući nepoštovanje procedura održavanja ili IT, kontaminiranje čistih prostora, fizičko oštećenje objekata ili brisanje koda radi sprečavanja redovnih operacija.
139. **Sajber bezbednost** predstavlja primenu tehnologije, procesa i kontrole radi odbrane računara, servera, mobilnih uređaja, elektronskih sistema, mreža i podataka od sajber napada.
140. **Sajber pretnja** uključuje krađu, špijunažu, nasilje i sabotazu svega što je povezano sa tehnologijom, virtualnom stvarnošću, računarima, uređajima ili internetom.
141. **Sertifikat za pristup tajnim podacima** je dokument koji potvrđuje da lice ima pravo pristupa i korišćenja tajnih podataka u odgovarajućoj meri po principu „potreba da zna“.
142. **Sertifikovanje privrednih subjekata** omogućava njihovo učešće na raspisanim tenderima u državama sa kojima Republika Srbija ima zaključene i ratifikovane međunarodne sporazume o razmeni i uzajamnoj zaštiti tajnih podataka.
143. **Segmentacija**: Podela informacija prema potrebi da zna.
144. **Sistem monitoringa i revizije** je sistem za praćenje i reviziju koji osigurava da se sve mere zaštite primenjuju na adekvatan način.
145. **Sistem upravljanja bezbednošću informacija (SUIB / ISMS)**: Organizacioni okvir.
146. **Skrivanje podataka** – Lice namerno ili nenamerno ne prijavi sve relevantne informacije u svrhu vršenja bezbednosne provere (neprijavljivanje kontakata sa stranim državljanima, skrivanje radnog ili kriminalnog dosijea, skrivanje medicinskih podataka, lažiranje informacija o obrazovanju..).
147. **Služba bezbednosti** je služba bezbednosti u smislu zakona kojim se uređuju osnove bezbednosno-obaveštajnog sistema Republike Srbije.
148. **Strani tajni podatak** je podatak koji Republici Srbiji poveri strana država ili međunarodna organizacija uz obavezu da ga čuva kao tajni, kao i tajni podatak koji nastane u saradnji Republike Srbije sa drugim državama, međunarodnim organizacijama i drugim međunarodnim subjektima, u skladu sa zaključenim međunarodnim sporazumom koji je sa stranom

državom, međunarodnom organizacijom ili drugim međunarodnim subjektom zaključila Republika Srbija;

149. **Strani uticaj** – Česti kontakti ili porodične veze sa stranim državljanima koji se mogu smatrati bezbednosnim rizikom.
150. **Stručni nadzor u sistemu zaštite tajnih podataka** predstavlja proces stručne procene i verifikacije primene Zakona o tajnosti podataka kod organa javne vlasti, sa ciljem osiguranja usklađenosti propisa i efikasnosti mera zaštite. Ovaj proces omogućava identifikaciju potencijalnih rizika i slabosti, pružajući stručne preporuke za unapređenje sistema zaštite tajnih podataka.
151. **Sudski postupci** - Ako se utvrdi da je postupak označavanja ili obrade podataka bio nezakonit, mogu se pokrenuti civilni postupci, gde se može zahtevati odgovornost za štetu koju su organi javne vlasti ili njihovi zaposleni naneli.
152. **Security breaches/kršenje bezbednosti** predstavlja neovlašćeni pristup informacijama na mrežama, serverima ili uređajima, zaobilaženje sigurnosti na tim sistemima, što na kraju rezultira oticanjem ili kompromitacijom podataka.
153. **Tajni podatak** je podatak od interesa za Republiku Srbiju koji je zakonom, drugim propisom ili odlukom nadležnog organa donesenom u skladu sa zakonom, određen i označen određenim stepenom tajnosti.
154. **Tajni podatak označen stepenom tajnosti “DRŽAVNA TAJNA”** predstavlja podatak čijim bi otkrivanjem neovlašćenom licu, njegovom zloupotrebom ili uništavanjem nastala neotklonjiva teška šteta po interese Republike Srbije.
155. **Tajni podatak označen stepenom tajnosti “INTERNO”** predstavlja podatak čijim bi otkrivanjem neovlašćenom licu, njegovom zloupotrebom ili uništavanjem nastala šteta po rad, odnosno obavljanje zadataka i poslova organa javne vlasti.
156. **Tajni podatak označen stepenom tajnosti “POVERLJIVO”** predstavlja podatak čijim bi otkrivanjem neovlašćenom licu, njegovom zloupotrebom ili uništavanjem nastala šteta po interese Republike Srbije.
157. **Tajni podatak označen stepenom tajnosti “STROGO POVERLJIVO”** predstavlja podatak čijim bi otkrivanjem neovlašćenom licu, njegovom zloupotrebom ili uništavanjem nastala teška šteta po interese Republike Srbije.
158. **Tajnost** je svojstvo koje znači da podatak nije dostupan neovlašćenim licima.
159. **Tehnička zaštita** je obezbeđenje lica i imovine koje se vrši tehničkim sredstvima i uređajima, njihovim planiranjem, projektovanjem, ugradnjom i održavanjem.
160. **Tehničke mere zaštite** predstavljaju obezbeđenje i zaštitu podataka i informacija i drugih elemenata informaciono-komunikacionog sistema, koji se ostvaruju primenom posebnih tehničko-tehnoloških procesa rada i/ili

