



# СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

**СКРИПТА**

Проф.др Горан Д. Матић

Приручник представља лично, научно и стручно виђење аутора изнете проблематике....

Рађен је на основу јавних извора.

Сврха овог приручника је да допринесе бољем разумевању различитих тема које заједно чине оквир за успостављање система заштите тајних података и унутрашње контроле у органима јавне власти.

**Не спровођење Закона о тајности података представља кршење и угрожавање националне безбедности Републике Србије...**

**Али и кривично дело, прекршај и повреду радне дисциплине**

**НЕ ПОЗНАВАЊЕ ПРОПИСА ШКОДИ!**

## ПРИЗМА ПОСМАТРАЊА

- РЕФОРМА ДРЖАВНЕ УПРАВЕ
- РЕФОРМА СЕКТОРА БЕЗБЕДНОСТИ
- У СУСРЕТ ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА...
- ПРЕГОВАРАЧКА ПОГЛАВЉА СА ЕУ - КЛАСТЕРИ (10, 23, 24 и 31)

## АСПЕКТИ РАЗМАТРАЊА ПРОБЛЕМА:

- ТЕХНОЛОШКИ
- ПРАВНИ
- БЕЗБЕДНОСНЕ ПОЛИТИКЕ И СТРАТЕГИЈЕ

## САДРЖАЈ

УВОДНА РАЗМАТРАЊА.....	1
СИСТЕМ РАДА И ЗАШТИТЕ ПОДАТАКА У Р. СРБИЈИ.....	1
РАД СА ТАЈНИМ ПОДАЦИМА.....	2
ЗАКОН О ТАЈНОСТИ ПОДАТАКА.....	2
РАД СА ТАЈНИМ ПОДАЦИМА.....	2
НЕОПХОДНИ КОРАЦИ.....	3
ОРГАНИЗАЦИЈА РАДА СА ТАЈНИМ ПОДАЦИМА.....	4
РЕГИСТАРСКИ СИСТЕМ.....	5
МЕЂУНАРОДНА САРАДЊА.....	5
ПЕРСОНАЛНА БЕЗБЕДНОСТ.....	7
БЕЗБЕДНОСНЕ ПРОВЕРЕ.....	9
ВРСТЕ БЕЗБЕДНОСНИХ ПРОВЕРА.....	9
СВРХА БЕЗБЕДНОСНЕ ПРОВЕРЕ.....	10
БЕЗБЕДНОСНЕ ПРОВЕРЕ.....	10
БЕЗБЕДНОСНИ СЕРТИФИКАТИ.....	10
ПРАВО ПРИСТУПА ТАЈНИМ ПОДАЦИМА.....	10
УПОЗНАВАЊЕ СА БЕЗБЕДНОСНИМ ПРОЦЕДУРАМА -БРИФИНГ-.....	11
ЛИСТА „ПОТРЕБНО ДА ЗНА“.....	12
УСЛОВИ ЗА ПРИСТУП ТАЈНОМ ПОДАТКУ.....	12
СЕРТИФИКАТИ.....	13
ПРЕСТАНАК ВАЖЕЊА СЕРТИФИКАТА.....	13
КРИВИЧНО ДЕЛО.....	13
БЕЗБЕДНОСНИ СЕРТИФИКАТ - за физичка лица –.....	14
АДМИНИСТРАТИВНА БЕЗБЕДНОСТ.....	15
ПОДАТАК ОД ИНТЕРЕСА ЗА РЕПУБЛИКУ СРБИЈУ ИЛИ ТАЈНИ ПОДАТАК.....	17
КРИТЕРИЈУМИ ЗА ОДРЕЂИВАЊЕ ТАЈНИХ ПОДАТАКА „ДРЖАВНА ТАЈНА“.....	18
КРИТЕРИЈУМИ ЗА ОДРЕЂИВАЊЕ ТАЈНИХ ПОДАТАКА НА ОСНОВУ ПРОПИСА О ОДБРАНИ...19	
КРИТЕРИЈУМИ И ШТЕТА КОД ТАЈНИХ ПОДАТАКА.....	20
ПРОЦЕНА ШТЕТЕ.....	20
ТАЈНОСТ ПОДАТАКА ЈЕ УВЕК УСЛОВЉЕНА.....	20
ОПОЗИВ ТАЈНОСТИ.....	20
ПРОБЛЕМ У ПРАКСИ - ТАЈНИ ПОДАТАК (ОРГАН ЈАВНЕ ВЛАСТИ).....	21
Податак који се може одредити као тајни податак.....	21
Одређивање степена тајности.....	21
Овлашћено лице за одређивање тајности податка.....	22
Тајним податком се не сматра.....	22
Документ који садржи тајне податке означава се:.....	22
Када се одређује тајност податка.....	23
Одлука о одређивању степена тајности.....	23
Поступак означавање докумената.....	24
Остваривање увида у тајни податак.....	25
Руковање са документом.....	26
Законски рок престанка тајности података.....	27
Престанак тајности података.....	27
Припрема за слање тајног података.....	28
Достављање тајног података.....	29
Обрађивање тајног податка ван безбедносне зоне.....	30
Архивирање и уништавање тајних података.....	30
ИНФОРМАЦИОНА ГАРАНЦИЈА.....	31
ПОСТОЈЕЋЕ СТАЊЕ.....	32
Прописи на снази:.....	32
ИНФОРМАЦИОНА БЕЗБЕДНОСТ.....	32

ШТА ЧИНИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ:.....	32
САЈБЕР БЕЗБЕДНОСТ .....	33
ЕЛЕКТРОНСКА УПРАВА.....	33
ИНФОРМАЦИОНА БЕЗБЕДНОСТ У СРБИЈИ.....	34
ИНФОРМАЦИОНА БЕЗБЕДНОСТ .....	34
ОПШТЕ БЕЗБЕДНОСНЕ ПОЛИТИКЕ И ПОСТУПЦИ .....	35
УРЕДБА О БЛИЖЕМ УРЕЂЕЊУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА .....	35
УРЕДБА О БЛИЖЕМ САДРЖАЈУ АКТА О БЕЗБЕДНОСТИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА, НАЧИНУ ПРОВЕРЕ И САДРЖАЈУ ИЗВЕШТАЈА ПРОВЕРЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА .....	35
СРПСКИ СТАНДАРД.....	37
SRPS ISO 27001 .....	37
СТАНДАРДИ ISO/IAS 17799 .....	38
ФИЗИЧКА БЕЗБЕДНОСТ.....	39
ПРОПИСИ.....	40
ФИЗИЧКА БЕЗБЕДНОСТ .....	40
РЕЛЕВАНТНИ ФАКТОРИ .....	41
Опште мере заштите.....	42
Посебне мере физичко-техничке заштите.....	42
Опрема за обраду ТП .....	43
Простори са рестриктивним приступом:.....	43
Противприслушни преглед.....	44
Уништавање тајних података .....	44
ИНДУСТРИЈСКА БЕЗБЕДНОСТ .....	45
ИНДУСТРИЈСКА БЕЗБЕДНОСТ - ПРАВНИ ОКВИР.....	46
ИНДУСТРИЈСКА БЕЗБЕДНОСТ - КОРЕЛАЦИЈА СА ЈАВНИМ НАБАВКАМА? .....	46
ПОСЕБНИ ИЗУЗЕЦИ У ОБЛАСТИ БЕЗБЕДНОСТИ И ОДБРАНЕ.....	47
УРЕДБА О ЈАВНИМ НАБАВКАМА У ОБЛАСТИ БЕЗБЕДНОСТИ И ОДБРАНЕ (СЛ.Г.РС 93/2020) ...	48
УРЕДБА О ПОСЕБНИМ МЕРАМА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА КОЈЕ СЕ ОДНОСЕ НА УТВРЂИВАЊЕ ИСПУЊЕНОСТИ ОРГАНИЗАЦИОНИХ И ТЕХНИЧКИХ УСЛОВА ПО ОСНОВУ УГОВОРНОГ ОДНОСА (СЛ.Г.РС 63/2013).....	49
УСЛОВИ ЗА ПОДНОШЕЊЕ ЗАХТЕВА ЗА ИЗДАВАЊЕ СЕРТИФИКАТА .....	50
ОСНОВ ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА.....	50
ПОСТУПАК ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА .....	51
ПОСТУПАК ИЗДАВАЊА СЕРТИФИКАТА.....	51
БЕЗБЕДНОСНЕ ПРОВЕРЕ врше се по основу: .....	51
КОНТРОЛА И НАДЗОР.....	52
ПРОПИСИ.....	53
ПОЈАМ БЕЗБЕДНОСНЕ КУЛТУРЕ И СВЕСТИ.....	53
ШТА ЈЕ ТО БЕЗБЕДНОСНА КУЛТУРА И СВЕСТ? .....	53
УЛОГА КАНЦЕЛАРИЈЕ САВЕТА .....	53
ПРАВНИ ОКВИР УНУТРАШЊЕ КОНТРОЛЕ: .....	53
ЗАКОН О ТАЈНОСТИ ПОДАТАКА .....	53
ОБАВЕЗА ИЗ ПРОПИСА О ЗАШТИТИ ТАЈНИХ ПОДАТАКА:.....	54
ПИТАЊА ПО КОЈИМА СЕ ВРШИ УНУТРАШЊА КОНТРОЛА: .....	54
Системска неправилност .....	56
Једнократна неправилност.....	56
Грешке .....	57
ПРЕВЕНТИВНЕ И „AD NOS“ МЕРЕ ЗАШТИТЕ ТП.....	57
ОБУКЕ.....	58
Уместо закључка .....	58

# **СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА**

## УВОДНА РАЗМАТРАЊА

У сваком друштву постоје одређени подаци и информације, које су не доступне јавности и као такве изузете из обавезе увида и давања грађа нима, а као такве су проглашене тајним, због чега је током дуге историје човечанства, тајни податак представљао једно од основних средстава моћи у рукама власти. Када говоримо о корацима уређења области тајних података у Републици Србији, морамо имати у виду да је то била област националне безбедности, којој је у последњих 20 година било посвећено најмање пажње у законодавној делатности. Питање приме не Закона о тајности података своди се на базична питања функцио нисања демократске и правне државе, цивилне контроле над сектором безбедности и успостављања сарадње и поверења на свим нивоима, уз неизбежан ефекат подизања општег стања безбедности у Републици Србији.

Систем националне безбедности и заштита тајних података представљају два концепта који се узајамно преплићу.

Систем националне безбедности представља материјални (суштински) део.

Заштита тајних података представља формални (процедурални) део система националне безбедности, али и регионалне....

Систем заштите тајних података осмишљен је првенствено са циљем да се обезбеди усаглашеност за законским и институционалним захтевима, да се реализује концепт „заштите националне безбедности“ и успостави међународна сарадња, као и високи стандарди квалитета корпоративног управљања и адекватног понашања, те да се осигура стварна одговорност и добри системи заштите тајних података.

**Обавезе које произлазе из Закона о тајности података** – Закон о тајности података унео је у правни систем Републике Србије један нов системски приступ утемељен на безбедносним, правним и техничким стандардима који се примењују у Европској унији, НАТО, али и земља ма у окружењу које су га имплементирале у своје правне системе. Сам Закон о тајности података је наметнуо одређене обавезе органима јав не власти које се огледају у следећем: 1) израда подзаконске регулативе о одређивању критеријума за степен тајности Интерно и Поверљиво; 2) израда подзаконске регулативе која се односи на поједине посебне мере заштите; 3) усаглашавање прописа са Законом о тајности подата ка који се односе на рад са тајним подацима (канцеларијско послова ње и слично); 4) измене међународних споразума који подразумевају размену тајних података и формирање посебних регистара за те наме не; 5) измене аката о унутрашњој организацији и систематизацији или формацији, увођењем степена тајности коме лице има приступ у обављању својих послова; 6) израда аката о преносу тајних података, при мени општих и посебних мера и слично; 7) одређивање руковаоца тајних података у органу јавне власти и формирање регистарског система за рад са тајним подацима Републике Србије; 8) организовање система перманентне едукације из области заштите тајних података; 9) вођење службених евиденција у складу са Законом о тајности података; 10) успостављање непосредне сарадње и комуникације са Канцеларијом Савета за националну безбедност и заштиту тајних података; 11) унутрашње регулативе о информатичкој сигурности/безбедности

## СИСТЕМ РАДА И ЗАШТИТЕ ПОДАТАКА У Р. СРБИЈИ

Законска регулатива која се бави ЗАШТИТОМ ПОДАТАКА:

- Закона о слободном приступу информацијама од јавног значаја
- Закона о заштити података о личности
- Закона о тајности података
- Закон о информационој безбедности

- Закон о заштити пословне тајне/Закон о привредним друштвима
- одређеног броја уредби
- АУТОНОМНО ИЛИ УНУТРАШЊЕ ПРАВО?

## РАД СА ТАЈНИМ ПОДАЦИМА

- Стратегија националне безбедности
- Стратегија одбране
- Закон о основама уређења служби безбедности
- Закон о одбрани и Закон о Војсци
- Закон о полицији
- Закон о спољним пословима
- Закон о Безбедносно-информативној агенцији
- Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији
- Законик о кривичном поступку и Кривични законик
- Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције
- Закон о државним службеницима
- Закон о информационој безбедности
- Закон о јавним набавкама и Уредба о јавним набавкама у области одбране и безбедности "Службени гласник РС", број 93 од 1. јула 2020.
- Закон о електронским комуникацијама
- Закон о пореском поступку и пореској администрацији
- Закон о заштити узбуњивача
- Закон о приватном обезбеђењу

## ЗАКОН О ТАЈНОСТИ ПОДАТАКА

Овим законом уређује се јединствен систем одређивања и заштите тајних података који су од интереса за националну и јавну безбедност, одбрану, унутрашње и спољне послове Републике Србије, заштите страних тајних података, приступ тајним подацима и престанак њихове тајности, надлежност органа и надзор над спровођењем овог закона, као и одговорност за неизвршавање обавеза из овог закона и друга питања од значаја за заштиту тајности података.

## РАД СА ТАЈНИМ ПОДАЦИМА

- УРЕДБА о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА” и „СТРОГО ПОВЕРЉИВО” - "Службени гласник РС", број 46 од 24. маја 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у органима јавне власти - "Службени гласник РС", број 79 од 29. јула 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству одбране - "Службени гласник РС", број 66 од 29. јуна 2014.



- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству унутрашњих послова "Службени гласник РС", број 105 од 29. новембра 2013.
  - УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Безбедносно-информативној агенцији "Службени гласник РС", број 70 од 7. августа 2013.
  - УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Канцеларији Савета за националну безбедност и заштиту тајних података "Службени гласник РС", број 86 од 30. септембра 2013.
  - УРЕДБА о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа "Службени гласник РС", број 63 од 19. јула 2013.
  - УРЕДБА о посебним мерама физичко-техничке заштите тајних података "Службени гласник РС", број 97 од 21. децембра 2011.
  - УРЕДБА о посебним мерама надзора над поступањем са тајним подацима „Службени гласник РС“, број 90 од 30. новембра 2011.
  - УРЕДБА о посебним мерама заштите тајних података у информационо-телекомуникационим системима "Службени гласник РС", број 53 од 20. јула 2011.
  - УРЕДБА о начину и поступку означавања тајности података, односно докумената "Службени гласник РС", број 8 од 11. фебруара 2011.
  - УРЕДБА о садржини, облику и начину вођења евиденција за приступ тајним подацима "Службени гласник РС", број 89 од 29. новембра 2010.
  - УРЕДБА о садржини, облику и начину достављања сертификата за приступ тајним подацима „Службени гласник РС“, број 54 од 4. августа 2010.
  - УРЕДБА о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података у Канцеларији Савета за националну безбедност и заштиту тајних података и Министарству правде "Службени гласник РС", број 79 од 29. октобра 2010.
  - УРЕДБА о обрасцима безбедносних упитника "Службени гласник РС", број 30 од 07. маја 2010.
- ПРАВИЛНИК о службеној легитимацији и начину рада лица овлашћених за вршење надзора "Службени гласник РС", бр. 85 од 27. септембра 2013, 71 од 11. јула 2014.

