Проф.др Горан Д. Матић

2025

ПЕРСОНАЛНА БЕЗБЕДНОСТ

ПОСТУПАК ИЗДАВАЊА БЕЗБЕДНОСНОГ СЕРТИФИКАТА - СКРИПТА

САДРЖАЈ

ТЕМЕ

- Уводна разматрања
- О управном поступку
- Процес издавања сертификата
- Безбедносне провере
- Орган јавне власти
- Сертификати
- Индустријска безбедност
- Службене евиденције
- Кривична и прекршајна одговорност
- Закључна разматрања

НАПОМЕНА

СКРИПТА ПРЕДСТАВЉА ЛИЧНО, СТРУЧНО И НАУЧНО ВИЂЕЊЕ ПРОБЛЕМАТИКЕ ОД СТРАНЕ АУТОРА….

ОВА СКРИПТА ЈЕ РАЂЕНА НА ОСНОВУ АНАЛИЗЕ ЈАВНИХ ИЗВОРА ПОДАТАКА….

- ПРОПИСА
- ПРАКСЕ
- НАУЧНИХ И СТРУЧНИХ ТЕКСТОВА
- МЕДИЈА
- ИСКУСТВА У РАДУ СА ПОДАЦИМА

СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

УВОДНА РАЗМАТРАЊА

ТЕОРИЈА:
СВЕ ЗНАМО АЛИ НИШТА НЕ ФУНКЦИОНИШЕ

ПРАКСА:
СТВАРИ ФУНКЦИОНИШУ, АЛИ НЕ ЗНАМО ЗАШТО

АСПЕКТИ РАЗМАТРАЊА ПРОБЛЕМА

- ТЕХНОЛОШКИ
- ПРАВНИ
- ПОЛИТИЧКИ

ПРИЗМА ПОСМАТРАЊА

- РЕФОРМА ДРЖАВНЕ УПРАВЕ
- РЕФОРМА СЕКТОРА БЕЗБЕДНОСТИ
- У СУСРЕТ ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА...

Безбедносна култура - 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, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности.

Организациона култура рада са тајним подацима се бави „појединачним и групним вредностима, ставовима, менаџерским праксама, перцепцијом,компетенцијом и обрасцима активности" и стога утиче на сваки аспект организације, зато безбедносна култура спада под „персоналну безбедност" у оквиру отпорности на угрожавање безбедности.

То је методологија рада који се често назива „начин на који се ствари овде раде" или „ДНК" организације.

СУПРОТСТАВЉЕНИ КОНЦЕПТИ

БЕЗБЕДНОСТ	-	ЉУДСКА ПРАВА
ПРИВАТНОСТ	-	БЕЗБЕДНОСНА ПРОВЕРА?
ПРАВО ДА СЕ БУДЕ ОСТАВЉЕН НА МИРУ	-	ПЕРСОНАЛНА БЕЗБЕДНОСТ
ТРАНСПАРЕНТНОСТ	-	ТАЈНОСТ

Које су границе до којих се може ићи у успостављању система заштите?