sprovođenjem fizičko-manipulativnih mera zaštite u bilo kojoj proceduri u okviru rada IKT sistema.

161. **Tehnički uslovi** odnose se naročito na fizičko-tehničku zaštitu prostora, odnosno prostorija u kojima se čuvaju tajni podaci, protivpožarnu zaštitu, zaštitu tajnih podataka prilikom prenošenja i dostavljanja izvan prostorija u kojoj se čuvaju, transport tajnih podataka, obezbeđivanje i zaštitu informaciono-telekomunikacionim sredstava kojima se vrši prenošenje i dostavljanje tajnih podataka i sprovođenje propisanih mera kriptozastite.
162. **Tehnološka akreditacija** - Fokusira se na tehničke aspekte kao što su zaštita od kompromitacije elektromagnetnim zračenjem (KEMZ) i primena specifičnih bezbednosnih mera, na osnovu propisa o odbrani, uključujući EU i NATO standarde.
163. **TEMPEST** je standardizovani skup tehnika i testova za sprečavanje kompromitacije. Dok KEMZ označava sve mere zaštite, TEMPEST je konkretno orijentisan ka sertifikaciji i testiranju uređaja (npr. NATO SDIP-27).
164. **Ugovor** je dokument koji podrazumeva posebne mere zaštite tajnih podataka koje se primenjuju na sve organizacione i tehničke uslove za čuvanje tajnih podataka u postupku zaključenja ugovora između organa javne vlasti i pravnog ili fizičkog lica na osnovu kojeg se tajni podaci dostavljaju ovim licima.
165. **Unutrašnja kontrola** je proces ustanovljen i sproveden od strane rukovodioca organa javne vlasti, organizacione jedinice ili ovlašćenog pojedinca.
166. **Upravni postupak** je postupak donošenja upravnih akata. Pod upravnim postupkom podrazumevaju se proceduralna pravna pravila koja se primenjuju u vezi sa donošenjem odluka u upravnim stvarima.
167. **Usaglašenost sa standardima bezbednosti** predstavlja obavezu organa da se usaglasa sa nacionalnim i međunarodnim standardima u oblasti informacione bezbednosti, posebno u oblasti bezbednosti IT sistema koji obrađuju tajne podatke.
168. **Upravljanje incidentima bezbednosti** – organizovani skup aktivnosti za otkrivanje, analizu, ograničavanje i oporavak od bezbednosnih incidenata.
169. **Fizička bezbednost/sigurnost** predstavlja primenu mera fizičke i tehničke zaštite na pojedinačnim lokacijama, zgradama ili otvorenim prostorima na kojima se nalaze ili čuvaju štićeni podaci (informacije) koje zahtevaju zaštitu od gubljenja, neovlašćenog pristupa, kompromitovanja ili otuđenja.
170. **Fizička zaštita** je usluga obezbeđenja koja se pruža prvenstveno ličnim prisustvom i neposrednom aktivnošću službenika obezbeđenja u određenom prostoru i vremenu u skladu sa planom obezbeđenja, primenom mera i ovlašćenja službenika obezbeđenja;
171. **Fizičko-tehnička zaštita** je obezbeđenje lica i imovine primenom fizičke zaštite i korišćenjem sredstava tehničke zaštite.
172. **Finansijska nestabilnost** – Veliki dugovi, loša finansijska situacija ili neregularno poslovanje, pokretanje likvidacije odnosno stečaja pravnih lica.