## НЕОПХОДНИ КОРАЦИ

- Имплементација Закона о тајности података у органу јавне власти (организациона безбедност)
  1. Процена стања и безбедности
  2. Доношење нормативе за рад са тајним подацима
  3. Одређивање руковоаца тајних података
  4. Успостављање и спровођење унутрашње контроле
  5. Креирање листе «потребно да зна» за запослене
  6. Процес сертификације физичких и правних лица (поверљиве набавке)
  7. Успостављање општих и посебних мера заштите тајних података
  8. Формирање регистра за рад са тајним подацима (страним тајним подацима)
  9. Успостављање система интерних едукације за рад са тајним подацима у органу јавне власти
  10. Успостављање ИКТ система за рад са тајним подацима
  11. Надзор (стручни) од стране Канцеларије Савета за националну безбедност и заштиту тајних података
  12. Инспекцијски надзор Министарства правде

## ОРГАНИЗАЦИЈА РАДА СА ТАЈНИМ ПОДАЦИМА

- Руковалац тајним подацима
- Одлука о подацима од интереса за Републику Србију (информатор о раду органа)...
- УНУТРАШЊА КОНТРОЛА
- План рада са тајним подацима
- План за ванредне и хитне ситуације
- Мере заштите тајних података
- ИКТ системи
- Акт о информационој безбедности
- Остало...

**Наслеђено стање** је врло хетерогено, јер су администрације преузете са нормативом, које је потицало из савезних институција и републичких органа на нивоу Републике Србије. Сам модел заштите тајних података, када су у питању критеријуми за одређивање степена тајности, до распада СФРЈ (али и касније!), био је заснован на концепту Општенародне одбране и друштвене самозаштите и законима и прописима СФРЈ са којима су били усаглашени одговарајући републички прописи из ове области. Интересантно је да се модел одређивања степена тајности по прописима СФРЈ примењује још увек у Словенији, Хрватској, Македонији и БиХ, док Црна Гора још увек примењује старе прописе из области одбране СРЈ. Током 90-их година ХХ века дошло је до процеса напуштања концепта Општенародне одбране и друштвене самозаштите, који је за последицу имао и разарање уређених капацитета за заштиту тајних података који су наслеђени од СФРЈ, а у пракси је на савезном нивоу дата алтернатива за овај концепт као систем одбране, док је безбедност препуштена федералним републикама, односно државама чланицама. Тако је на пример, Централни регистар страних тајних података и регистар председништва СФРЈ трансформисан у ресторан и место за одлагање смећа, а касе за чување тајних података уклоњене из радних простора и углавном продате у старо гвожђе. У свим државним органима расформиране су организационе јединице које су се бавиле унутрашњом контролом и заштитом тајних података (процеси рационализације), а да при томе нису формиране нове, док је формално задржан систем рада са тајним подацима који је у пракси често злоупотребљаван и ненаменски коришћен што за последицу има константно отицање тајних података у медије. Када говоримо о тренутном стању у области заштите тајних података, карактеристично је да све три гране власти имају одређене особености у раду са тајним подацима, али да су генерално преузеле стандарде из области одбране и канцеларијског пословања. Поред тога, већина нормативе и прописа које су донели старешине органа потиче из периода СФРЈ или из 90-их година ХХ века, али постоје и „новоформирани” органи који ову област уопште нису уредили.

### МЕЂУНАРОДНИ ПРИНЦИПИ У РАДУ СА ТАЈНИМ ПОДАЦИМА

**-NEED TO KNOW – ПОТРЕБНО ДА ЗНА – СТРОГО ПЕРСОНАЛНИ ПРИНЦИП И ОДНОСИ СЕ НА ПРИСТУП ТАЈНИМ ПОДАЦИМА У ОКВИРУ ЈЕДНОГ ДРЖАВНОГ ОРГАНА НА ОСНОВУ ЛИСТЕ ДУЖНОСТИ И ЛИЦА...**

**-NEED TO SHARE - ПОТРЕБНО ПОДЕЛИТИ СА – ПРИНЦИП КОЈИ СЕ ОДНОСИ НА ДИСТРИБУЦИЈУ ПОДАТАКА ИЗМЕЂУ РАЗЛИЧИТИХ ДРЖАВНИХ ОРГАНА**

## РЕГИСТАРСКИ СИСТЕМ

Руковање ТП предвиђено је само у уређеном систему који мора да буде реализован у складу са прописима и стандардима из области ЗТП. Тако уређен и акредитован систем представља регистарски систем.

За реализацију регистарског система неопходно је обезбедити:

- Адекватан простор који испуњава захтеве за рестриктивни приступ
- Лица одговорна за руковање и ЗТП (руковалац тајним подацима и руковалац регистра)
- Прописивање политике заштите и процедура за поступање са тајним подацима
- Едукације запослених из области ЗТП

## МЕЂУНАРОДНА САРАДЊА

- НАТО – потписан 2008. г. (ратификован)
- ЕУ - потписан 2011. г. (ратификован)
- Словачка, Бугарска - потписан 2011. г. (ратификован)
- Чешка Република, Словенија, БиХ - потписани 2013.г. (ратификовани )
- САД (GSOMIA) – потписан 2014. г. (ратификован)
- Македонија – потписан 2014. г. (ратификован)
- Шпанија – потписан 2014. г. (ратификован)
- Русија – потписан 2014. г. (ратификован)
- Пољска – потписан 2015. г. (ратификован)
- Румунија – потписан 2017. г. (ратификован)
- Кипар – потписан 2017. г. (ратификован)
- Француска – потписан 2018. г. (ратификован)
- Луксембург – потписан 2020. г. (ратификован)
- Мађарска – потписан 2023. г. (ратификован)



# ПЕРСОНАЛНА БЕЗБЕДНОСТ

Персонална безбедност представља примену мера којима се обезбеђује приступ тајним подацима само за лица која испуњавају следеће:

- Безбедносне провере
- Упознавање са прописаним политикама и процедурама заштите ТП - „брифинг“
- Безбедносни сертификат
- Листа „потребно да зна“

Мере и активности које се спроводе у домену персоналне безбедности имају веома важну улогу у процесу заштите тајних података.

Оне обухватају спровођење безбедносне провере за физичка лица, издавање безбедносног сертификата, подизање безбедносне културе и свести корисника тајних података, као и упознавање са организационом безбедношћу и системом заштите тајних података - обавезама рада са тајним подацима које проистичу из добијања безбедносног сертификата, ризиком од неовлашћеног приступа тајним подацима.

Испуњавање услова за издавање безбедносног сертификата је први корак и један од услова за приступ тајним подацима. Услови за издавање сертификата утврђују се кроз безбедносну проверу коју врше надлежне службе, на захтев органа јавне власти, а преко Канцеларије Савета за националну безбедност и заштиту тајних података.

Безбедносна провера се спроводи пре издавања сертификата и има за циљ да утврди лојалност, поверљивост и интегритет, односно да утврди одсуство/постојање безбедносног ризика лица за које се захтева безбедносни сертификат.

Безбедносни сертификат је документ који потврђује да лице има право приступа и коришћења тајних података у одговарајућој мери по принципу „потреба да зна“.

Подизање безбедносне културе и свести корисника тајних података спроводи се кроз континуирану обуку из области заштите и рада са тајним подацима, која се спроводи на свим нивоима, као и кроз редовне брифинге и дебрифинге о обавезама које произилазе из стицања безбедносног сертификата.

Ималац сертификата треба да буде у потпуности свестан мера и активности заштите тајних података, а за то га треба редовно подсећати на обавезе заштите тајних података, као и на опасност од одавања тајних података неовлашћеним лицима.

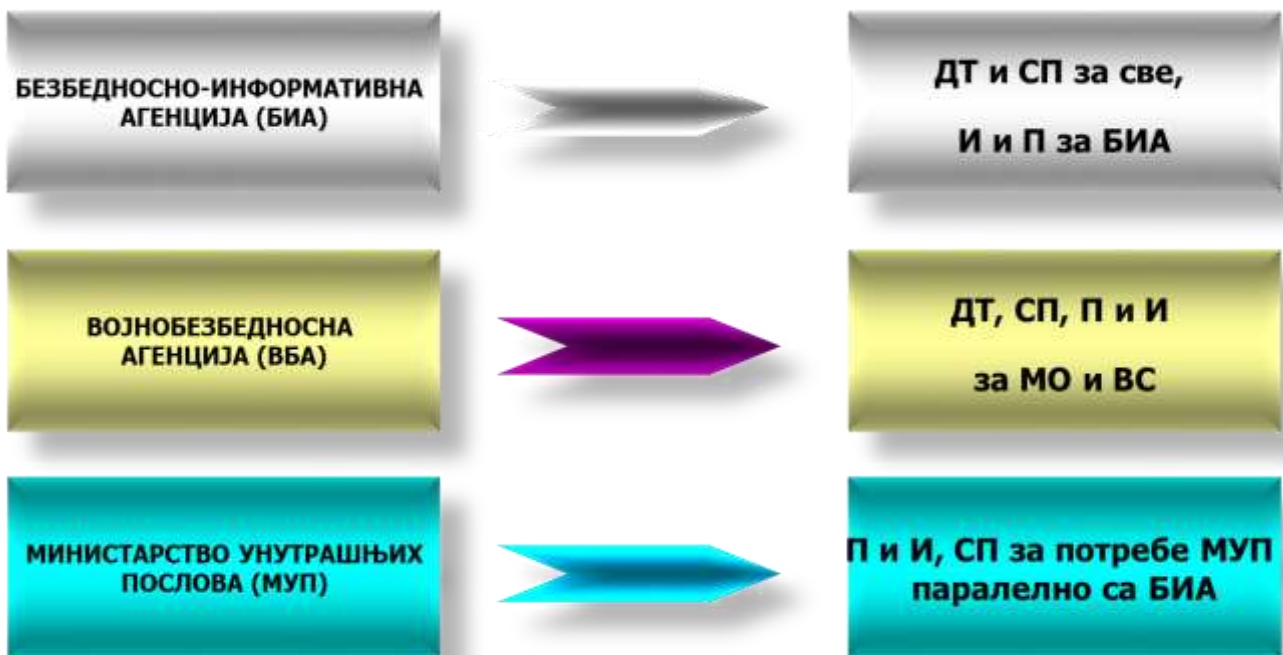
## НАЦИОНАЛНИ ПРОПИСИ

- Закон о тајности података
- Уредба о обрасцима безбедносних упитника
- Уредба о садржини, облику и начину вођења евиденција за приступ тајним подацима
- Уредба о садржини, облику и начину достављања сертификата за приступ тајним подацима
- Јединствена методологија за процену безбедносног ризика код физичких лица

## ПРОЦЕС ИЗДАВАЊА СЕРТИФИКАТА



## БЕЗБЕДНОСНЕ ПРОВЕРЕ



## ВРСТЕ БЕЗБЕДНОСНИХ ПРОВЕРА





### СВРХА БЕЗБЕДНОСНЕ ПРОВЕРЕ

Безбедносном провером подносиоца захтева врши се процена безбедносног ризика, нарочито од приступа и коришћења тајних података;

У оквиру безбедносне провере надлежан орган са аспекта безбедности оцењује наводе у попуњеном безбедносном упитнику;

Надлежан орган, у вези са наводима из безбедносног упитника, прикупља личне и друге податке од лица на које се ти подаци односе, од других органа јавне власти, организација и лица, из регистра, евиденција, датотека и збирки података које се воде на основу закона.

### БЕЗБЕДНОСНЕ ПРОВЕРЕ

Методологија процене безбедносног ризика код физичких лица за приступ тајним подацима. Извештај о резултатима безбедносне провере са препоруком.

### БЕЗБЕДНОСНИ СЕРТИФИКАТИ

Приступ тајним подацима, без извршене безбедносне провере и издатог безбедносног сертификата (на основу функције и у циљу обављања послова из своје надлежности) имају:

- председник Народне скупштине,
- председник Републике,
- председник Владе.

### ПРАВО ПРИСТУПА ТАЈНИМ ПОДАЦИМА

Имају само за лица која:



1. На основу одлуке председника Републике, Владе, старешине органа јавне власти...
2. На основу законског овлашћења, описа радног места и конкретне ситуације...
  - имају извршену безбедносну проверу одговарајућег нивоа
  - поседују безбедносни сертификат – одређеног СТ
  - задовољавају принцип „потребно да зна” (један од међународних принципа у раду са ТП)
  - која су детаљно информисана о својим одговорностима (извршен брифинг)

**НАПОМЕНА: поседовање решења, без издатог сертификата, не значи могућност приступања тајном податку!**

**Систематизована/формацијска радна места која у свом опису обухватају приступ тајним подацима уз процену могуће штете националној безбедности:**

- **ПОСЕБНО ОСЕТЉИВА – ТЕШКА НЕОТКЛОЊИВА ШТЕТА:** приступ тајним подацима ДРЖАВНА ТАЈНА; Пројектима ДТ и СП; Документа Савета за националну безбедност...
- **КРИТИЧНО ОСЕТЉИВА – ТЕШКА ШТЕТА:** приступ тајним подацима ДТ и СП;
- **НЕКРИТИЧНО ОСЕТЉИВА – ШТЕТА:** приступ тајним подацима СП и П;
- **НЕОСЕТЉИВА** (штета за рад органа јавне власти) - БЕЗ МОГУЋНОСТИ НАНОШЕЊА ШТЕТЕ НАЦИОНАЛНОЈ БЕЗБЕДНОСТИ

### УПОЗНАВАЊЕ СА БЕЗБЕДНОСНИМ ПРОЦЕДУРАМА -БРИФИНГ-

- Упознавање са безбедносним прописима у погледу заштите тајних података који су од интереса за националну безбедност, одбрану, унутрашње и спољне послове Републике Србије, као и правним и дисциплинским последицама кршења тих прописа
- Потписивање изјаве којом се лице обавезује да ће са тајним подацима поступати у складу са законском регулативом Републике Србије
- Последња фаза у поступку издавања безбедносних сертификата
- Пре издавања сертификата, односно дозволе, лице коме се издаје сертификат дужно је да потпише изјаву, којом потврђује да ће поступати са тајним подацима у складу са законом и другим прописом.
- Ако не потпише изјаву, поступак издавања сертификата, односно дозволе се обуставља.
- Писана изјава чини саставни део документације на основу које је издат сертификат, односно дозвола.
- По овом основу се устројава и посебна јединствена централна евиденција издатих сертификата....

## ЛИСТА „ПОТРЕБНО ДА ЗНА“

СПИСАК ЛИЦА КОЈА ИМАЈУ ПРИСТУП ТАЈНИМ ПОДАЦИМА У ЦЕНТРАЛНОМ РЕГИСТРУ МИНИСТАРСТВА X

РБ	Име и презиме	Степен тајности	Функција	Потребно да зна
1.		СТРОГО ПОВЕРЉИВО		ДА
2.		ИНТЕРНО		ДА
3.		ДРЖАВНА ТАЈНА		ДА
4.		СТРОГО ПОВЕРЉИВО		ДА
5.		СТРОГО ПОВЕРЉИВО		ДА
6.		ДРЖАВНА ТАЈНА		ДА
7.		ПОВЕРЉИВО		ДА
8.		СТРОГО ПОВЕРЉИВО		ДА
		ИНТЕРНО		ДА
9.		ИНТЕРНО		ДА
10.		СТРОГО ПОВЕРЉИВО		ДА

## УСЛОВИ ЗА ПРИСТУП ТАЈНОМ ПОДАТКУ



**„ПОВЕРЉИВО“ и више**



**„ИНТЕРНО“**

## СЕРТИФИКАТИ

Период важења сертификата је за:

- „ДРЖАВНУ ТАЈНУ“ - 3 године,
- „СТРОГО ПОВЕРЉИВО“ - 5 година,
- „ПОВЕРЉИВО“ - 10 година и
- „ИНТЕРНО“ - 15 година

За приступ подацима степена тајности „ИНТЕРНО“ сертификат се издаје само правним лицима, док физичка лица потписују изјаву којом се обавезују да ће са тајним подацима поступати у складу са позитивно правном регулативом Р. Србије.

### ПРЕСТАНАК ВАЖЕЊА СЕРТИФИКАТА

1. Истеком времена за које је издат,
2. Престанком функције лица из члана 38. закона,
3. Престанком обављања дужности и послова из делокруга рада лица из члана 40. закона,
4. На основу решења Канцеларије Савета донетог у поступку провере издатог сертификата,
5. Смрћу физичког лица или престанком правног лица коме је издат сертификат.