АСПЕКТИ ЗАШТИТЕ ПОДАТАКА

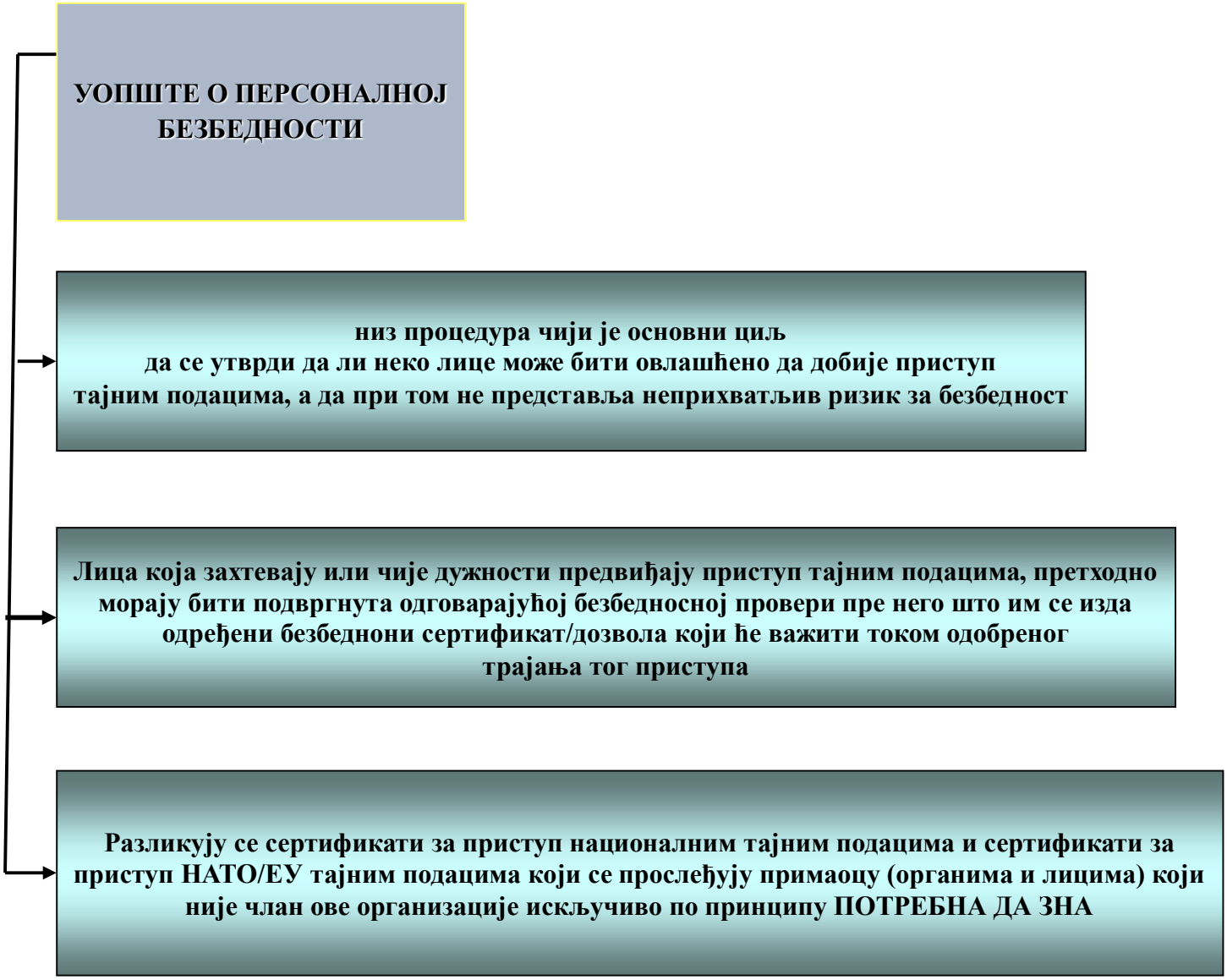
- Регистарски систем
- **Персонална безбедност**
- Административна безбедност
- Физичка и техничка безбедност
- Информатичка безбедност
- Индустријска безбедност (поверљиве набавке везане за државу)

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

ПЕРСОНАЛНА БЕЗБЕДНОСТ

Дисциплина процене понашања, интегритета, расуђивања, лојалности, поузданости и стабилности појединаца за дужности и одговорности које захтевају поверење.



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

- Која су „прошла“ безбедносну проверу
- Која су упозната са прописаним политикама и процедурама заштите ТП - „брифинг“
- Која поседују безбедносни сертификат
- Која се налазе на листи „Потребно да зна“

ПРОПИСИ

- Закон о тајности података
- Закон о општем управном поступку
- 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
- Правилник о безбедносним проверама лица које обавља Војнобезбедносна агенција («СЛ. Војни гласник» 25/2015)
- Јединствена методологија за процену безбедносног ризика код физичких лица
- Инструкција за процену безбедносног ризика за приступ и коришћење тајних података за правна лица

О УПРАВНОМ ПОСТУПКУ КОЈИ СЕ ПРИМЕЊУЈЕ ЗА ИЗДАВАЊЕ БЕЗБЕДНОСНОГ СЕРТИФИКАТА

НА ПОСТУПАК ИЗДАВАЊА БЕЗБЕДНОСНИХ СЕРТИФИКАТА СХОДНО СЕ ПРИМЕЊУЈЕ ЗАКОН О ОПШТЕМ УПРАВНОМ ПОСТУПКУ

ЗАКОН О ОПШТЕМ УПРАВНОМ ПОСТУПКУ («СЛ. ГЛАСНИК РЕПУБЛИКЕ СРБИЈЕ» број 18/2016; 95/2018 – аутентично тумачење и 2/2023 – Уставни суд)

Управни поступак је поступак доношења управних аката.

Под управним поступком подразумевају се процедурална правна правила која се примењују у вези са доношењем одлука у управним стварима.

