



ОЗНАЧАВАЊЕ ТАЈНИХ ПОДАТАКА

Процедура за означавање и одређивање степена тајности података представља кључни корак у заштити осетљивих информација, докумената и података, као и очувању интереса Републике Србије. Ова процедура има за циљ да обезбеди безбедност података, уз транспарентност и одговорност органа јавне власти. Као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја. Поступак означавања и одређивања степена тајности у органима јавне власти у Републици Србији регулисан је Законом о тајности података и подзаконским актима, и обухвата следеће кораке:

1. Доношење формалне одлуке о тајности:

Орган јавне власти је у обавези да донесе генеричну или појединачну писмену одлуку о одређивању степена тајности података, уз процену утицаја и потенцијалне штете по интересе Републике Србије у случају откривања, злоупотребе или уништења података. Тајност податка, под условима и на начин утврђен законом о тајности података, одређује овлашћено лице. При одређивању степена тајности податка, овлашћено лице одређује најнижи степен тајности који спречава настанак штете по интересе Републике Србије. Овлашћена лица која имају право да одређују степен тајности података према члану 9. Закона о тајности података су: председник Републике, председник Владе, руководиоца органа јавне власти, изабрани, постављени или именовани функционер органа јавне власти који је за одређивање тајних података овлашћен законом, односно прописом донесеним на основу закона, или га је за то писмено овластио руководиоца органа јавне власти, као и лице запослено у органу јавне власти које је за то писмено овластио руководиоца тог органа.

2. Идентификација категорија података:

Подаци се анализирају како би се утврдило да ли испуњавају услове за означавање као тајни, укључујући прописима предвиђене категорије података, као и процену могућег утицаја на националну безбедност, јавни интерес, територијални интегритет и економске интересе. У овом кораку се такође разматра и општи значај података, као и последице које би њихово откривање могло имати на рад органа јавне власти.



ОЗНАЧАВАЊЕ ТАЈНИХ ПОДАТАКА

3. Одређивање степена тајности:

На основу процене, подаци се разврставају или категоришу у један од следећих степена тајности узимајући у обзир озбиљност потенцијалне штете по нарушавање интереса Републике Србије настало као последицу неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последицу друге радње обраде тајних података у складу са уредбама о ближим критеријумима за одређивање степена тајности „државна тајна“, „строго поверљиво“, „поверљиво“ и „интерно“ („Службени гласник Републике Србије“ број 46/2013, 70/2013, 86/2013, 105/2013, 66/2014 и 79/2014):

- **државна тајна** - који се одређује ради спречавања настанка неотклоњиве тешке штете по интересе Републике Србије;
- **строго поверљиво** - који се одређује ради спречавања настанка тешке штете по интересе Републике Србије;
- **поверљиво** - који се одређује ради спречавања настанка штете по интересе Републике Србије; или
- **интерно** - који се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио.

4. Означавање података:

Подаци добијају јасну ознаку која укључује степен тајности, начин престанка тајности, податке о овлашћеном лицу, датум означавања, назив органа који је донео одлуку и правну основу. Ознака мора бити видљива и у складу са прописаним стандардима у Уредби о начину и поступку означавања тајности података, односно документа („Службени гласник Републике Србије“ број 8/2001). Документ који садржи тајни податак означава се одговарајућим степеном тајности, изнад назива документа, на врху сваке странице, на средини. Ознака одговарајућег степена тајности на документу исписује се тамнијим словима већег формата од слова текста документа. Ако документ садржи више страница, свака страница се означава редним бројем странице у односу на укупан број страница. Сваки документ мора имати ознаку степена тајности на врху прве стране и спољне стране предњих корица ако оне постоје или на врху насловне стране. Ако документ нема насловну страну, прва страна ће се сматрати као насловна. Приликом означавања документа не сме доћи до уништења или оштећења тајног податка, односно документа на којем се он налази.



ОЗНАЧАВАЊЕ ТАЈНИХ ПОДАТАКА

5. Евиденција и контрола:

Тајни подаци се уписују у регистар и евиденцију тајних података ради праћења и контроле. Евиденција о тајним подацима води се одвојено од осталих евиденција органа јавне власти. Евиденција садржи: редни број, назив органа јавне власти, назив унутрашње организационе јединице органа јавне власти која је одредила степен тајности, садржај предмета, датум пријема предмета, класификациона ознака предмета, податке о уступању документа другом органу, податке о промени степена тајности, начин и датум престанка тајности, податак када је предмет архивиран и напомену. Орган јавне власти је у обавези да обезбеди адекватну административну, физичку и информациону безбедност.

6. Ревизија и ажурирање:

Ознаке тајности се периодично преиспитују и ревидирају како би се утврдило да ли је потребно задржати, променити или укинути степен тајности, због временског ограничења, престанка тајности утврђивањем датума, наступањем одређеног догађаја и истеком рока. Одлука о опозиву тајности податка доноси се ако наступе чињенице и околности услед којих податак престаје да буде од интереса за Републику Србију.