Ако је против лица коме је издат сертификат:

- покренут дисциплински поступак због теже повреде службене дужности,
- кривични поступак због основане сумње да је починио кривично дело за које се гони по службеној дужности, односно
- прекршајни поступак за прекршај предвиђен Законом о тајности података,

Руководилац органа јавне власти може решењем привремено забранити приступ тајним подацима том лицу, до правоснажног окончања поступка.

**ЗАБРАНА ПРИСТУПА ТАЈНИМ ПОДАЦИМА БЕЗ ГУБИТКА СЕРТИФИКАТА!**

### КРИВИЧНО ДЕЛО

Ко неовлашћено непозваном лицу саопшти, преда или учини доступним податке или документа који су му поверени или до којих је на други начин дошао или прибавља податке или документа, а који представљају тајне податке са ознаком тајности

- "ИНТЕРНО" или "ПОВЕРЉИВО", казниће се затвором од три месеца до три године.
- "СТРОГО ПОВЕРЉИВО", казниће се затвором од шест месеци до пет година.
- "ДРЖАВНА ТАЈНА", казниће се затвором од једне до десет година.

## БЕЗБЕДНОСНИ СЕРТИФИКАТ - за физичка лица –

Република Србија Канцеларија Савета за информациону безбедност и заштиту личних података

**СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА СТЕПЕНА  
ДРЖАВНА ТАЈНА**

Број сертификата \_\_\_\_\_ ДЛБГ \_\_\_\_\_  
 Име прилике \_\_\_\_\_  
 Име органа јавне власти или правног лица \_\_\_\_\_  
 Датум издавања \_\_\_\_\_ Валидо \_\_\_\_\_

М.П.                      Директор

Република Србија Канцеларија Савета за информациону безбедност и заштиту личних података

**СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА СТЕПЕНА  
СТРОГО ПОВЕРЉИВО**

Број сертификата \_\_\_\_\_ ДЛБГ \_\_\_\_\_  
 Име прилике \_\_\_\_\_  
 Име органа јавне власти или правног лица \_\_\_\_\_  
 Датум издавања \_\_\_\_\_ Валидо \_\_\_\_\_

М.П.                      Директор

Република Србија Канцеларија Савета за информациону безбедност и заштиту личних података

**СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА СТЕПЕНА  
ПОВЕРЉИВО**

Број сертификата \_\_\_\_\_ ДЛБГ \_\_\_\_\_  
 Име прилике \_\_\_\_\_  
 Име органа јавне власти или правног лица \_\_\_\_\_  
 Датум издавања \_\_\_\_\_ Валидо \_\_\_\_\_

М.П.                      Директор

ОВАЈ СЕРТИФИКАТ ИЗДАЈЕ СЕ У ОКЛАДУ СА ЧЛАНОМ 17. ЗАКОНА О ТАЈНОСТИ ПОДАТАКА („СЛУЖБЕНИ ГЛАСНИК РС“ БРОЈ 104/09) И ИМАЛАЦ СВОГ СЕРТИФИКАТА ИМА ПРАВО ПРИСТУПА ПОДАЦИМА СТЕПЕНА ТАЈНОСТИ „ДРЖАВНА ТАЈНА“ ПРИ ОВАВЉАЊУ ДУЖНОСТИ У ОКВИРУ РАДНИХ ЗАДАТАКА.

ИМАЛАЦ СВОГ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА УПОСНАТ ЈЕ СА ЗАКОНОМ И ДРУГИМ ПРОЦИСНИМА КОЈИМА СЕ УРЕЂУЈЕ ТАЈНОСТ ПОДАТАКА И ОБАВЕЗАН ЈЕ ДА ТАЈНЕ ПОДАТКЕ КОРИСТИ У ОКЛАДУ СА ТИМ ПРОЦИСНИМА.

ПОТПИС КОРИСНИКА СЕРТИФИКАТА

ОВАЈ СЕРТИФИКАТ ИЗДАЈЕ СЕ У ОКЛАДУ СА ЧЛАНОМ 17. ЗАКОНА О ТАЈНОСТИ ПОДАТАКА („СЛУЖБЕНИ ГЛАСНИК РС“ БРОЈ 104/09) И ИМАЛАЦ СВОГ СЕРТИФИКАТА ИМА ПРАВО ПРИСТУПА ПОДАЦИМА СТЕПЕНА ТАЈНОСТИ „СТРОГО ПОВЕРЉИВО“ ПРИ ОВАВЉАЊУ ДУЖНОСТИ У ОКВИРУ РАДНИХ ЗАДАТАКА.

ИМАЛАЦ СВОГ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА УПОСНАТ ЈЕ СА ЗАКОНОМ И ДРУГИМ ПРОЦИСНИМА КОЈИМА СЕ УРЕЂУЈЕ ТАЈНОСТ ПОДАТАКА И ОБАВЕЗАН ЈЕ ДА ТАЈНЕ ПОДАТКЕ КОРИСТИ У ОКЛАДУ СА ТИМ ПРОЦИСНИМА.

ПОТПИС КОРИСНИКА СЕРТИФИКАТА

ОВАЈ СЕРТИФИКАТ ИЗДАЈЕ СЕ У ОКЛАДУ СА ЧЛАНОМ 17. ЗАКОНА О ТАЈНОСТИ ПОДАТАКА („СЛУЖБЕНИ ГЛАСНИК РС“ БРОЈ 104/09) И ИМАЛАЦ СВОГ СЕРТИФИКАТА ИМА ПРАВО ПРИСТУПА ПОДАЦИМА СТЕПЕНА ТАЈНОСТИ „ПОВЕРЉИВО“ ПРИ ОВАВЉАЊУ ДУЖНОСТИ У ОКВИРУ РАДНИХ ЗАДАТАКА.

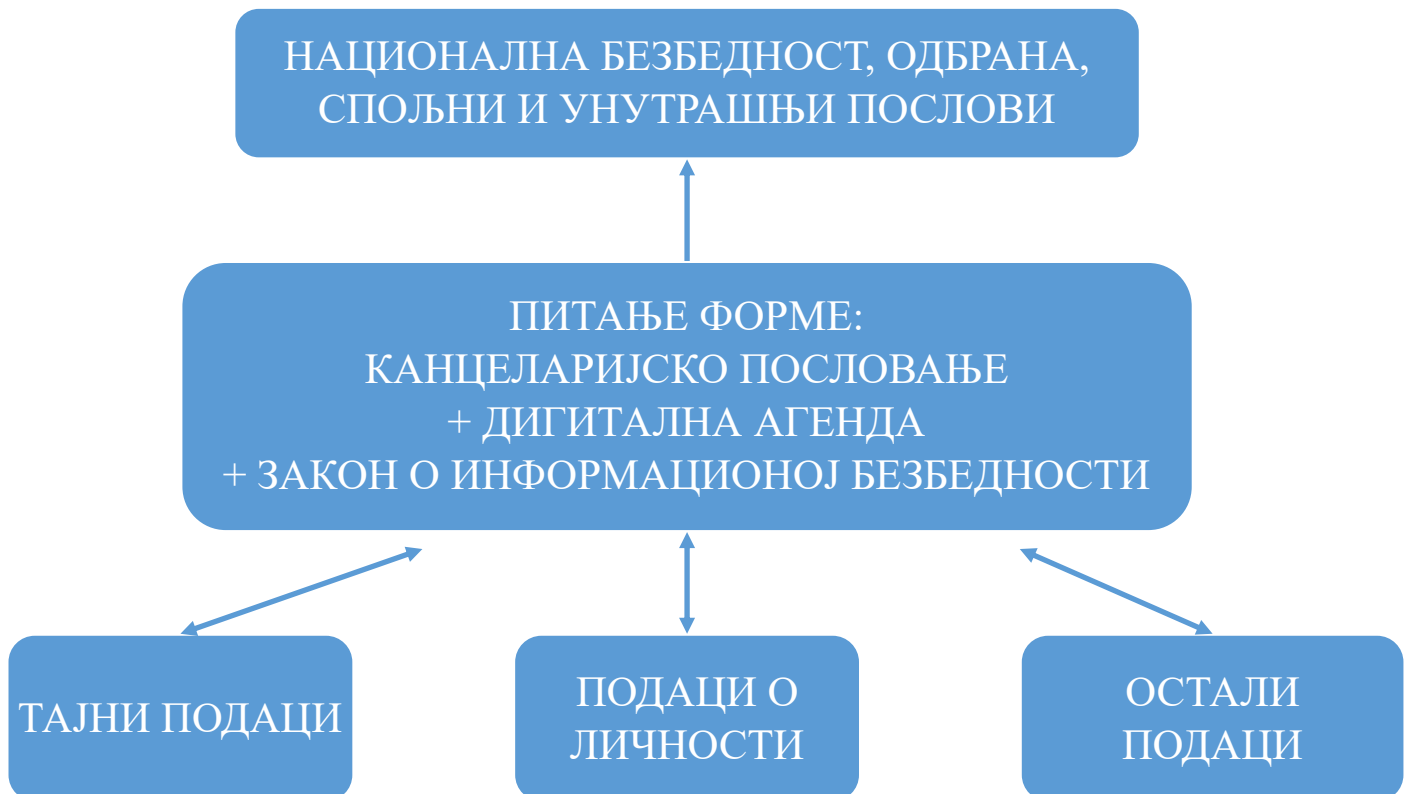
ИМАЛАЦ СВОГ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА УПОСНАТ ЈЕ СА ЗАКОНОМ И ДРУГИМ ПРОЦИСНИМА КОЈИМА СЕ УРЕЂУЈЕ ТАЈНОСТ ПОДАТАКА И ОБАВЕЗАН ЈЕ ДА ТАЈНЕ ПОДАТКЕ КОРИСТИ У ОКЛАДУ СА ТИМ ПРОЦИСНИМА.

ПОТПИС КОРИСНИКА СЕРТИФИКАТА

# АДМИНИСТРАТИВНА БЕЗБЕДНОСТ

## ЖИВОТНИ ЦИКЛУС У РАДУ СА БИЛО КОЈИМ ПОДАТКОМ ОБУХВАТА

- НАСТАНАК (ПРОВЕРА И ИЗНОШЕЊЕ ПОДАТКА У ОДГОВАРАЈУЋОЈ ФОРМИ + УНОШЕЊЕ У ОДГОВАРАЈУЋУ ЗБИРКУ ПОДАТАКА)
- КОРИШЋЕЊЕ И ДИСТРИБУЦИЈУ (ПРИСТУП, ИНФОРМАЦИЈА, АНАЛИЗА, КРИВИЧНА ПРИЈАВА, УПРАВНИ АКТ, СУДСКИ АКТ...)
- ПРЕНОШЕЊЕ (ДИГИТАЛНА АГЕНДА, КУРИРИ...)
- ЧУВАЊЕ И СКЛАДИШТЕЊЕ
- АРХИВИРАЊЕ ИЛИ УНИШТАВАЊЕ



Административна безбедност је адекватна и ефикасна класификација и заштита званичних информација које захтевају заштиту у интересу националне безбедности као и њихова декласификација када више не захтевају заштиту.

Административна безбедност тајних података предузима се у циљу обезбеђивања њихове правне, ефикасне и потпуне заштите при руковању истим, као и смањења или отклањања могућих ризика од неовлашћеног приступа, коришћења и руковања неовлашћеним лицима.

Административна безбедност тајног податка претпоставља се од тренутка доношења одлуке о одређивању тајности податка и траје до тренутка његовог физичког уништења или скидања ознаке тајности.

## Законски оквир

- Закон о тајности података
- Уредба о начину и поступку означавања тајности података, односно докумената

## ПОДАТАК ОД ИНТЕРЕСА ЗА РЕПУБЛИКУ СРБИЈУ ИЛИ ТАЈНИ ПОДАТАК

- 1) **податак од интереса за Републику Србију** је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и сувереност, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове;
- 2) **тајни податак** је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности;

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, односе се нарочито на:

- 1) националну безбедност Републике Србије, јавну безбедност, односно на одбрамбене, спољнополитичке, безбедносне и обавештајне послове органа јавне власти;
- 2) односе Републике Србије са другим државама, међународним организацијама и другим међународним субјектима;
- 3) системе, уређаје, пројекте, планове и структуре који су у вези са подацима из тач. 1) и 2) овог става;
- 4) научне, истраживачке, технолошке, економске и финансијске послове који су у вези са подацима из тач. 1) и 2) овог става.

### Закон о одбрани чл. 102 – мере заштите тајних података

Тајни подаци који се односе на систем одбране означени као подаци од интереса за националну безбедност Републике Србије, као и тајни подаци настали у раду команди, јединица и установа Војске Србије, чијим би откривањем неовлашћеним лицима настала штета, штите се у складу са законом којим се уређује заштита тајности податка и не могу се учинити доступним јавности.

### Тајним подацима значајним за систем одбране сматрају се:

- 1) подаци и документа од значаја за систем националне безбедности, чијим би откривањем неовлашћеним лицима могла настати штета по интересе и циљеве у области одбране;

- 2) подаци о плановима употребе Војске Србије, ратној организацији и формацији команди, јединица и установа Војске Србије, подаци о борбеним и другим материјалним средствима, односно врстама покретних ствари намењених потребама одбране, чијим би откривањем неовлашћеним лицима могла настати штета по оперативну и функционалну способност Војске Србије;
- 3) подаци о патентима значајним за одбрану земље и средствима и уређајима намењеним одбрани који су у процесу усвајања и испитивања;
- 4) подаци о војним објектима и другим непокретностима значајним за одбрану земље, изузев података који су према прописима о заштити животне средине неопходни за процену утицаја на животну средину;
- 5) подаци о предузетим мерама, радњама и поступцима садржани у одлукама, наређењима, саопштењима и другим актима у области одбране земље, чије би откривање нанело штету интересима снага одбране.

**МАТЕРИЈАЛНИ ЕЛЕМЕНТИ** – садржина, основи критеријума чл. 2, 8 и 14. ЗТП

**ФОРМАЛНИ ЕЛЕМЕНТИ** – облик испољавања, ознака тајности чл. 13 ЗТП + Уредба о начину и поступку означавања тајности података, односно докумената; Уредба о ближим критеријумима за одређивање степена тајности ДРЖАВНА ТАЈНА и СТРОГО ПОВЕРЉИВО...

## КРИТЕРИЈУМИ ЗА ОДРЕЂИВАЊЕ ТАЈНИХ ПОДАТАКА „ДРЖАВНА ТАЈНА“

Тајни податак из Уредбе о ближим критеријумима за одређивање степена тајности Државна тајна и Строго поверљиво, може се одредити и означити степеном тајности „ДРЖАВНА ТАЈНА“ ако би његовим откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала неотклоњива тешка штета по интересе Републике Србије, која за последицу може имати:

- 1) непосредно и изузетно озбиљно угрожавање територијалног интегритета и суверености Републике Србије;
- 2) непосредно и изузетно озбиљно угрожавање уставног поретка и демократских принципа Републике Србије;
- 3) масован губитак људских живота или изузетно озбиљну претњу по живот или здравље људи или имовину великог обима;
- 4) изузетно озбиљну и дугорочну штету по економске интересе Републике Србије;
- 5) изузетно озбиљно угрожавање националне и јавне безбедности, одбране или активности безбедносних и обавештајних служби;
- 6) изузетно озбиљно угрожавање интереса кривичног гоњења, сузбијања кривичних дела и функционисања правосуђа;
- 7) изузетно озбиљно угрожавање оперативних и функционалних способности Војске Србије и других снага одбране Републике Србије;
- 8) изузетно озбиљно угрожавање међународног положаја Републике Србије и сарадње са другим државама, међународним организацијама и другим међународним субјектима.