- 173. Horizontalna i vertikalna koordinacija** - Planiranje i primena mera zaštite tajnih podataka podrazumeva saradnju između različitih nivoa rukovođenja i sektora unutar organa javne vlasti. Horizontalna koordinacija obuhvata razmenu informacija i uniformnu primenu mera bezbednosti među različitim sektorima, dok vertikalna koordinacija osigurava jasnu podršku i nadzor rukovođenja.
- 174. Šifra** je preslikavanje (transformacija, pravilo) kojim se tajna poruka preslikava u nerazumljiv niz znakova (slova, brojeve...)
- 175. Špijun** - (uhoda, doušnik, dostavljač, potkazivač, vrebač, žbir...)
- 176. Špijunaža** je prikrivena ili nedozvoljena praksa špijuniranja za potrebe strane vlade, organizacije, entiteta ili osobe radi dobijanja poverljivih informacija radi vojne, političke, strateške ili finansijske koristi.
- 177. Šteta** je narušavanje interesa Republike Srbije nastalo kao posledica neovlašćenog pristupa, otkrivanja, uništavanja i zloupotrebe tajnih podataka ili kao posledica druge radnje obrade tajnih podataka i stranih tajnih podataka.
- 178. Štićeni prostor** je objekat ili prostor na kojem se vrše usluge obezbeđenja.

OBRASCI, MODELI ODLUKA I ZAHTEVA ZA IMPLEMENTACIJU ZAKONA O TAJNOSTI PODATAKA

Modeli odluka koje su neophodne za implementaciju Zakona o tajnosti podataka u organu javne vlasti

1. Odluka o određivanju tajnih podataka u organu javne vlasti
2. Odluka o određivanju rukovaoca tajnim podacima
3. Odluka o određivanju unutrašnje kontrole u organu javne vlasti
4. Lista „Potrebno da zna“
5. Lista „Potrebno podeliti sa“
6. Plan zaštite podataka za vandredne i hitne slučajeve
7. Uputstvo za rad sa tajnim podacima

Obrasci i uputstvo za popunjavanje bezbednosnog upitnika

1. Obrazac bezbednosnog upitnika za fizička lica
2. Obrazac bezbednosnog upitnika za pravna lica
3. Uputstvo za popunjavanje bezbednosnog upitnika
4. Izjava

Modeli zahteva za implementaciju Zakona o tajnosti podataka u organu javne vlasti

1. Model zahteva za izdavanje sertifikata za organe javne vlasti
1. Zahtev za davanje mišljenja Ministarstva pravde (status organa javne vlasti)
2. Model zahteva za izdavanje sertifikata za pravna lica
3. Model zahteva za organizaciju sastanka na temu implementacije Zakona o tajnosti podataka

Modeli odluka

1. Model odluke o ovlašćenom licu za određivanje tajnosti podataka
2. Model odluke o određivanju Administrativne zone
3. Model odluke o određivanju Bezbednosne zone
4. Model odluke o promeni stepena tajnosti

5. Model odluke o opozivu tajnosti – periodična procena
 6. Model odluke o prestanku tajnosti istekom roka
 7. Model izveštaja prilikom dostavljanja izveštaja o radu sa tajnim podacima
 8. Model Akta o informacionoj bezbednosti
 9. Evidencije za rad sa tajnim podacima **Modeli obrazaca**
1. Obrazac bezbednosne napomene prilikom dostavljanja tajnog podatka drugoj državi ili međunarodnoj organizaciji
 2. Obrazac o kopiji dokumenta
 3. Obrazac o označavanju dokumenata koji sadrži tajne podatke stepena tajnosti DT, SP, P i I
 4. Obrazac potvrde o prijemu tajnog podatka