Првостепени управни поступак састоји се из 5 фаза:

1. фаза покретања управног поступка
2. фаза управног поступка до доношења решења (испитни и доказни поступак)
3. фаза доношења решења
4. фаза по жалби (евентуална фаза)
5. фаза административног (принудног) извршења (евентуална фаза)

ЖАЛБА СЕ ПОДНОСИ МИНИСТАРСТВУ ПРАВДЕ, ПРЕКО КАНЦЕЛАРИЈЕ САВЕТА

МОГУЋНОСТ ВОЂЕЊА УПРАВНОГ СПОРА ПРЕД УПРАВНИМ СУДОМ У БЕОГРАДУ

РЕШЕЊЕ

- ФОРМА РЕШЕЊА У СКЛАДУ СА ЗУП-ом
- УТВРЂИВАЊЕ ПРАВА НА ПРИСТУП ТАЈНИМ ПОДАЦИМА И ИЗДАВАЊУ СЕРТИФИКАТА
- ПОУКА О ПРАВНОМ ЛЕКУ (ЖАЛБА)
- ДОСТАВЉА СЕ И РУКОВОДИОЦУ И ЛИЦУ

Канцеларија савета – 1. Степени орган,

По жалби (2. Степени орган) решава министарство правде

У писаном облику садржи:

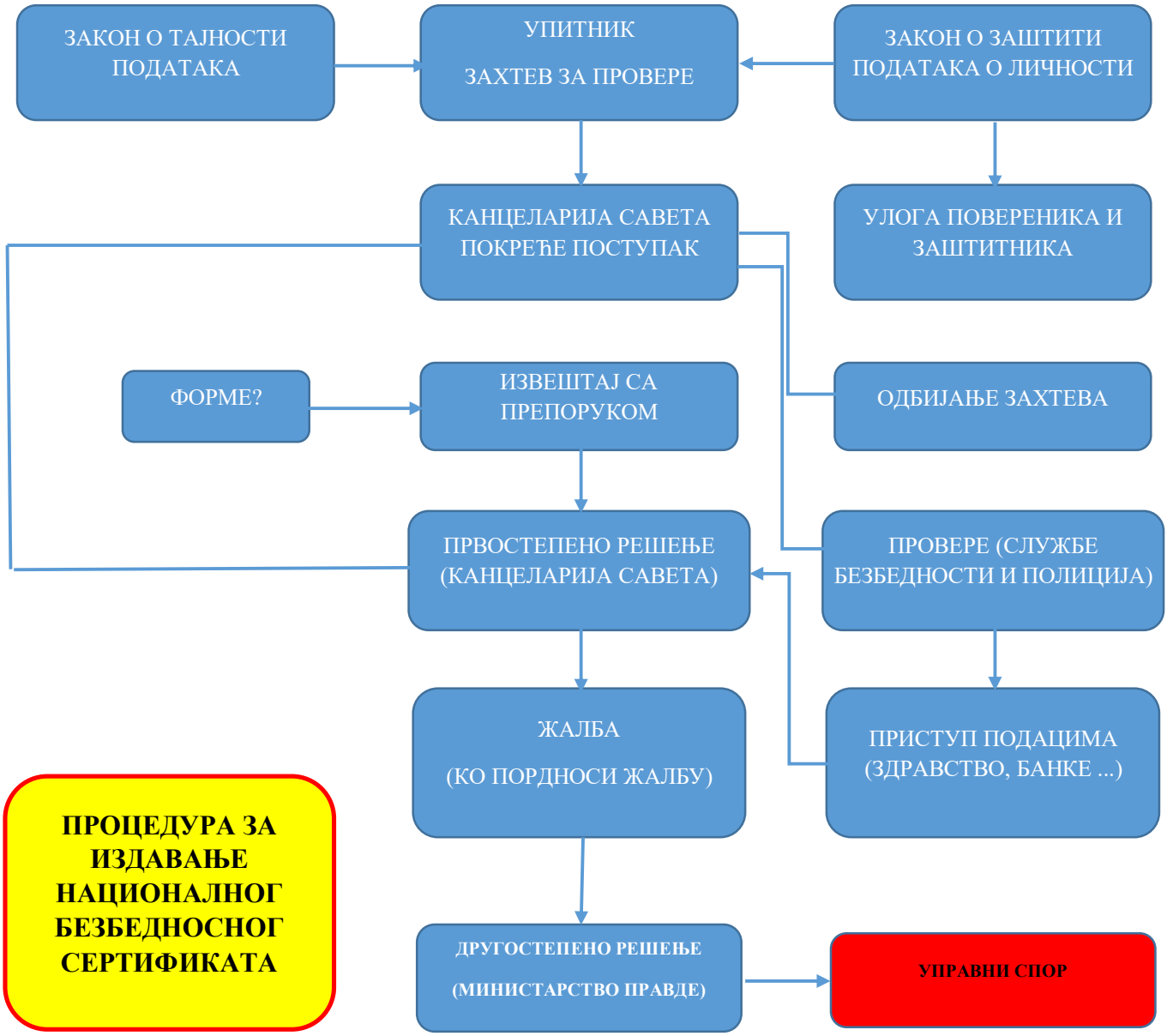
- увод,
- диспозитив (изреку),
- образложење,
- упутство о правном средству,
- потпис овлашћеног службеног лица и печат органа или други вид потврде о аутентичности (члан 141 ЗУП).