## КРИТЕРИЈУМИ ЗА ОДРЕЂИВАЊЕ ТАЈНИХ ПОДАТАКА НА ОСНОВУ ПРОПИСА О ОДБРАНИ

Подаци значајни за систем одбране који се морају чувати и штитити у складу са законом којим се уређује заштита тајности података су:

- 1) подаци садржани у војним, економским и другим проценама, на којима се заснива политика Републике Србије;
- 2) подаци садржани у Плану одбране Републике Србије;
- 3) подаци садржани у плановима употребе Војске Србије;
- 4) подаци о оперативним и функционалним способностима Министарства одбране и Војске Србије, као и других органа, предузећа и правних лица када су у функцији одбране;
- 5) подаци садржани у актима о организацији и формацији Војске Србије;
- 6) подаци садржани у плановима и програмима развоја за јавна предузећа, привредна друштва и друга правна лица која су од посебног значаја за одбрану земље;
- 7) подаци о врсти, укупној количини и размештају робних резерви Републике Србије и капацитетима и могућностима ратне производње;
- 8) подаци садржани у анализама и оценама стања припрема за одбрану Републике Србије;
- 9) подаци садржани у плановима припрема и уређења државне територије за потребе одбране земље;
- 10) подаци о војним објектима и објектима који су одлуком надлежног органа одређени као објекти од посебног значаја за одбрану земље (локација, назив, структура, опремљеност и други подаци који би у ратном и ванредном стању били од посебног значаја за одбрану земље);
- 11) подаци о научним, техничким и технолошким проналасцима који су од посебног значаја за одбрану земље;
- 12) подаци о средствима и уређајима намењеним одбрани земље, који су у процесу усвајања и испитивања;
- 13) подаци садржани у проценама, анализама и појединим мерама државних органа, који су од посебног значаја за одбрану земље;
- 14) подаци који се односе на организацију телекомуникационо-информационих система у миру и рату, планове и средства за криптозаштиту, као и подаци који се односе на прописане норме и поступке спровођења криптозаштите;
- 15) подаци који се односе на ратну организацију државних органа;
- 16) подаци садржани у мобилизацијским плановима јавних предузећа, привредних друштава и других правних лица која су од посебног значаја за одбрану земље;
- 17) подаци садржани у плановима организације безбедносно-обавештајних служби, оперативни подаци служби безбедности у вези са контраобавештајном и безбедносном заштитом и обавештајни подаци и подаци у вези са њима;
- 18) подаци Војне полиције о обављању послова сузбијања криминалитета, обезбеђења одређених личности, најзначајнијих војних објеката, докумената и наоружања и подаци у вези са њима;
- 19) подаци садржани у безбедносним проценама и подаци садржани у документима донетим у складу са безбедносним проценама;
- 20) подаци о материјалним средствима намењеним потребама одбране;
- 21) подаци који проистекну из истраживања геолошког састава земљишта, геомагнетизма, хидролошких карактеристика терена, који су од посебног значаја за одбрану земље;
- 22) подаци садржани у анализама и оценама стања припрема за одбрану јединица локалне самоуправе, појединих државних органа и других правних лица;
- 23) подаци садржани у инспекцијским извештајима са обилазака о стању одбрамбених припрема;

- 24) прописи о раду државних органа, привредних друштава и других правних лица за време ратног и ванредног стања;
- 25) подаци о дужностима и радним и формацијским местима значајним за одбрану земље;
- 26) подаци о организацији, формацији и структури војнотериторијалних органа и јединица;
- 27) подаци садржани у картографским публикацијама који су од интереса за одбрану земље;
- 28) аерофото снимци подручја значајних за одбрану;
- 29) подаци о укупној структури кадра и њиховом распореду на ратне дужности;
- 30) подаци о врстама и капацитетима природних и вештачких склоништа за заштиту становништва и материјалних добара у рату;
- 31) подаци о предузетим мерама и спроведеним радњама и поступцима, на основу одлука, наређења, саопштења и других аката којима се регулише област одбране земље, а чијим откривањем би се могла нанети штета по интересе Републике Србије и снагама одбране земље;
- 32) други подаци који су од стране надлежног органа утврђени као подаци од значаја за систем одбране.

Послови од посебног значаја за систем одбране које у државним органима, предузећима и другим правним лицима треба штитити применом посебних мера безбедности - чл. 3 Уредбе је предвиђено 10 категорија...

## КРИТЕРИЈУМИ И ШТЕТА КОД ТАЈНИХ ПОДАТАКА

- **ДРЖАВНА ТАЈНА** – неотклоњива тешка штета
- **СТРОГО ПОВЕРЉИВО** – тешка штета
- **ПОВЕРЉИВО** – штета
- **ИНТЕРНО** – штета за рад, обављање задатака и послова органа јавне власти

## ПРОЦЕНА ШТЕТЕ

- КО ЈЕ ВРШИ?
- НА КАКАВ НАЧИН?
- ПОСТОЈИ ЛИ МЕТОДОЛОГИЈА?
- ПИТАЊЕ ПОСЛЕДИЦА?

ПИТАЊЕ: ПРАВНА ИЛИ БЕЗБЕДНОСНА ПРОЦЕНА?

## ТАЈНОСТ ПОДАТАКА ЈЕ УВЕК УСЛОВЉЕНА

- Која врста података је у питању?
- Под каквим околностима?
- Колико дуго се морају чувати (максимално)?

## ОПОЗИВ ТАЈНОСТИ

- Окончањем правног посла или реализацијом неког догађаја...
- У периодичној процени....
- На предлог...
- У поступку вршења контроле...
- На основу одлуке надлежног органа...
- У јавном интересу (питање посебно интересантно у пракси...)

## ПРОБЛЕМ У ПРАКСИ - ТАЈНИ ПОДАТАК (ОРГАН ЈАВНЕ ВЛАСТИ)

**Орган јавне власти** је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује;

### ТУМАЧЕЊЕ чл. 2. т. 7 ЗТП – даје Министарство правде

Људске слободе и права и заштита личних података представљају два концепта који се узајамно преплићу.

Људске слободе и права (приватност) представљају материјални (суштински) део.

### Податак који се може одредити као тајни податак

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.

Подаци који подлежу означавању степена тајности и који су заштићени једним од законом утврђених степена тајности су из области: националне и јавне безбедности, одбране, спољних и унутрашњих послова (безбедносна, обавештајна и контраобавештајна делатност органа државне управе Републике Србије) и оно је што је везано за опстанак државе, а предмет је интересовања лица или организација које обављају обавештајне активности и активности које би могле да угрозе опстанак државе.

### Одређивање степена тајности

Степен тајности одређујемо у односу на штету која би се нанела Републици Србији у случају компромитације тог податка.

- Неотклоњива тешка штета – ДРЖАВНА ТАЈНА
- Тешка штета – СТРОГО ПОВЕРЉИВО
- Штета - ПОВЕРЉИВО,
- Штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио – ИНТЕРНО

## Овлашћено лице за одређивање тајности податка

- Председник Народне скупштине;
- Председник Републике;
- Председник Владе;
- Руководилац 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 руководилац органа јавне власти;
- Лице запослено у органу јавне власти које је за то писмено овластио руководилац тог органа.

**Овлашћено лице за одређивање тајности података (произвођач)** – креатор тајних података може бити свако лице које има одговарајући безбедносни сертификат и које према својим дужностима и задацима треба да креира, тј. рукује тајним подацима - информацијама.

Лица која рукују тајним подацима (креатори и корисници) у складу са Законом о тајности података предузимају мере и радње за административну безбедност где год постоји потреба за руковањем и чувањем тајних података.

Мере и активности за административну безбедност тајних података предузимају органи јавне власти (државни органи, јавне установе и службе, органи јединица локалне самоуправе) и друга правна и физичка лица у циљу обезбеђења заштите и правног поступања са тајним подацима као што су:

- правилно утврдити и означити степен тајности података;
- одмах их примите и евидентирајте у књиге евиденције;
- да обезбеди њихово правилно чување и руковање;
- да изврши правилну децимацију (даљу дистрибуцију), припрему копија, превода и извода и реализацију контроле дистрибуције до крајњих корисника по принципу „ТРЕБА ДА ЗНА“;
- да спречи и пријави сваки покушај неовлашћеног приступа и руковања од стране неовлашћених лица;
- да изврши правилан одабир архивске грађе, као и уклањање и уништавање одабране грађе за њу.
- правилном применом административних безбедносних мера и активности у великој мери ће се омогућити смањење ризика од неовлашћеног одавања тајних података, као и лакше откривање лица које је објавило или нарушило безбедност тајних података.

## Тајним податком се не сматра

Податак који је степенован ради:

- Прикривања кривичног дела;
- Прекорачења овлашћења;
- Злоупотребе службеног положаја;
- Другог незаконитог акта или поступања органа јавне власти.

Документ који садржи тајне податке означава се:

- Ознаком степена тајности;
- Начином престанка тајности;
- Подацима о овлашћеном лицу;

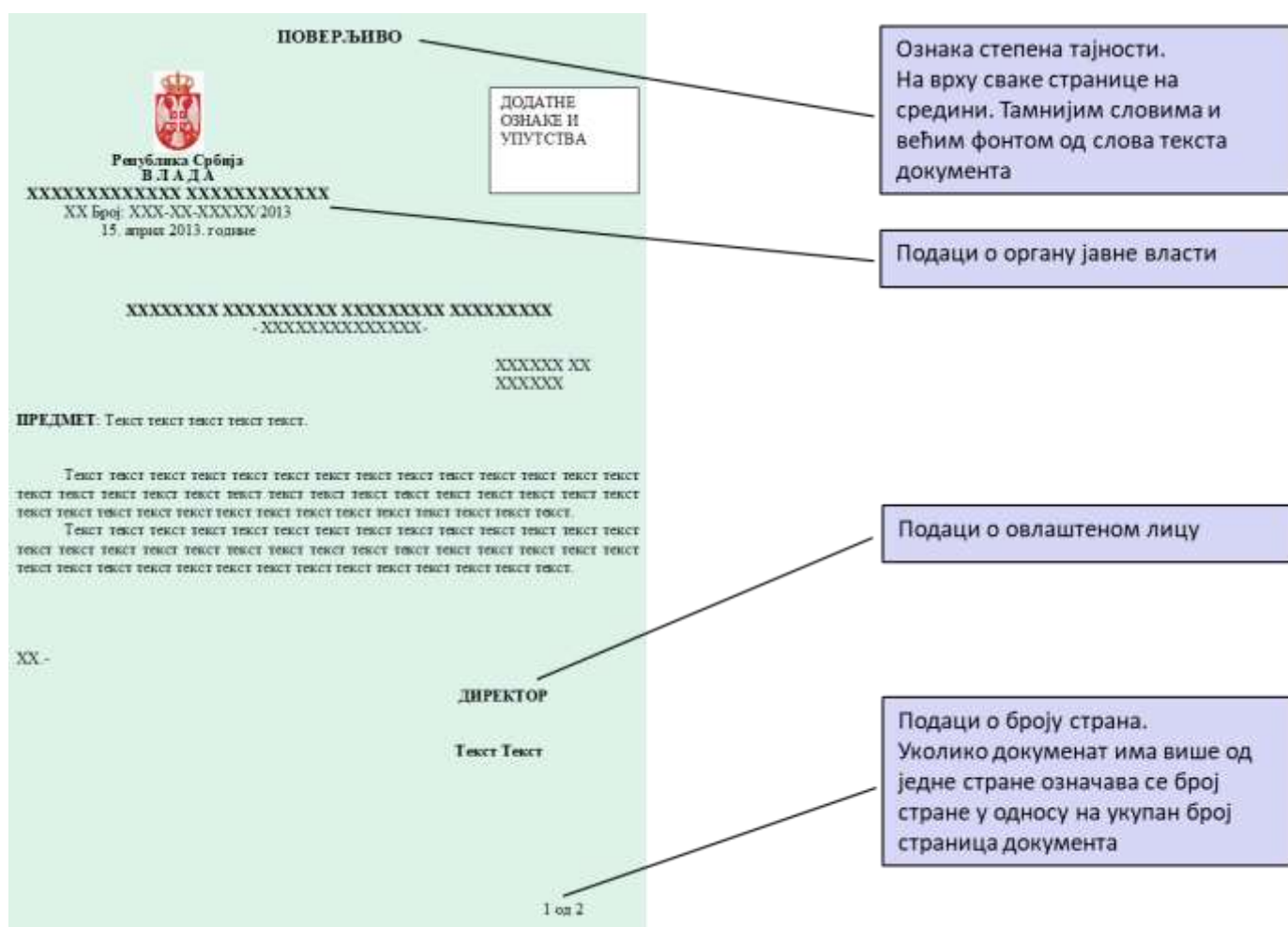
- Подацима о органу јавне власти.

### Када се одређује тајност податка

- Приликом настанка податка,
- При започињању посла који ће резултирати настанком тајног податка,
- Накнадно када се испуне критеријуми за одређивање,
- Лице које обрађује податке дужно је да обавести овлашћено лице о подацима који би могли да буду одређени као тајни.

### Одлука о одређивању степена тајности

- Овлашћено лице процењује могућу штету по интересе Републике Србије,
- Доноси одлуку у писаном облику са образложењем,
- Одређује најнижи степен тајности који спречава настанак штете.



## Поступак означавање докумената

**ОБРАЗАЦ**

**О ОЗНАЧАВАЊУ ДОКУМЕНТА КОЈИ САДРЖИ ТАЈНЕ ПОДАТКЕ СТЕПЕНА ТАЈНОСТИ "ПОВЕРЉИВО" И "ИНТЕРНО"**

1) ознака степена тајности \_\_\_\_\_

2) начин престанка тајности податка, односно документа \_\_\_\_\_

3) подаци о овлашћеном лицу \_\_\_\_\_

4) подаци о органу јавне власти \_\_\_\_\_

5) датум одређивања степена тајности \_\_\_\_\_

6) начин достављања тајног податка \_\_\_\_\_


ОВЛАШТЕНО ЛИЦЕ \_\_\_\_\_

- Датумом утврђеним на документу
- Настанком одређ. догађаја
- Истеком зак. рока
- Оповозом
- Ако је под. учињен дост. јавности

- Име и презиме лица
- Број овлашћења
- Ко је издао овлашћење

- Врши се на основу одредби члана 20. Уредбе о посебним мерама физичко техничке заштите тајних података

**ПОВЕРЉИВО**

  
Република Србија  
ВЛАДА  
XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
XX Број: XXX-XX-XXXXX/2013  
15. април 2013. године

XXXXXXXXXXXXXXXXXXXXXXXXXXXX  
-XXXXXXXXXXXXXXXXXXXX-

XXXXXX XX  
XXXXXX

**ПРЕДМЕТ:** Текст текст текст текст текст.

Текст текст текст текст текст **II** текст текст текст текст **II** текст текст текст текст  
текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст  
Текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст  
Текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст  
Текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст текст

XX-

**ДИРЕКТОР**

Текст Текст

1 од 2

- Ознака нај вишег степена тајности који се налази у документу
- Податак степена тајности интерно
- Податак степена тајности поверљиво





Остваривање увида у тајни податак

Кратак садржај предмета, број, датум, степен тајности и број примерака докуменатакоји садрже тајни податак:

РБр	Име и презиме лица које се упознало са тајним податком	Разлог увида	Датум и време када је увид остварен	Потпис лица које се упознало са тајним податком





## Законски рок престанка тајности података

ДРЖАВНА ТАЈНА – 30 година

СТРОГО ПОВЕРЉИВО – 15 година

ПОВЕРЉИВО – 5 година

ИНТЕРНО – 2 године

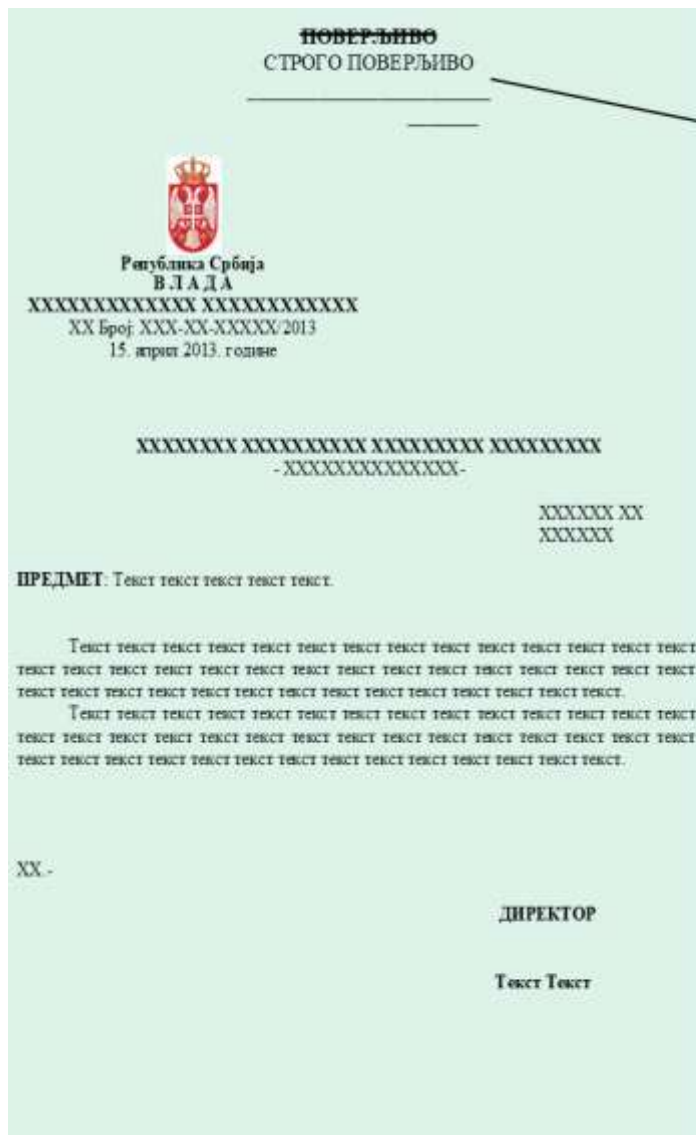
## Престанак тајности података

1. датумом утврђеним у документу у коме је садржан тајни податак;
2. наступањем одређеног догађаја утврђеног у документу у коме је садржан тајни податак;
3. истеком законом одређеног рока;
4. опозивом тајности;
5. ако је податак учињен доступним јавности.