Detaljnije pogledati na sajtu

<https://nsa.gov.rs/tekst/577/obraci.php>

KATALOG PROPISA ZA RAD SA TAJNIM PODACIMA

- Zakon o tajnosti podataka
- UREDBA o bližim kriterijumima za određivanje stepena tajnosti „DRŽAVNA TAJNA” i „STROGO POVERLjIVO” - "Službeni glasnik RS", broj 46 od 24. maja 2013.
- UREDBA o bližim kriterijumima za određivanje stepena tajnosti „POVERLjIVO” i „INTERNO” u organima javne vlasti - "Službeni glasnik RS", broj 79 od 29. jula 2014.
- UREDBA o bližim kriterijumima za određivanje stepena tajnosti „POVERLjIVO” i „INTERNO” u Ministarstvu odbrane - "Službeni glasnik RS", broj 66 od 29. juna 2014.
- UREDBA o bližim kriterijumima za određivanje stepena tajnosti „POVERLjIVO” i „INTERNO” u Ministarstvu unutrašnjih poslova "Službeni glasnik RS", broj 105 od 29. novembra 2013.
- UREDBA o bližim kriterijumima za određivanje stepena tajnosti „POVERLjIVO” i „INTERNO” u Bezbednosno-informativnoj agenciji "Službeni glasnik RS", broj 70 od 7. avgusta 2013.

- UREDBA o bližim kriterijumima za određivanje stepena tajnosti „POVERLjIVO” i „INTERNO” u Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka "Službeni glasnik RS", broj 86 od 30. septembra 2013.
- UREDBA o posebnim merama zaštite tajnih podataka koje se odnose na utvrđivanje ispunjenosti organizacionih i tehničkih uslova po osnovu ugovornog odnosa "Službeni glasnik RS", broj 63 od 19. jula 2013.
- UREDBA o posebnim merama fizičko-tehničke zaštite tajnih podataka "Službeni glasnik RS", broj 97 od 21. decembra 2011.
- UREDBA o posebnim merama nadzora nad postupanjem sa tajnim podacima „Službeni glasnik RS“, broj 90 od 30. novembra 2011.
- UREDBA o posebnim merama zaštite tajnih podataka u informacionotelekomunikacionim sistemima "Službeni glasnik RS", broj 53 od 20. jula 2011.
- UREDBA o načinu i postupku označavanja tajnosti podataka, odnosno dokumenata "Službeni glasnik RS", broj 8 od 11. februara 2011.
- UREDBA o sadržini, obliku i načinu vođenja evidencija za pristup tajnim podacima "Službeni glasnik RS", broj 89 od 29. novembra 2010.
- UREDBA o sadržini, obliku i načinu dostavljanja sertifikata za pristup tajnim podacima „Službeni glasnik RS“, broj 54 od 4. avgusta 2010.
- UREDBA o uvećanju plate državnih službenika i nameštenika koji obavljaju poslove u vezi sa zaštitom tajnih podataka u Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka i Ministarstvu pravde "Službeni glasnik RS", broj 79 od 29. oktobra 2010.
- UREDBA o obrascima bezbednosnih upitnika "Službeni glasnik RS", broj 30 od 07. maja 2010.
- -PRAVILNIK o službenoj legitimaciji i načinu rada lica ovlašćenih za vršenje nadzora "Službeni glasnik RS", br. 85 od 27. septembra 2013, 71 od 11. jula 2014.

OSTALI PROPISI

- Strategija nacionalne bezbednosti
- Strategija odbrane
- Zakon o osnovama uređenja službi bezbednosti
- Zakon o odbrani i Zakon o Vojsci
- Zakon o policiji
- Zakon o spoljnim poslovima

- Zakon o Bezbednosno-informativnoj agenciji
- Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji
- Zakonik o krivičnom postupku i Krivični zakonik
- Zakon o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije
- Zakon o državnim službenicima
- Zakon o informacionoj bezbednosti
- Zakon o javnim nabavkama i Uredba o javnim nabavkama u oblasti odbrane i bezbednosti "Službeni glasnik RS", broj 93 od 1. jula 2020.
- Zakon o elektronskim komunikacijama
- Zakon o poreskom postupku i poreskoj administraciji
- Zakon o zaštiti uzbunjivača
- Zakon o privatnom obezbeđenju

KANCELARIJA SAVETA ZA NACIONALNU BEZBEDNOST

I ZAŠTITU TAJNIH PODATAKA

Adresa elektronske pošte za zakazivanje online konsultacija:

online.konsultacije@nsa.gov.rs

Adresa elektronske pošte za zakazivanje aktuelnih obuka: obuke@nsa.gov.rs

Adresa elektronske pošte za zakazivanje brifinga:

termini.sertifikati@nsa.gov.rs

Web:

www.nsa.gov.rs

O AUTORU



Prof. dr Goran Matić

Direktor Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka Republike Srbije, vanredni profesor za oblast bezbednost Univerziteta UNION – „NIKOLA TESLA” i stalni sudski veštak za bezbednost informacija.