7. Последице непоштовања процедура:

Непоштовање прописаних процедура означавања и заштите тајних података може довести до озбиљних последица. Ове последице не обухватају само административне и организационе последице, већ могу бити и озбиљне правне и кривичне природе. У зависности од врсте прекршаја и тежине поступка, могу се применити различите казнене мере, укључујући санкције против органа јавне власти и одговорних лица, као и опасност по безбедност Републике Србије.

Казнене мере: У складу са Законом о тајности података, непоштовање процедура означавања, чувања и обраде тајних података може довести до различитих казnenих мера:

Прекршајне санкције се могу изрећи у случају када одговорна лица не испуне обавезе у погледу означавања, чувања или размене тајних података, или ако дође до њиховог неовлашћеног откривања. Прекршаји могу обухватити:

- Неадекватно означавање степена тајности.
- Недовољну заштиту тајних података.
- Неоправдано откривање података без одобрења или одлуке овлашћеног лица.



ОЗНАЧАВАЊЕ ТАЈНИХ ПОДАТАКА

Кривичне санкције су озбиљније и применљиве су у случају кршења процедура које могу довести до значајне штете по безбедност Републике Србије. Члан 98. Закона о тајности података прописује кривично дело које укључује:

- **Неовлашћено откривање тајних података:** Лице које без овлашћења открије тајне податке или их користи у незаконите сврхе, може бити кривично гонјено.
- **Злоупотреба тајних података:** Лице које злоупотреби тајне податке, било да их дели, продаје или на неки други начин користи против националне безбедности, може бити осуђено на казне затвора.
- **Недопуштена измена или уништавање тајних података:** Лица која униште, измене или на неки начин ометају очување тајних података, као и лица која не предузму прописане мере заштите података, могу бити кривично санкционисана.

У складу са чланом 98. Закона, **кажњавање се може изрећи казном затвора до 5 година**, зависно од природе дела. Утврђивање казне зависи од тога да ли је дошло до озбиљне штете по безбедност Републике Србије, односно да ли је дело довело до нарушавања националне безбедности.

Угрожавање безбедности - Непоштовање процедура означавања и заштите тајних података може директно угрозити националну безбедност, што може довести до:

- **Штете по безбедност Републике Србије:** Откривање, злоупотреба или уништавање тајних података може нанети озбиљну штету одбрани, дипломатским и политичким односима или економским интересима земље.
- **Откривање података од војног или обавештајног значаја:** Ако дође до откривања података који се односе на војне операције, обавештајну активност или стратегије одбране, то може довести до директне претње по сигурност земље и њених грађана.
- **Злоупотреба информација:** Неовлашћени приступ тајним подацима може довести до извоза осетљивих информација и коришћења од стране странака које имају непријатељске намере према Србији.

Губитак поверења - Недостатак адекватне заштите тајних података може довести до значајног губитка поверења у органе јавне власти. Када грађани, правни субјекти или међународни партнери сазнају да се подаци који су од великог значаја за националну безбедност не чувају на адекватан начин, то може:



ОЗНАЧАВАЊЕ ТАЈНИХ ПОДАТАКА

- **Нарушити углед органа јавне власти:** Откривање пропуста у заштити тајних података може довести до негативних реакција јавности и партнерских земаља, што нарушава кредибилитет власти.
- **Нарушити однос са међународним партнерима:** Недовољна заштита података може довести до кршења међународних споразума, што отежава сарадњу са иностранством.
- **Погоршање унутрашњег поверења:** Институтима и грађанима може бити изгубљено поверење у способност органа јавне власти да адекватно управљају тајним подацима и да гарантују националну безбедност.

Правне импликације - Када дође до кршења процедура означавања и заштите тајних података, могу се покренути и правни поступци против одговорних лица:

- **Судски поступци:** Ако се утврди да је поступак означавања или обраде података био незаконит, могу се покренути цивилни поступци, где се може захтевати одговорност за штету коју су органи јавне власти или њихови запослени нанели.
- **Прекршајни поступци:** Уколико је дошло до прекршаја у смислу неправилног чувања или поступања са тајним подацима, могу се изрећи новчане казне или друге мере као што су упозорење или јавна опомена.
- **Поступци због повреда радне дисциплине:** Одговорна лица која су прекршила процедуре могу бити предмет дисциплинских мера, као што су опомена, суспензија или отказ.

Поштовање процедура означавања и заштите тајних података није само законска обавеза, већ и морална и професионална одговорност свих запослених у органима јавне власти. Адекватна примена ових мера је основа за јачање поверења грађана, очување националне безбедности и интегритета државних институција, као и за заштиту од опасности које могу угрозити интересе Републике Србије. **Свако кршење ових процедура представља значајан ризик који може довести до озбиљних последица, укључујући угрожавање сигурности земље, економског интегритета и међународних односа.** Доследност у примени мера заштите тајних података осигурава стабилност, повећава међународни кредибилитет и јача безбедност државних институција, чиме се ствара чврст основ за адекватно реаговање на претње националној безбедности.

**КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА**

e-mail: office@nsa.gov.rs, kontakt@nsa.gov.rs

web: www.nsa.gov.rs