Начин означавања престанка тајности документа, унети:

- Разлог
- Датум
- Потпис



- Начин означавања документа у случају промене степена тајности, унети:
- Број обавештења о промени степена тајности
  - Датум
  - Потпис

Припрема за слање тајног података

**СПОЉНА КОВЕРТА:**

Од тврдог, непровидног, непропусног материјала.

Ознаке органа коме се податак доставља и органа који податак доставља.

**УНУТРАШЊА КОВЕРТА:**

Поред ознака са спољне коверте, степен тајности, број и датум акта

**ДРЖАВНА ТАЈНА:**

Доставља се у две затворене коверте које морају бити у затвореном кофери, кутији или торби, са затварањем на кључ или са шифрованом комбинацијом

**СТРОГО ПОВЕРЉИВО и ПОВЕРЉИВО:**

Доставља се у две затворене коверте

Достављање тајног података

ДРЖАВНА ТАЈНА:

Доставља се преко најмање два курира

СТРОГО ПОВЕРЉИВО и ПОВЕРЉИВО:

Доставља се преко једног курира

ИНТЕРНО:

Преко курира или путем поште препорученом пошиљком са повратницом

РЕПУБЛИКА СРБИЈА

(назив органа јавне власти)

Број: \_\_\_\_\_

Датум: \_\_\_\_\_ године \_\_\_\_\_ (место)

На основу члана 161. Закона о општем управном поступку („Службени лист СРГ”, бр. 33/97 и 31/01 и „Службени гласник РС”, бр. 50/10), издаје се

**УВЕРЕЊЕ**

\_\_\_\_\_ (име и презиме лица коме се издаје уверење), који обавља послове радног места \_\_\_\_\_ (назив радног места) у \_\_\_\_\_ (навести назив органа јавне власти), поседује издат сертификат за приступ тајним подацима, означеним степеном тајности \_\_\_\_\_ (навести степен тајности).

\_\_\_\_\_ (име и презиме лица коме се издаје уверење) дужан-дужна је да покаже ово уверење на захтев лица којем предаје или од кога преузима тајни податак.

Ово уверење се издаје у циљу доказивања да лице \_\_\_\_\_ (име и презиме лица коме се издаје уверење), поседује одговарајући сертификат за приступ тајним подацима, као и да може преносити тајне податке и у друге сврхе се не може користити.

Назив функције руководиоца органа јавне власти, име, презиме и потпис

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Име и презиме курира

Назив радног места курира

Степен тајности за који курир поседује сертификат

Име и презиме курира

Име и презиме курира

**ПОТВРДА О ПРИЈЕМУ ТАЈНОГ ПОДАТКА**

\_\_\_\_\_ (навести ознаку степена тајности)  
 \_\_\_\_\_ (навести класификациони број предмета)

Потврђујем да сам дана \_\_\_\_\_ године (уписати тачан датум пријема), у \_\_\_\_\_ часова (уписати тачно време пријема тајног податка) примио тајни податак, означен степеном тајности \_\_\_\_\_, (уписати ознаку степена тајности) од \_\_\_\_\_ (уписати назив органа јавне власти који предаје тајни податак), који ми је предало лице \_\_\_\_\_ (уписати име и презиме лица које предаје тајни податак), за које је претходно утврђено да му је издат сертификат за приступ тајним подацима одговарајућег степена тајности.

У \_\_\_\_\_ (уписати назив места и број просторије у којој је извршена примопредаја тајног податка).

Име, презиме и потпис лица које је предало тајни податак \_\_\_\_\_  
 Назив корисника тајног податка, име и презиме лица које је примило тајни податак \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

### Обрађивање тајног податка ван безбедносне зоне

- Простор мора бити физички и технички обезбеђен;
- Тајни податак мора цело време бити под надзором;
- По завршеној обради тајни податак се враћа у безбедносну зону;
- Свако изношење и враћање тајног податка се евидентира;
- Лице које преузима тајни податак то потврђује потписом.

### Архивирање и уништавање тајних података

- Архивирање тајних података се врши у складу са прописима који уређују канцеларијско пословање органа јавне власти;
- Уништавање се врши средствима која елиминишу ризик препознавања или реконструкције информација (УКЉУЧУЈУЋИ РАДНА ДОКУМЕНТА);
- Комисија најмање три лица која поседују сертификат;
- Записник који потписују чланови комисије;
- Записник се чува трајно;
- О уништавању се писмено обавештава лице које је одредило степен тајности.

# ИНФОРМАЦИОНА ГАРАНЦИЈА

## ПОСТОЈЕЋЕ СТАЊЕ

- УПОТРЕБА ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА У РЕПУБЛИЦИ СРБИЈИ;
- ЈАВНА УПРАВА (E-GOVERNMENT);
- ИКТ СЕКТОР И
- ИНФОРМАЦИОНА БЕЗБЕДНОСТ.

### Прописи на снази:

- Закон о тајности података
- Закон о информационој безбедности
- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима

## ИНФОРМАЦИОНА БЕЗБЕДНОСТ

БЕЗБЕДНОСТ НА МРЕЖИ, ОДНОСНО ОНЛАЈН БЕЗБЕДНОСТ ЈЕ АКТУЕЛНА ТЕМА КОЈА ИЗАЗИВА ПАЖЊУ МНОГИХ СУБЈЕКТА, А НАРОЧИТО ЈЕ ЗНАЧАЈНА ЗА КОРИСНИКЕ И ПРОВАЈДЕРЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ (IT)

ПОЈАМ ИНФОРМАЦИОНА БЕЗБЕДНОСТ ПРЕДСТАВЉА СКУП МЕРА КОЈЕ ОМОГУЋАВАЈУ ДА ПОДАЦИ КОЈИМА СЕ РУКУЈЕ ПУТЕМ ИКТ СИСТЕМА БУДУ ЗАШТИЋЕНИ ОД НЕОВЛАШЋЕНОГ ПРИСТУПА, КАО И ДА СЕ ЗАШТИТИ ИНТЕГРИТЕТ, РАСПОЛОЖИВОСТ, АУТЕНТИЧНОСТ И НЕПОРЕЦИВОСТ ТИХ ПОДАТАКА, ДА БИ ТАЈ СИСТЕМ ФУНКЦИОНИСАО КАКО ЈЕ ПРЕДВИЂЕНО, КАДА ЈЕ ПРЕДВИЂЕНО И ПОД КОНТРОЛОМ ОВЛАШЋЕНИХ ЛИЦА.

ПРЕДСТАВЉА ПРАКСУ ЗАШТИТЕ ИНФОРМАЦИЈА УБЛАЖАВАЊЕМ РИЗИКА И ПРЕДСТАВЉА ДЕО УПРАВЉАЊА РИЗИКОМ (INFOSEC)...

## ШТА ЧИНИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ:

### 1. ЦИЉЕВИ

- очување поверљивости, интегритета и доступности информација
- заштита информација и инф.система од неовлашћеног приступа, коришћења, откривања, ометања, модификације или уништења у циљу обезбеђивања поверљивости, интегритета и доступности
- осигуравају да само овлашћени корисници (поверљивост) имају приступ тачним и потпуним информацијама (интегритет) када је то потребно (доступност)
- заштита интелектуалне својине организације
- управљање ризицима и трошковима информационог ризика за пословање
- обезбеђивање да су инф.ризички и контроле у равнотежи
- заштита информација, инф.система или база података од неовлашћеног приступа, оштећења, крађе или уништења

## 2. МЕРЕ

- скуп активности и радњи које предузимају државни органи, јавна предузећа, компаније и правна лица ради заштите одређених информација

## 3. АКТИВНОСТИ

- идентификација информација и сродних средстава, потенцијалних претњи, рањивости и утицаја
- процена ризика
- доношење одлука о третирању ризика (избегавњу, ублажавању, расподели или прихватању)
- избор и дизајн безбедносних контрола и спровођење
- надгледање активности и прилагођавање променама....

### САЈБЕР БЕЗБЕДНОСТ

**Сајбер безбедност** се може представити као примена технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.

Циљ сајбер безбедности јесте да се смањи ризик од сајбер напада и заштити од неовлашћеног искоришћавања система, мреже и технологије.

### ЕЛЕКТРОНСКА УПРАВА

**Електронска управа или е-управа** (енгл. e-administration) је термин чије дефиниције варирају од употребе информатичке технологије како би се олакшао промет информација и савладале физичке препреке традиционалних система до коришћења технологије како би се повећала доступност и олакшало извршење јавних служби у корист грађана, привредника, као и запослених у тим службама.

Устаљено виђење ствари иза ових дефиниција је да је е-управа заправо аутоматизација, односно компјутеризација постојећег „папир система“, која ће довести до нових стилова управљања, нових начина расправљања и одређивања стратегија, обављања послова, као и организовања и достављања информација.

**Развој е-управе у Републици Србији** подразумева успостављање ефикасне и кориснички оријентисане управе у дигиталном окружењу, која је интероперабилна како између различитих нивоа јавне управе у Србији, тако и са јавном управом држава чланица ЕУ.

Међутим, пут од стадијума на коме се тренутно налази еУправа у Србији, до наведеног жељеног стања, представља распон жељене промене, који подразумева јасно дефинисање циљева Програма, као и мера за постизање тих циљева, са јасно уочљивим узрочно последичним везама

На основу претходних реченица уочљиво је да сам развој подразумева концепцију и примену електронског пословања које користе сви (запослени у јавној управи, грађани, пословни људи, запослени људи у приватним објектима итд.).

Развојем е-управе омогућава се ефикаснија услуга према становништву, смањење трошкова, једноставније обављање послова уз добру организацију, сузбијање корупције и ефикаснији однос са привредним објектима.



Такође боља функционалност приступа подацима помаже развоју еУправе у Србији јер су грађани у прилици да лако провере тачност својих података и да се по потреби обратe надлежној институцији како би се ти подаци исправили.

### **Закон о информационој безбедности**

- Овим законом су уређене мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

### **ИКТ системи од посебног значаја су системи који се користе:**

- у обављању послова у органима јавне власти;
- за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности;

## **ИНФОРМАЦИОНА БЕЗБЕДНОСТ У СРБИЈИ**

Информациона безбедност је аспект безбедности који се односи на безбедносне ризике повезане са употребом информационо-комуникационих технологија, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца.

### **(Стратегија развоја инф.безбедности 2017...)**

## **ИНФОРМАЦИОНА БЕЗБЕДНОСТ**

- Безбедност локације (“сајта”)
- Безбедност ресурса
- Безбедност комуникацијске мреже
- Безбедност сервиса
- Безбедност приватности - личних података.

У рачунарским мрежама се у циљу спречавања евентуалних напада и могућих оштећења података примењују одређени сигурносни сервиси, од којих су најзначајнији:

- Аутентификација (authentication);
- Тајност података (data confidentiality);
- Непорицање порука (nonrepudiation);
- Интегритет података (data integrity);
- Контрола приступа (access control) и
- Распољивост ресурса (resource availability)

Ради повећања ИТ безбедности органи јавне власти, предузећа, односно компанија обично се примењује шест категорија безбедносних мера.

### **Избор мера зависиће од потребног нивоа безбедности**

- опште безбедносне политике и процедуре,
- софтвер за заштиту од вируса,
- дигитални потписи,
- шифровање,
- заштитни и (противпожарни) зидови и



- прокси сервери

## ОПШТЕ БЕЗБЕДНОСНЕ ПОЛИТИКЕ И ПОСТУПЦИ

- Честа промена приступних лозинки
- Ограничавање употребе система
- Ограничавање приступа подацима
- Успостављање контроле физичког приступа
- Подела одговорности
- Шифровање (енкрипција) података
- Успостављање процедуралне контроле
- Провођење едукативних програма
- Инспекција активности унутар система
- Бележење свих трансакција и активности корисника

## УРЕДБА О БЛИЖЕМ УРЕЂЕЊУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

- Ближе уређење мера заштите ИКТ система
- Послови и одговорност запослених
- Заштита информационог добара
- Средства и имовина за надзор над пословним процесима
- Управљање ризицима
- Постизање безбедности рада на даљину и мобилних уређаја
- Образовање, обуке и едукације + одговорност
- Заштита после промене радног места (уговор о поверљивости, клаузула забране конкурентности...)
- Класификовање података
- Заштита носача података
- Ограничење приступа и овлашћен приступ
- Мере криптозаштите...

## УРЕДБА О БЛИЖЕМ САДРЖАЈУ АКТА О БЕЗБЕДНОСТИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА, НАЧИНУ ПРОВЕРЕ И САДРЖАЈУ ИЗВЕШТАЈА ПРОВЕРЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Садржина акта о безбедности ИКТ система:

- мере заштите
- принципи
- начини и процедуре постизања нивоа безбедности
- овлашћења и одговорности
- Ресурси

КОМПАТИБИЛНО СА ISO/SRPS 27001

**Информациона безбедност тајних података** обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних информација које се обрађују у комуникационо-информаци-

оним системима – КИС. Процесом безбедносне акредитације ЦИС-а утврђује се да ли је имплементирани ЦИС постигао адекватан ниво заштите тајних података. ЦСИ безбедносна верификација обезбеђује:

- Потврда да ли су планиране мере безбедности КИС-а правилно спроведене;
- Потврда да су мере безбедности правилно спроведене и да је одговарајућим тестирањем постигнут захтевани ниво безбедности;
- Документовање резултата верификације безбедносне имплементације КИС-а; Ово потврђује да су испоштовани минимални безбедносни стандарди ЦСИ за обраду, складиштење и размену поверљивих информација.

Проценом могућег нарушавања безбедности тајних информација и безбедности ЦИС, односно проценом безбедносног ризика, вероватноћа да ће одређена рањивост ЦИС бити искоришћена претњом и довести до нарушавања безбедности ЦИС-а, сам систем је одређен. Процена безбедносног ризика служи за утврђивање безбедносних ризика, тј. претње и рањивост ЦСИ, утврђивање њихове величине, како би се идентификовале и одредиле области у којима је потребна заштита поверљивих информација у ЦСИ.

Рачунарска и комуникациона безбедност су суштински део информационе безбедности у заштити комуникационо-информационих система у којима се обрађују поверљиве информације. Применом мера безбедности из рачунарске и комуникационе безбедности постижу се следећи ефекти:

Идентификација особа које приступају систему;

Контрола и евиденција приступа системским објектима на основу датог права приступа из дефинисане базе података;

- Обезбеђивање поузданог начина да се укаже на степен класификације;
- Идентификација корисника и сигуран запис одштапаног, копираног, модификованог, копираног или избрисаног поверљивог документа;
- Заштита важних техничких и програмских елемената, могућности система и функционалност система;
- Контрола и управљање руковањем и преносом преносивих меморијских медија на којима се бележе поверљиви подаци;
- Планирање, конфигурирање, управљање и контрола мрежних уређаја.

Криптографска заштита комуникационо-информационих система у којима се обрађују поверљиве информације је део информационе безбедности. Применом криптографских средстава и метода обезбеђује се сигуран и заштићен пренос тајних података у ЦИС између две тачке кроз неконтролисани простор. Тиме се значајно повећава безбедност поверљивих информација, уз могућност њиховог компромитовања и штете

Информације електронски ван контролисаног простора, криптографске методе и средства морају се применити да би се сачувала аутентичност, интегритет и доступност поверљивих информација. Употреба је значајно смањена. Приликом преноса тајних, сваки комуникационо-информациони систем који обрађује тајнер податке састепеном тајности „ПОВЕРЉИВО“ и више требало би да буде заштићен компромитујућег електромагнетног зрачења (КЕМЗа).