Učestvovao je u procesu izrade predloga više zakona, Strategije za suprotstavljanje i borbu protiv terorizma, Strategije nacionalne bezbednosti i Strategije odbrane i u radu Radnih grupa Vlade Republike Srbije za implementaciju akcionih planova za poglavlja 10, 24 i 31 za pristupanje Republike Srbije EU.

Od 2015. do 2019. godine rukovodio je Stalnom mešovitom radnom grupom za borbu protiv terorizma (SMRG) – formirane odlukom Biroa za koordinaciju rada službi bezbednosti, od 2019/2021. godine obavljao i dužnost zamenika nacionalnog koordinatora Nacionalnog koordinacionog tela (NKT) za sprečavanje i borbu protiv terorizma Republike Srbije.

U okviru međunarodne saradnje Republike Srbije na planu zaštite tajnosti podataka učestvovao je kao šef delegacije u pregovorima za potpisivanje 14 međunarodnih sporazuma i bio potpisnik više sporazuma koje je R. Srbija potpisala sa međunarodnim telima i stranim državama u oblasti zaštite tajnih podataka. Takođe, sa Misijom OEBS-a u Beogradu učestvovao je u više projekata oko zaštite tajnih podataka, sajber bezbednosti i obrade i zaštite ličnih podataka u sektoru bezbednosti i odbrane.

Od 2012. godine učestvuje u radu Forumu direktora nacionalnih bezbednosnih organa za zaštitu tajnih podataka zemalja Jugoistočne Evrope (SEENSA), kao i u okviru Inicijative „6S” koja okuplja direktore nacionalnih bezbednosnih organa zemalja regiona.

Autor je više objavljenih naučnih i stručnih radova i učesnik više naučnih konferencija, kao i naučne monografije „Politički delikti – atentat i pobuna” i koautor knjige „Taktika i metodika delovanja obaveštajno-bezbednosnih službi” u izdanju Medija centra Odbrana u Beogradu, i „Osnovi bezbednosti” u izdanju Fakulteta za poslovne studije i pravo u Beograd

Predavač je na osnovnim akademskim studijama Vojne akademije Univerziteta odbrane i na Fakultetu za poslovne studije i pravo Univerziteta Nikola Tesla Union u Beogradu.

Gostujući je predavač na Fakultetu bezbednosti i Fakultetu organizacionih nauka Univerziteta u Beogradu, kao i na Kriminalističko-policijskom univerzitetu, Akademiji za nacionalnu bezbednost i na Visokim studijama bezbednosti i odbrane

pri Univerzitetu odbrane u Beogradu. Pored toga predavač je na kratkim strukovnim studijama na Fakultetu bezbednosti: "Zaštita tajnih podataka i poslovne tajne" i "Zaštita ličnih podataka" od 2022. godine. Bio je gostujući predavač na master studijama Univerziteta u Beogradu – Terorizam, organizovani kriminal i bezbednost do 2024. godine

Akreditovani je predavač Nacionalne akademije za javnu upravu. Učestvuje je u radu posebnih stručnih tela te institucije, i to kao član Stalne programske komisije za elektronsku upravu i digitalizaciju (2022-2023) i Stalne programske komisije za javnu upravu (2023-2024).

Član je Ispitne komisije za državni ispit (visoko obrazovanje) državnih službenika i za komunalne milicionere u okviru ministarstva državne uprave i lokalne samouprave.

Predsednik je Saveta „SAMKB – Srpske asocijacije menadžera korporativne bezbednosti” u Beogradu; član udruženja „IT veštak” u Beogradu i „Udruženja za međunarodno krivično pravo” u Beogradu. U Privrednoj komori Srbije i Privrednoj komori Beograda više godina izvodi edukacije na temu korporativne bezbednosti i obrade i zaštite podataka.