Према резултатима мерења спроведених уз помоћ одговарајуће опреме за зонирање објеката и мерења електромагнетног зрачења одређују се безбедносне зоне у објектима у којима се обрађују тајни

подаци. У ствари, то значи одређивање просторија према степену заштите од електромагнетног зрачења.

На основу резултата добијених мерењима, предузимају се одређене безбедносне мере за смањење електромагнетног зрачења ван контролисаног простора установе, чиме се избегава могућност настанка отицања тајних података преко електромагнетних таласних компоненти комуникационо-информационе опреме.

У области емисионе безбедности, мерења електромагнетног зрачења врше се на опреми која ће се користити за обраду тајних података. На основу добијених резултата утврђује се врста опреме која ће се користити у одговарајућим зонама безбедности. Ова врста безбедносних мера је неопходна, јер је данас велика могућност компромитовања поверљивих информација које емитује комуникациона и информациона опрема.

У области емисионе безбедности, мерења електромагнетног зрачења врше се на опреми која ће се користити за обраду тајних података. На основу добијених резултата утврђује се врста опреме која ће се користити у одговарајућим зонама безбедности. Ова врста безбедносних мера је неопходна, јер је данас велика могућност компромитовања тајних података.

ИГ треба да обезбеди:

- поверљивост
- интегритет
- расположивост
- аутентификација
- непорецивост

Тајни податак не сме се преносити кроз систем изван безбедносних зона без примене метода и средстава криптозаштите, који су одобрени од стране органа надлежног за спровођење послова у области криптозаштите.

Приватна информационо-телекомуникациона средства и преносиви документи (лични рачунари, преносиви рачунари, дискете, меморијски модули и др.) не могу се користити за обраду ТП.

## СРПСКИ СТАНДАРД

- SRPS ISO/IEC 27001:2014, Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација – Захтеви
- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима (ЗТП)
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја (ЗИБ + ЗЗЛП)

## SRPS ISO 27001

- **ISO/IEC 27001** је међународни стандард за управљање безбедношћу информација .
- Детаљно описује захтеве за успостављање, имплементацију, одржавање и континуирано побољшање система управљања безбедношћу информација (ИСМС) – чији је циљ да помогне организацијама да учине безбеднијом информациону имовину коју држе.
- Већина организација има бројне контроле безбедности информација.

- Међутим, без система управљања безбедношћу информација (ИСМС), контроле имају тенденцију да буду донекле неорганизоване и неповезане, пошто се често примењују као тачна решења за специфичне ситуације или једноставно као ствар конвенције.
- Контроле безбедности које раде обично се баве одређеним аспектима информационе технологије (ИТ) или посебно безбедности података; остављајући не-ИТ информациона средства (као што су папирологија и власничка знања) мање заштићена у целини.
- Штавише, планирањем континуитета пословања и физичком безбедношћу може се управљати сасвим независно од ИТ или информационе безбедности, док се у пракси људских ресурса може мало помињати потреба да се дефинишу и доделе улоге и одговорности у области безбедности информација у целој организацији.

ISO/IEC 27001 захтева да менаџмент:

- Систематски испита ризике по безбедност информација организације, узимајући у обзир претње, рањивости и утицаје;
- Дизајнира и примени кохерентан и свеобухватан скуп контрола безбедности информација и/или других облика третмана ризика (као што је избегавање ризика или пренос ризика) како би се адресирали они ризици који се сматрају неприхватљивим; и
- Усвоји свеобухватни процес управљања како бисте осигурали да контроле безбедности информација настављају да испуњавају потребе организације за безбедност информација на сталној основи.

## СТАНДАРДИ ISO/IEC 17799

- политику безбедности;
- организовање информатичке безбедности;
- управљање ресурсима;
- безбедност људских ресурса;
- физичку заштиту;
- управљање радом и комуникацијама;
- контролу приступа;
- набављање, развој и одржавање информатичких система, управљање безбедосним инцидентима;
- управљање континуитетом пословања и усаглашеност за законском регулативом.

# ФИЗИЧКА БЕЗБЕДНОСТ

## ПРОПИСИ

- Закон о тајности података
- Уредба о посебним мерама физичко-техничке заштите тајних података

## ФИЗИЧКА БЕЗБЕДНОСТ

Физичка безбедност представља примену физичких и техничких мера заштите ради спречавања неовлашћеног приступа тајним подацима и у суштини представља комбинацију безбедносних процедура и техничких стандарда који се заснивају на препорукама, процени и пракси.

Физичко обезбеђење тајних података спроводи се у циљу смањења ризика, спречавања неовлашћеног приступа, откривања покушаја неовлашћеног приступа и ефикасног одговора на њега.

Мере физичке безбедности спроводе се за све локације, зграде, канцеларије, просторије и друге просторе у којима се рукује и чувају тајни подаци, укључујући и просторе у којима се налазе ИКТ системи, са обавезом да:

- омогући чување тајних података и руковање њима на одговарајући начин;
- одвојити особље у зони приступа тајним подацима по принципу „Потребно да зна“, а где је могуће према њиховом безбедносном сертификату; одвратити, спречити и открити неовлашћени приступ; и
- одбити или одложити радње прикривених или насилних улазака уљеза и нелојалног особља.

Избор мера које ће се користити за физичку безбедност тајних података зависи од специфичности објекта, броја тајних података, њиховог степена, као и шире локације објекта. На основу ових параметара ради се општа процена ризика на основу које се примењују мере физичког обезбеђења. Сврха процене је да се она координира и оптимизује коришћење ресурса и надгледа, контролише и минимизира претње које могу да угрозе безбедност.

Мере физичког обезбеђења треба да се заснивају на принципу „дубинске одбране“, иако су мере физичког обезбеђења специфичне за сваки објекат посебно, увек треба примењивати принцип „дубинске одбране“.

Руковање и чување тајних података врши се у безбедносним и административним зонама.

Области у којима се обрађују и чувају тајни подаци степена тајности „поверљиво“ и више су успостављене као безбедносне зоне првог и/или другог нивоа.

Подручја у којима се обрађују и чувају тајни подаци „Интерног“ нивоа се успостављају као административне зоне. Административне зоне се успостављају испред и око безбедносних зона. Увек треба примењивати принцип „одбране по дубини“.

Тајни подаци који нису под контролом и надзором лица овлашћених за руковање, морају се ставити и закључати у сефове, просторије или зоне, одређене према степену тајности података.

Физичко обезбеђење тајних података прописује услове за пријем посетилаца у административно-безбедносним зонама, контролу кључева и шифри сигурносних сефова и сигурносних врата и њихову заштиту, као и стандарде за сертификовану безбедносну опрему која се користи. ради заштите и чувања тајних података.

Употреба сертификоване безбедносне опреме пружа адекватну заштиту поверљивих података, у складу са степеном њихове тајности, а у комбинацији са принципом „дубинске одбране“ представља моћно средство у борби против нелојалног особља и спољних уљеза који циљају тајне податке.

## РЕЛЕВАНТНИ ФАКТОРИ

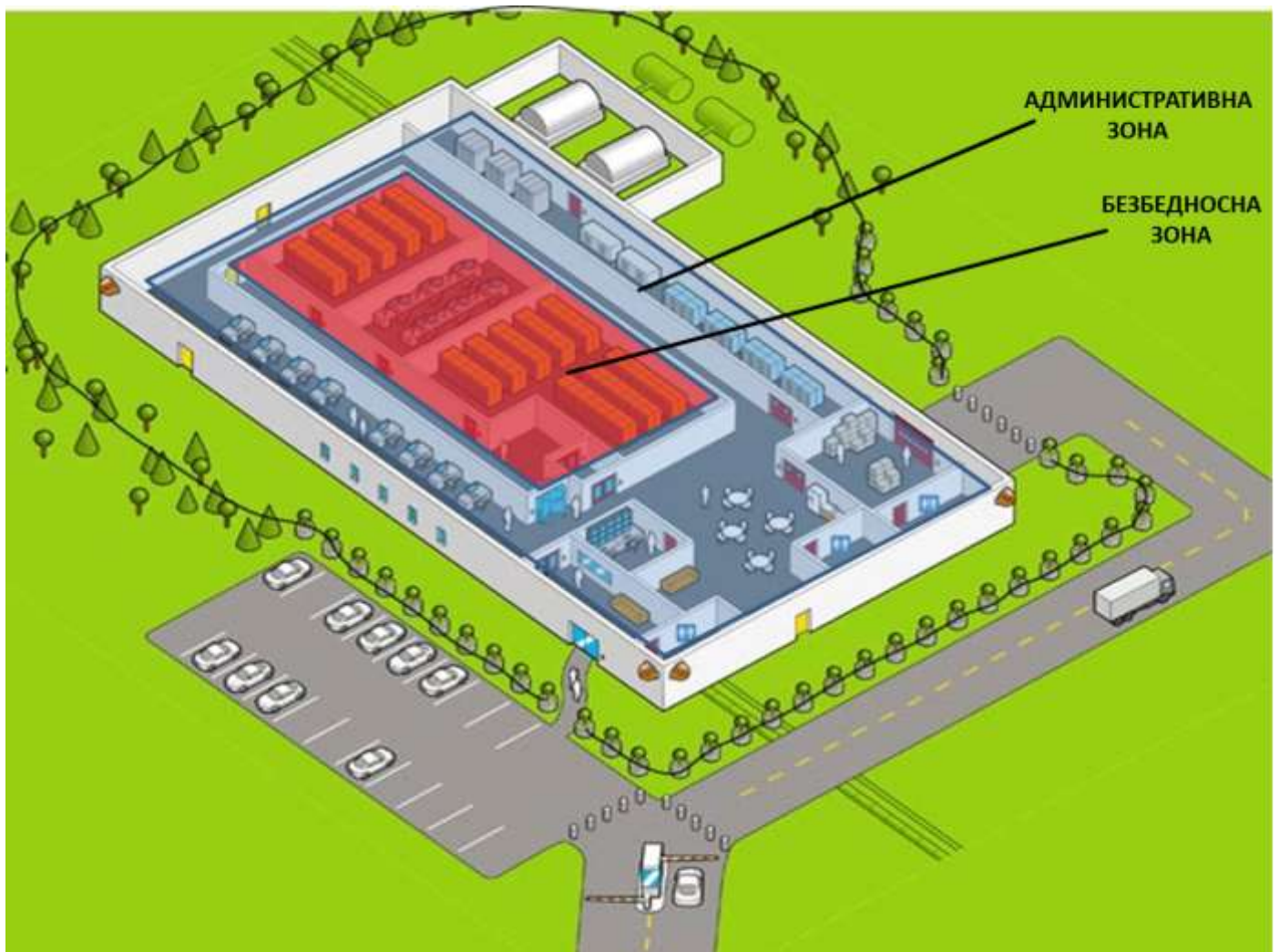
Релевантни фактори за одређивање степена потребних мера физичко-техничке заштите су:

- Процена претње за безбедност тајног података
- Степен тајности података
- Природа/облик документа у коме је садржан тајни податак (штампани/електронски)

За заштиту ТП примењује се вишеслојни систем заштите „одбрана по дубини“, уз коришћење одговарајуће комбинације комплементарних мера физичког и техничког обезбеђења које пружају степен заштите у складу са значајем и осетљивошћу тајног података.







### Опште мере заштите

- одређивање степена тајности
- процену претње за безбедност тајног податка
- одређивање начина коришћења и поступања са тајним податком
- одређивање одговорног лица за чување, коришћење, размену и друге радње обраде тајног податка
- одређивање руковоаца тајним подацима, укључујући и његову безбедносну проверу у зависности од степена тајности податка

### Посебне мере физичко-техничке заштите

Обезбеђују податке о стању безбедносних зона и податке о нарушавању безбедности. Могу бити:

- Системи за контролу приступа
- Противпровални системи
- Системи видео надзора
- Паник системи
- Опрема за детекцију предмета и супстанци
- Противпожарни системи



## Опрема за обраду ТП

Фотокопир апарат, телефакс и другу опрему неопходну за обраду ТП, могу употребљавати само лица која имају одговарајући сертификат за приступ ТП (означавају се одговарајућим степеном тајности).

### Простори са рестриктивним приступом:

- Административна подручја/зоне
- Безбедносна подручја / зоне:
  - подручје I степена заштите
  - подручје II степена заштите

**Безбедносна зона I степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО”. Самим уласком у ову зону сматра се да је остварен приступ тајним подацима.

Посебне физичко-техничке мере заштите тајних података у безбедносној зони I степена, обухватају:

- 1) надзор којим се обезбеђује потпуна контрола и евиденција улаза и излаза;
- 2) вођење евиденције о приступу тајним подацима;
- 3) забрану уношења механичких, електронских и магнетно-оптичких средстава и делова средстава, којима би се могао неовлашћено снимити, однети или пренети тајни податак;
- 4) непосредно и непрекидно физичко обезбеђење, које се, у складу са проценом, може допунити или заменити електронским системом за противпровално обезбеђење, чији је алармни систем повезан са одговарајућом јединицом за интервенцију;
- 5) непрекидно техничко обезбеђење са резервним напајањем, којим се остварује потпуни надзор безбедносне зоне, као замена непрекидном физичком обезбеђењу;
- 6) прегледање простора или просторије по завршеном радном времену.

Простор или просторије безбедносне зоне I степена морају испуњавати одговарајуће SRPS/EN техничке стандарде.

**Безбедносна зона II степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО”.

Улазак и кретање у тој зони не сматра се приступом тајним подацима.

Посебне физичко-техничке мере заштите тајних података у безбедносној зони II степена, обухватају:

- 1) надзор којим се обезбеђује потпуна контрола и евиденција улаза и излаза;
- 2) организацију рада која обезбеђује запосленима приступ само оним тајним подацима који су им потребни за извршавање радних задатака и до оног степена тајности за који имају сертификат;
- 3) надзор који обезбеђује да друга лица која имају дозволу за приступ тајним подацима улазе у ову зону само у пратњи запосленог;
- 4) забрану уношења механичких, електронских и магнетно-оптичких средстава и делова средстава, којима би се могао неовлашћено снимити, однети или пренети тајни податак, без одобрења овлашћеног лица;

5) физичко или противпробално обезбеђење простора или просторије, као и њихово повремено прегледање по завршеном радном времену.

### Противприслушни преглед

Врши се у свим просторима безбедносне зоне I или II степена и то:

- приликом одређивања безбедносне зоне
- код сваког насилног упада или неовлашћеног приступа у зону
- после распоређивања на друго радно место које не подразумева приступ ТП или престанка радног односа запосленог који је руковао ТП
- после извођења било које врсте грађевинских или радова на телекомуникационој опреми
- сваких шест месеци

МОГУ СЕ СПРОВЕСТИ И ДРУГЕ МЕРЕ ЗАШТИТЕ ТП

### Уништавање тајних података

- Уништавање хемијским разлагањем, спаљивањем, дробљењем, ...
- Комисија најмање три лица која поседују сертификат
- Записник који потписују чланови комисије
- Записник се чува трајно
- О уништавању се писмено обавештава лице које је одредило степен тајности

# ИНДУСТРИЈСКА БЕЗБЕДНОСТ

Да би заштитила националну безбедност Републике Србије, законодавац и Влада су морали заштите тајне податке (податке од интереса за Републику Србију), али у исто време Влада мора да дели ове информације са стотинама компанија које раде као државни извођачи и захтевају приступ тајним подацима током реализације поверљивих набавки и поверљивих уговора, програма, понуда и истраживања и развоја различитих средстава од значја за националну безбедност и одбрану.

Да би се у складу са прописима и безбедно уступали тајни подаци са државним извођачима, Влада је успоставила Систем заштите тајних података, заснован на прописима о заштити тајних података и поверљивим набавкама. Да би заштитили тајни подаци поверени индустрији, Систем заштите тајних података се ослања на многе појединце, из индустрије и владе, у широком спектру улога и са различитим одговорности.

Као неко ко игра улогу у индустријској безбедности, важно је да се разумеју не само дужности, али улоге и одговорности другог кључног особља за индустријску безбедност као национално добро Републике Србије.

Заједничко разумевање сврхе и структуре Система заштите тајних података и концепта индустријске безбедности, као и улога и одговорности његових кључних играча, помоћи ће свим корисницима да изврше свој део посла у заштити националне безбедности.

## ИНДУСТРИЈСКА БЕЗБЕДНОСТ - ПРАВНИ ОКВИР

- Закон о тајности података
- Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа – примењује се од јануара 2014 године.

## ИНДУСТРИЈСКА БЕЗБЕДНОСТ - КОРЕЛАЦИЈА СА ЈАВНИМ НАБАВКАМА?

**члан 46. ЗТП** - Овлашћено лице може тајне податке доставити другим правним или физичким лицима, која по основу уговорног односа пружају услуге органу јавне власти, ако:

1. правно или физичко лице испуњава организационе и техничке услове за чување тајних података у складу са овим законом и прописом донетим на основу овог закона;
2. су за лица која обављају уговорене послове извршене безбедносне провере и издати сертификати;
3. лица из тачке 2) овог става писаном изјавом потврде да су упозната са овим законом и другим прописима који уређују чување тајних података и обавезу се да ће са тајним подацима поступати у складу са тим прописима;
4. је приступ тајним подацима неопходно потребан ради реализације послова предвиђених уговором.

Мере заштите тајних података које проистичу из става 1. овог члана морају бити садржане у уговору који у вези са реализацијом послова закључе орган јавне власти и правно или физичко лице.

**ЗАКОН О ЈАВНИМ НАБАВКАМА** препознаје у члану 2. под тачкама:

25) војна опрема је опрема која је посебно израђена или прилагођена за војне потребе и намењена за употребу као оружје, муниција или војни материјал, а нарочито војна опрема из Прилога 2. овог закона (I. Списак војне опреме);

26) безбедносно осетљива опрема, услуге и радови су добра, услуге и радови за безбедносне потребе, које укључују, захтевају и/или садрже тајне податке.

## ПОСЕБНИ ИЗУЗЕЦИ У ОБЛАСТИ БЕЗБЕДНОСТИ И ОДБРАНЕ

**Члан 20. ЗЈН** - Одредбе овог закона наручиоци не примењују на доделу уговора о јавним набавкама и конкурса за дизајн у области одбране и безбедности:

1. на које се примењују посебна правила набавки, у складу са међународним уговором или аранжманом који се односи на размештај снага и тиче се активности Републике Србије, државе чланице Европске уније или треће државе;
2. код којих би примена одредаба овог закона обавезала Републику Србију да открије податке чије откривање је у супротности са битним интересима њене безбедности, а на основу одлуке Владе;
3. за потребе обавештајних активности;
4. у оквиру програма сарадње који се заснивају на истраживању и развоју новог производа, који заједно реализује Република Србија и једна или више држава чланица Европске уније, када је то примењиво на наредне фазе целог или дела животног циклуса тог производа;
5. који се закључују у трећој држави, укључујући и набавке за цивилне потребе, када су снаге размештене изван територије Републике Србије и Европске уније, ако оперативне потребе захтевају да уговори буду закључени са привредним субјектима на територији вршења активности;
6. које закључује Република Србија са органима државне, регионалне или локалне самоуправе других држава, а односе се на:
  - (1) набавку војне опреме или безбедносно осетљиве опреме;
  - (2) радове и услуге директно повезане са таквом опремом или
  - (3) радове и услуге искључиво за војне потребе или безбедносно осетљиве радове и безбедносно осетљиве услуге.

**Члан 21.** – Посебни изузеци за јавне набавке које имају одбрамбене или безбедносне аспекте

Одредбе овог закона не примењују се:

1. на закључење уговора о јавној набавци и конкурсе за дизајн који нису изузети чланом 20. став 1. овог закона, уколико би Република Србија применом овог закона била обавезна да пружи информације за које сматра да би њихово откривање штетило битним интересима њене безбедности;
2. на закључење уговора о јавној набавци и конкурсе за дизајн који нису изузети чланом 20. став 1. овог закона, уколико се заштита битних безбедносних интереса Републике Србије не може гарантовати другим мерама, као што је одређивање захтева у циљу заштите тајности података које наручилац ставља на располагање у поступку јавне набавке, у складу са овим законом;

3. ако су набавка и извршење уговора о јавној набавци и конкурси за дизајн проглашени тајним или морају бити пропраћени посебним безбедносним мерама, у складу са законима, подзаконским актима или управним актима под условом да је Република Србија утврдила да битне безбедносне интересе није могуће заштитити другим мерама, попут мера из тачке 2) овог става.

Влада одлучује о примени изузетака из става 1. овог члана.

## УРЕДБА О ЈАВНИМ НАБАВКАМА У ОБЛАСТИ БЕЗБЕДНОСТИ И ОДБРАНЕ (СЛ.Г.РС 93/2020)

Овом уредбом уређују се врсте поступака јавних набавки у области одбране и безбедности, услови и начин њиховог спровођења, као и комуникација у поступцима јавних набавки.

**члан 2.** – Значење израза

3. уговор о јавној набавци који садржи тајне податке је теретни уговор закључен у писаној форми између једног или више понуђача и једног или више наручилаца који за предмет има набавку добара, пружање услуга или извођење радова, а који садржи тајне податке или чије извршење захтева приступ тајним подацима;
4. **уговор са подизвођачем** је теретни уговор закључен у писаној форми између понуђача којем је додељен уговор о јавној набавци и једног или више привредних субјеката с циљем извршења дела тог уговора о јавној набавци који за предмет има набавку добара, пружање услуга или извођење радова;

Јавне набавке у области одбране и безбедности, у складу са Законом о јавним набавкама (у даљем тексту: Закон) су набавке:

1. војне опреме, укључујући и било који њен саставни део, компоненту или склоп;
2. безбедносно осетљиве опреме, укључујући и било који њен саставни део, компоненту или склоп;
3. добара, услуга или радова директно повезаних са опремом из тач. 1) и 2) овог става у току било којег периода или читавог њеног животног века;
4. услуга и радова искључиво за војне намене;
5. безбедносно осетљивих радова и безбедносно осетљивих услуга.

**члан 4.** - **Заштита тајних података током поступка јавне набавке**

Када наручилац током поступка јавне набавке намерава да привредним субјектима стави на располагање тајне податке, обавезан је да одреди захтеве које привредни субјекти морају да испуне у циљу заштите тајних података у складу са посебним прописима којима се уређује заштита тајности података.

У складу са ставом 1. овог члана дужан је да поступа и понуђач којем је додељен уговор о јавној набавци када при закључењу уговора са подизвођачем ставља на располагање тајне податке.

Ако би објављивање појединих података из одлуке о додели уговора о јавној набавци или оквирног споразума било противно одредбама Закона или на други начин било противно општем интересу, посебно интересима одбране или безбедности, ако би нанело штету оправданим пословним интересима одређеног привредног субјекта или би могло да доведе до повреде конкуренције на тржишту, ти подаци из одлуке неће се објавити.

**Члан 27.** - **Заштита тајних података током извршења уговора**

Ако наручилац намерава да закључи уговор о јавној набавци који садржи тајне податке, дужан је да у документацији о набавци одреди мере и захтеве неопходне да се обезбеди сигурност тих података

на захтеваном нивоу током извршења уговора у складу са посебним прописима којима се уређује заштита тајности података.

У циљу заштите тајних података из става 1. овог члана наручилац мора захтевати да понуда, између осталог, садржи:

1. обавезу понуђача и већ одређених подизвођача да ће у складу са посебним прописима којима се уређује заштита тајности података на одговарајући начин да штите поверљивост, поузданост и целовитост тајних података које поседују или које ће сазнати током трајања и након извршења, као и у случају раскида уговора који садржи тајне податке;
2. обавезу понуђача да ће од осталих подизвођача са којима ће закључити уговоре, током извршења уговора који садржи тајне податке, захтевати да на одговарајући начин штите поверљивост, поузданост и целовитост тајних података које поседују или које ће сазнати током трајања и након извршења, као и у случају раскида уговора који садржи тајне податке;
3. довољно информација о већ одређеним подизвођачима како би наручилац могао да утврди да сваки од њих поседује капацитет неопходан да на одговарајући начин заштити поверљивост, поузданост и целовитост тајних података који су му доступни или који ће настати током извршења уговора са подизвођачем;
4. обавезу понуђача да обезбеди информације из тачке 3) овог става за сваког новог подизвођача пре закључења уговора са подизвођачем.

Наручилац може да захтева да понуђач и већ одабрани подизвођачи поседују сертификат за приступ тајним подацима захтеваног нивоа заштите у складу са посебним прописима којима се уређује заштита тајности података.

Наручилац прихвата издати безбедносни сертификат које је привредном субјекту издала друга држава, под условом да је орган Републике Србије надлежан за националну безбедност и заштиту тајних података спровео поступак утврђивања еквивалентности издатог сертификата.

Ако је потребно наручилац може да затражи путем органа надлежног за националну безбедност и заштиту тајних података спровођење додатних поступака провере и у том случају дужан је да узме у обзир и резултате тих поступака.

Ако наручилац оцени да понуђач не испуњава мере и захтеве за заштиту тајних података из овог члана, дужан је да у одлуци о додели уговора наведе разлоге за своју одлуку, водећи рачуна при томе да у одлуци не износи информације које представљају тајни податак.

## УРЕДБА О ПОСЕБНИМ МЕРАМА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА КОЈЕ СЕ ОДНОСЕ НА УТВРЂИВАЊЕ ИСПУЊЕНОСТИ ОРГАНИЗАЦИОНИХ И ТЕХНИЧКИХ УСЛОВА ПО ОСНОВУ УГОВОРНОГ ОДНОСА (СЛ.Г.РС 63/2013)

Овом уредбом прописују се посебне мере заштите тајних података, које се односе на начин и поступак утврђивања испуњености организационих и техничких услова за чување тајних података достављених правном или физичком лицу по основу уговорног односа.

**Организациони услови** односе се нарочито на:

- организацију процеса рада,
- заштиту приступа тајним подацима,
- заштиту од неовлашћеног коришћења тајних података,
- одређивање одговорног лица задуженог за спровођење мера заштите, као и
- утврђивање поступка у случају ванредних и хитних околности.

**Технички услови** односе се нарочито на:

- физичко-техничку заштиту простора, односно просторија у којима се чувају тајни подаци,
- противпожарну заштиту,
- заштиту тајних података приликом преношења и достављања изван просторија у којој се чувају, транспорт тајних података,
- обезбеђивање и заштиту информационо-телекомуникационим средстава којима се врши преношење и достављање тајних података и спровођење прописаних мера крипто-заштите.

Испуњеност организационих и техничких услова правних или физичких лица за чување тајних података означених степеном тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” или „ПОВЕРЉИВО” утврђује овлашћено лице органа јавне власти пре закључења поверљивог уговора са правним или физичким лицем.

Пре закључења поверљивог уговора који садржи тајне податке означене степеном тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” или „ПОВЕРЉИВО”, правно или физичко лице које закључује поверљиви уговор, као прилог уговору, израђује упутство о мерама заштите тајних података.

### ОБАВЕЗЕ УГОВАРАЧА

Од уговарача се тражи да пријаве сваки губитак, компромитацију или сумњу на угрожавање тајних података и информација, који су добијени од органа јавне власти или страних тајних података, што проистиче директно из одредби Закона о тајности података.

Сваки орган јавне власти, када је у питању индустријска безбедност, може да обезбеди додатна упутства и смернице у вези са временским периодом извештавања и захтевају додатне информације или радњу, чија је сврха да се припреми реаговање и санирање безбедносних инцидената и пријављивање губитка, компромитовања или сумње на компромитовање тајних података.

## УСЛОВИ ЗА ПОДНОШЕЊЕ ЗАХТЕВА ЗА ИЗДАВАЊЕ СЕРТИФИКАТА

- Регистровано седиште на територији РС
- Да није у поступку ликвидације или стечаја
- Да није кажњено мером забране вршења делатности
- Уредно плаћа порезе и доприносе

## ОСНОВ ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА

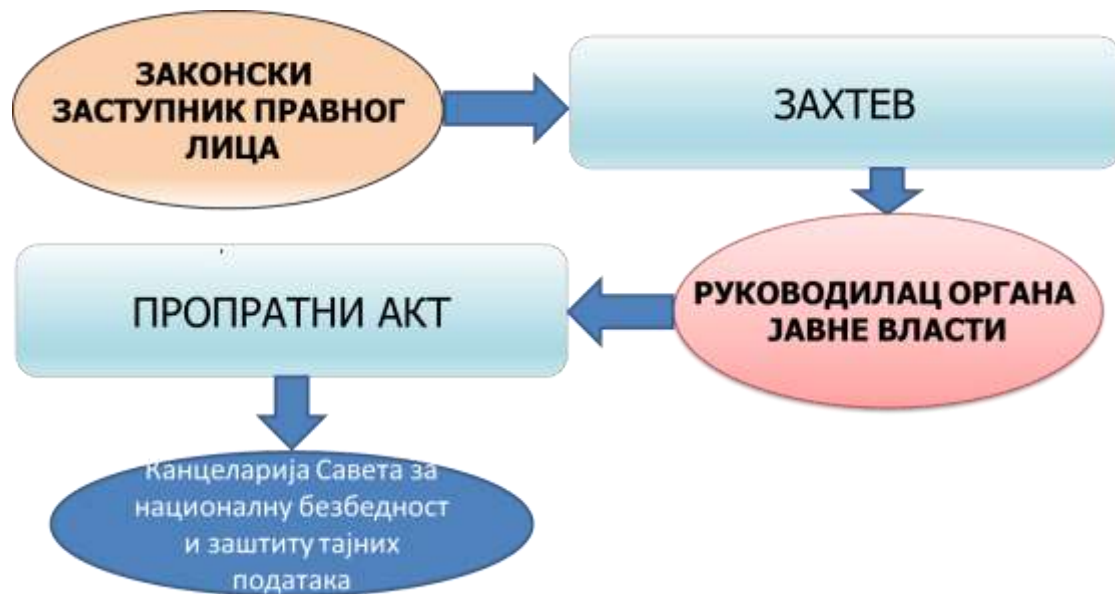
Основ за издавање сертификата за приступ тајним подацима за правно лице:

- На основу Закључка Владе Републике Србије, или
- Постојање тендера, односно планираног поверљивог уговорног односа између:

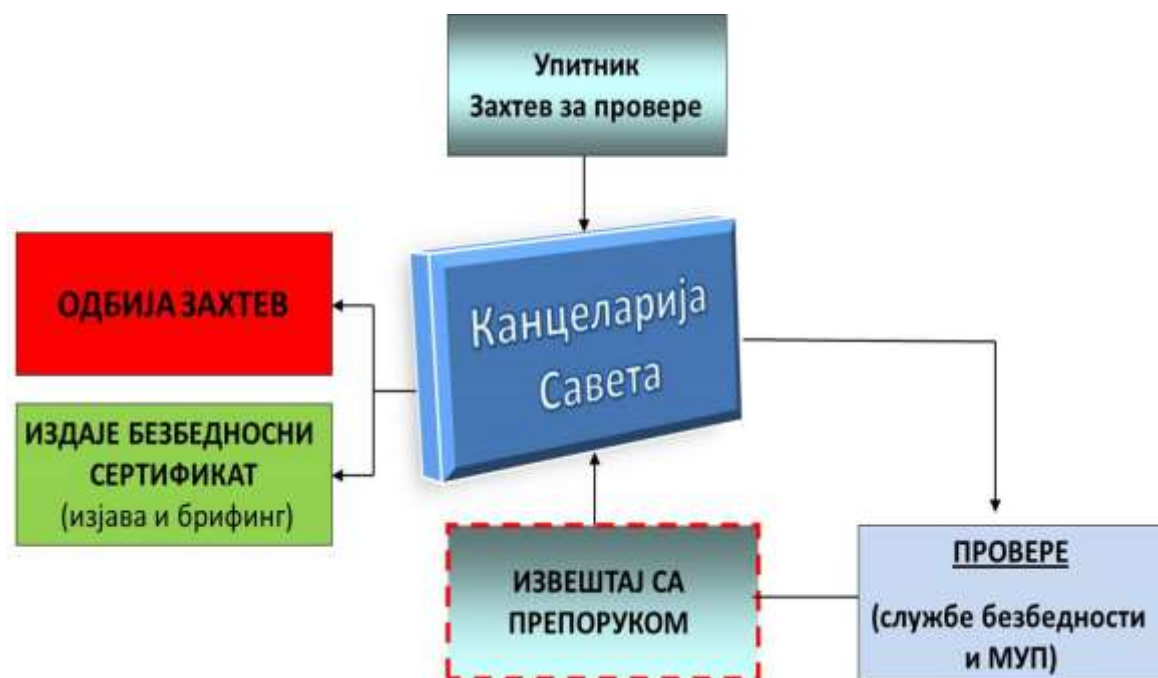




## ПОСТУПАК ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА



## ПОСТУПАК ИЗДАВАЊА СЕРТИФИКАТА



## БЕЗБЕДНОСНЕ ПРОВЕРЕ врше се по основу:

- ИНСТРУКЦИЈА за процену безбедносног ризика за приступ и коришћење тајних података за правна лица
- МЕТОДОЛОГИЈА процене безбедносног ризика код физичких лица за приступ тајним подацима
- За вршење безбедносних провера надлежни органи БИА и МУП

# КОНТРОЛА И НАДЗОР

## ПРОПИСИ

- Закон о тајности података
  - Уредба о посебним мерама надзора над поступањем са тајним подацима
  - Правилник о службеној легитимацији и начину рада лица овлашћених за вршење надзора над спровођењем закона
- **Унутрашња контрола** – руководилац органа јавне власти а у случају потребе систематизује се посебно радно место или се задужује посебна организациона јединица у саставу органа јавне власти
- **Контрола и стручни надзор** - КСНБ и ЗТП
- **Контрола и инспекцијски надзор** - Министарство надлежно за послове правосуђа

## ПОЈАМ БЕЗБЕДНОСНЕ КУЛТУРЕ И СВЕСТИ

### ШТА ЈЕ ТО БЕЗБЕДНОСНА КУЛТУРА И СВЕСТИ?

Безбедносна култура је безбедносна активност, која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима.

Огледа се у:

- препознавању опасности!
- реаговању на њих избегавањем опасности
- отклањању опасности
- упућивању на оне субјекте који ће професионално реаговати и сачувати угрожене вредности

## УЛОГА КАНЦЕЛАРИЈЕ САВЕТА

Организовање обуке корисника тајних података у складу са националним и међународним стандардима и прописима (укључујући и безбедносне брифинге приликом реализације сертификовања физичких и правних лица)

Анализа и праћење учинка обуке и активности подршке у имплементацији закона о тајности података и делотворности спровођења мера заштите тајних података у Р. Србији

## ПРАВНИ ОКВИР УНУТРАШЊЕ КОНТРОЛЕ:

- Члан 84 и 85. **Закон о тајности података**, „Службени гласник РС“, број 104 од 16. децембра 2009.
- **Уредба о посебним мерама надзора над поступањем са тајним подацима**, „Службени гласник РС“, број 90 од 30. новембра 2011.

## ЗАКОН О ТАЈНОСТИ ПОДАТАКА

- **члан 99.** - Новчаном казном у износу од 5.000 до 50.000 динара казниће се за прекршај **одговорно лице у органу јавне власти** ако:

- 16) не организује унутрашњу контролу над заштитом тајних података (члан 84. став 1);

За унутрашњу контролу над спровођењем овог закона и прописа донетог на основу овог закона одговоран је руководиоца органа јавне власти.

**У министарству надлежном за унутрашње послове, министарству надлежном за послове одбране и Безбедносно-информативној агенцији, а по потреби и у другим органима јавне власти, за унутрашњу контролу и друге стручне послове у вези са одређивањем и заштитом тајних података систематизује се посебно радно место, или се за обављање ових задатака и послова посебно задужује постојећа организациона јединица у саставу министарства или агенције.**

## ОБАВЕЗА ИЗ ПРОПИСА О ЗАШТИТИ ТАЈНИХ ПОДАТАКА:

### Уредба о посебним мерама надзора над поступањем са тајним подацима

Канцеларија Савета за националну безбедност и заштиту тајних података врши обуку лица овлашћених за послове унутрашње контроле.

Обуке, едукације и тренинзи се спроводе у оквиру:

- Самог органа јавне власти
- Канцеларије Савета за националну безбедност и заштиту тајних података
- Националне академије за јавну управу
- Високошколских установа кроз струковне специјалистичке студије, мастер студије и слично

**ПОСЕБНО МЕСТО: - самоедукација свих запослених у органима јавне власти.**

## ПИТАЊА ПО КОЈИМА СЕ ВРШИ УНУТРАШЊА КОНТРОЛА:

Персонал за руковање тајним подацима,

Инфраструктура за смештај и чување тајних података,

Технички системи за заштиту и обраду тајних података,

Регулатива/норматива за заштиту тајних података,

Уступање тајних података приликом уговорног односа са физичким и правним лицима.

Ако у току вршења унутрашње контроле контролор открије незаконитост, односно неправилности у раду субјекта контроле, која је изван границе дате налогом, дужан је да о томе одмах обавести непосредног руководиоца, који ће му дати упутство о начину даљег поступања, о чему контролор сачињава службену забелешку у записнику о вршењу унутрашње контроле.

Приликом вршења унутрашње контроле контролор из приложених предмета надзора, као и других докумената, у границама датог налога, може да проверава:

1. законитост поступања у предметима који садрже аналитичке материјале са ознаком тајности, управним и другим предметима, као и радњама у којима се обрађују и штите тајни подаци;
2. поштовање прописаних упутстава, односно процедура;
3. поштовање одредби из информационе безбедности, криптозаштите и канцеларијског пословања;
4. остале послове радног места и утврђених радних циљева;
5. савесно извршавање дужности из радног односа;

6. однос према странкама, непосредном руководиоцу, као и према другим лицима запосленим у организационој јединици, као и поступање сагласно етичком кодексу понашања државних службеника.

Унутрашњом контролом проверава се спровођење мера заштите тајних података, а нарочито у односу на:

- 1) одређивање степена тајности податка;
- 2) означавање докумената и омота докумената;
- 3) посебну просторију за пријем тајних података;
- 4) евидентирање, чување и депоновање тајних података;
- 5) означавање ормара и каса у којима се чувају и депонују тајни подаци;
- 6) начин коришћења и приступа тајном податку, вођење евиденције корисника и евиденције о приступу тајном податку, као и чување тих евиденција;
- 7) начин вршења умножавања, превођења и израде извода из тајних података;
- 8) паковање и достављање тајних података унутар и ван безбедносне зоне;
- 9) поступак уништавања тајних података;
- 10) евиденцију улаза и излаза лица и возила, коришћење безбедносних пропусница и посебних безбедносних пропусница, функционисање физичког и електронског система за обезбеђење објекта и простора;
- 11) поседовање, евиденцију и чување сертификата за приступ тајним подацима;
- 12) пријем, обраду, пренос, чување, архивирање и уништавање тајних података у електронској форми;
- 13) чување крипто кључева;
- 14) чување уговора који садрже тајне податке;
- 15) начин заштите тајних података страних правних и физичких лица.

### **О вршењу унутрашње контроле овлашћено лице сачињава записник.**

Унутрашња контрола (контролор) сачињава записник, који садржи:

- 1) назив организационе јединице;
- 2) број и датум налога;
- 3) навођење радњи које су предузете, њиховом току и садржини;
- 4) место, дан и час када се радња предузимала;
- 5) назнаку о предмету вршења унутрашње контроле;
- 6) личноме имену контролора, субјекта контроле и других присутних лица;
- 7) навођење исправа које су коришћене;
- 8) чињенично стање утврђено у контроли;
- 9) податке о затеченим лицима, који потписују записник о извршеној унутрашњој контроли;
- 10) изјаве субјекта контроле;
- 11) изјаве других лица;
- 12) време завршетка вршења унутрашње контроле;
- 13) потпис контролора и лица која су учествовала у предузимању радњи и лица од којих је узета изјава и др.

Овлашћено лице, најкасније у року од три дана од дана извршене унутрашње контроле, подноси руководиоцу органа извештај о извршеној унутрашњој контроли. Уз извештај се доставља и записник из члана 6. ове уредбе.

Ако је унутрашњом контролом утврђено постојање неправилности, у извештају из става 1. овог члана могу се предложити мере за њихово отклањање.

У зависности од садржине налога, утврђеног чињеничног стања констатованог записником, контролор, у налазу/мишљењу, за сваки од елемената провере у вези заштите тајних података и за све

елементе укупно, износи свој суд о контролисаном вршењу унутрашњег надзора и резултатима рада организационе јединице у органу јавне власти који је био субјект контроле, које изражава описно и исказује као:

1. нарочито високо;
2. високо;
3. задовољавајуће;
4. ниско;
5. незадовољавајуће.

У случају давања „ниског” или „незадовољавајућег” суда контролор је у обавези да предложи једну или више мера, односно:

1. додатну обуку субјекта контроле, са предлогом начина обуке у области заштите тајних података;
2. континуирану едукацију у одређеним областима надзора;
3. препоручи непосредном руководиоцу да, у одређеном временском периоду ангажује субјекта контроле на мање сложеним пословима у органу јавне власти.

Ако приликом вршења унутрашње контроле, контролор уочи такве незаконитости, односно неправилности, које чине повреду радне дужности, прекршај или кривично дело, дужан је да о томе, без одлагања, ради даљег поступања, обавести надлежног руководиоца.

Неправилности по природи се разврставају на основу разлога појављивања, односно да ли се јављају због недостатака у система заштите тајних података или због недоследне примене контролних активности у оквиру унутрашње контроле.

На основу наведеног, неправилности по природи можемо разврстати на:

- Системске
- Једнократне
- Грешке

#### Системска неправилност

- одступања у процесу примене правила код примене општих и посебних мера заштите тајних података које се периодично понављају или имају велику вероватноћу да ће се поновити у систему као такве, током времена и кроз различите послове у раду са тајним подацима.
- Оне настају због недостатака у дизајну система рада са тајним подацима и могу се појавити хоризонтално кроз све пословне процесе.
- Генерално, ово су најчешће ненамерне неправилности које су резултат недостатка у систему (недефинисане или недовољно дефинисане процедуре и активности у систему, непостојање праћења рада са тајним подацима и сл.).

#### Једнократна неправилност

- То су неправилности које се јављају само једном, код једнократних пројеката са тајним подацима у дужем временском периоду (нпр. једном у четири године) или први пут и не могу се у потпуности подвести под постојећа правила и процедуре система општих и посебних мера заштите тајних података у органу јавне власти.
- Оне настају због радњи у оквиру одређеног пројекта и не јављају током осталих пројеката, ако се правилно поштују процедуре заштите тајних података и контроле.
- Генерално, ради се о неправилностима које најчешће настају због недовољне посвећености и недостатака одговарајућих квалификација појединаца (проблем едукација) који спровode

поједине активности, а проузроковане су одређеним специфичностима унутар пројекта са тајним подацима.

## Грешке

- преставаља недовољну или супротну радњу од онога што је прописано за извођење одређене активности у раду са тајним подацима и може бити намерна или ненамерна.
- У суштини представља недоследно извођење одређених активности у раду са тајним подацима за које је појединац задужен и најчешће настају због непажње или због недовољне обучености запослених.
- Ако је грешка откривена у току стандардног спровођења других контролних активности у пословном процесу и исправљена пре и без последица по резултат пословног процеса не евидентира се као неправилност, али мора бити забележена у пратећој документацији којом се документује процес (мора постојати документовани траг о учињеној грешци, особи која је начинила грешку, начину и особи која је грешку исправила)

**АКО ЗАКОНОНСКИ НИЈЕ ПОСЕБНО ДЕФИНИСАНО, РАД У СПЕЦИФИЧНИМ ОРГАНИЗАЦИЈАМА ИЛИ РАД СА ТАЈНИМ ПОДАЦИМА, КАО И ПРАВО ПРИСТУПА ТАЈНИМ ПОДАЦИМА У СМИСЛУ ЧИЊЕНИЦА, НЕ ПРЕДСТАВЉАЈУ ТАЈНИ ПОДАТАК**

Без обзира на наведено, лица која су обухваћена наведеним опсегом **МОРАЈУ ИМАТИ СВЕСТ** да припадност специфичној организацији, рад са осетљивим подацима и на специфичним пословима теоретски могу бити предуслов да таква лица постану **мете субјеката угрожавања тајних података**

## НЕКЕ ОД ОПШТИХ МЕРА ОПРЕЗА ПРИ ТРАНСФЕРУ ИНФОРМАЦИЈА

- **#1 ПРЕВЕНТИВНО ДЕЛОВАЊЕ У СКЛАДУ СА ОПШТИМ МЕРАМА ЗАШТИТЕ ТП!!!**
- **ПАЖЊА ПРИ УСМЕНОЈ И ПИСАНОЈ КОМУНИКАЦИЈИ (ПОСЛОВНА И ПРИВАТНА)**
- **ПАЖЉИВО КОРИШЋЕЊЕ ИНТЕРНЕТ СЕРВИСА ЗА ЗВУКОВНУ И ВИДЕО КОМУНИКАЦИЈУ („VOIP“ И СЛ. ТЕХНОЛОГИЈЕ) КАО И ТЕЛЕФОНА**
- **ПАЖЊА ПРИ ОДАБИРУ ПРОСТОРА ЗА ОСЕТЉИВЕ РАЗГОВОРЕ**
- **ПРОЦЕНА САГОВОРНИКА (ДРУГЕ СТРАНЕ У КОМУНИКАЦИЈИ)**
- **НЕПАЖЊА ПРИЛИКОМ РАЗГОВОРА (КОМУНИКАЦИЈЕ) СА ВЕШТИМ МАЛИЦИОЗНИМ САГОВОРНИКОМ**

## ПРЕВЕНТИВНЕ И „AD NOS“ МЕРЕ ЗАШТИТЕ ТП

**ЧИНИОЦИ СИСТЕМА ЗАШТИТЕ И ПОШТОВАЊЕ ПРОЦЕДУРА У ВЕЗИ ОПШТИХ И ПОСЕБНИХ МЕРА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА ЧИНЕ ОСНОВУ ПРЕВЕНТИВНОГ ПОСТУПАЊА!**

РЕДОВНА ЕДУКАЦИЈА НА ТЕМУ БЕЗБЕДНОСНЕ КУЛТУРЕ И СВЕСТИ

ПРЕВЕНТИВНЕ МЕРЕ ВРШЕНЕ ОД СТРАНЕ НАДЛЕЖНИХ ОРГАНА И ТЕЛА У ОБЛАСТИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА И БЕЗБЕДНОСНИХ ОРГАНА Р. СРБИЈЕ

## ОБУКЕ

- Надлежни органи који спроводе обуке: КСНБиЗТП, БИА, Министарство одбране, МУП
- КСНБиЗТП изводи следеће обуке:
  1. Оријентационе обуке:
    - Обуке у просторијама Канцеларије Савета (редовне- сваког другог четвртка у просторијама Канцеларије Савета одржавју се обуке за ЈЛС )
    - Обуке у Органима јавне власти (по позиву)
  2. Обуке у Националној академији за јавну управу (организација у подручним јединицама)
  3. Обуке на Факултету безбедности (специјалистичке студије)

### Уместо закључка

Уређење области рада са тајним подацима није само себи циљ и проблем већ је везано за реформске процесе комплет не државне управе, а посебно сектора националне безбедности који још увек није дефинисан у целости, нити је до краја креирана национална безбедносна политика. Имајући у виду изнето, можемо закључити да је уређење система заштите тајних података процес који траје, а упоредна искуства држава, које су прошле овакве процесе, говоре о периоду од 10 година или више.

Суштински, сама реформа области заштите тајних података подразумева:

- 1) реформу националног система безбедности;
- 2) уставне и законске измене, кроз хармонизацију прописа са прописима и стандардима Европске уније у овој области;
- 3) едукацију и обуку кадрова који непосредно учествују у креирању и заштити тајних података;
- 4) евалуацију од стране међународних институција кроз успостављање проце са билатералне сарадње, али и оне у вези са Европском унијом, НАТО и слично;
- 5) превођење практичних позитивних и негативних искустава у одговарајућу законску и подзаконску регулативу.

Закон о тајности података и поред примене у области рада са страним тајним подацима (ЕУ, НАТО; ЕУРОПОЛ итд), не примењује се још увек у целости у свим државним органима. Сама структура закона је изузетно сложена и рађена по узору на модел Чешке Републике, због чега се мора прећи на измене и допуне овог текста.

**ЧОВЕК ЈЕ УВЕК НАЈСЛАБИЈА КАРИКА СВАКОГ СИСТЕМА**