Други вид потврде аутентичности односи се првенствено на електронски документ.

Канцеларија Савета о издавању сертификата одлучује решењем, у року од 15 дана од дана достављања извештаја са препоруком из члана 65. став 1. ЗТП, односно од истека рока за извршење безбедносне провере из члана 63. ЗТП.

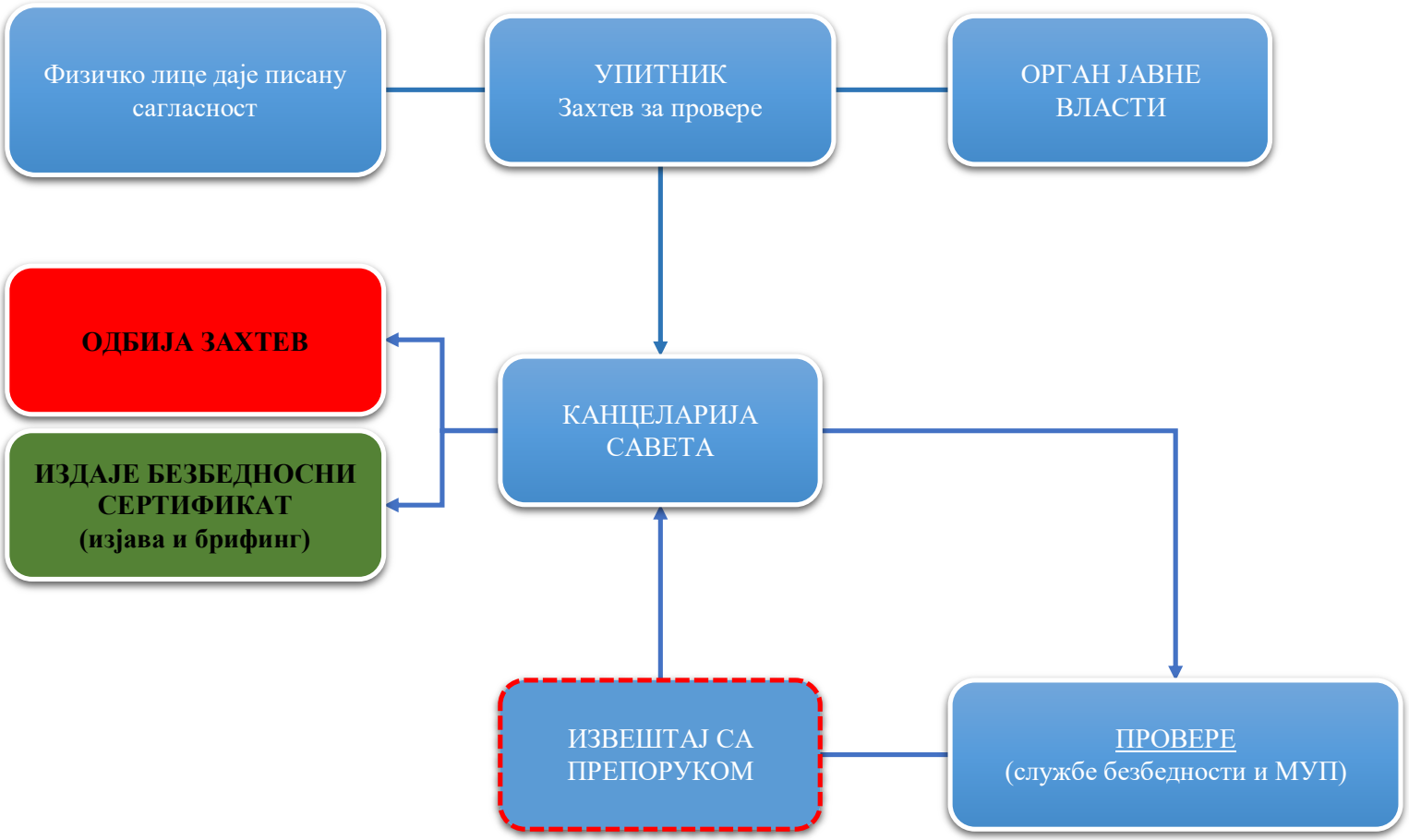
Ако је извештај непотпун или је достављен без препоруке, Канцеларија Савета доноси решење на основу података из достављеног извештаја.

Изузетно, ако се из извештаја о резултатима безбедносне провере и препоруке за издавање сертификата не може утврдити да ли су испуњени законом прописани услови за издавање сертификата физичком или правном лицу, Канцеларија Савета покреће допунску проверу (чл. 66. ст. 3 ЗТП)

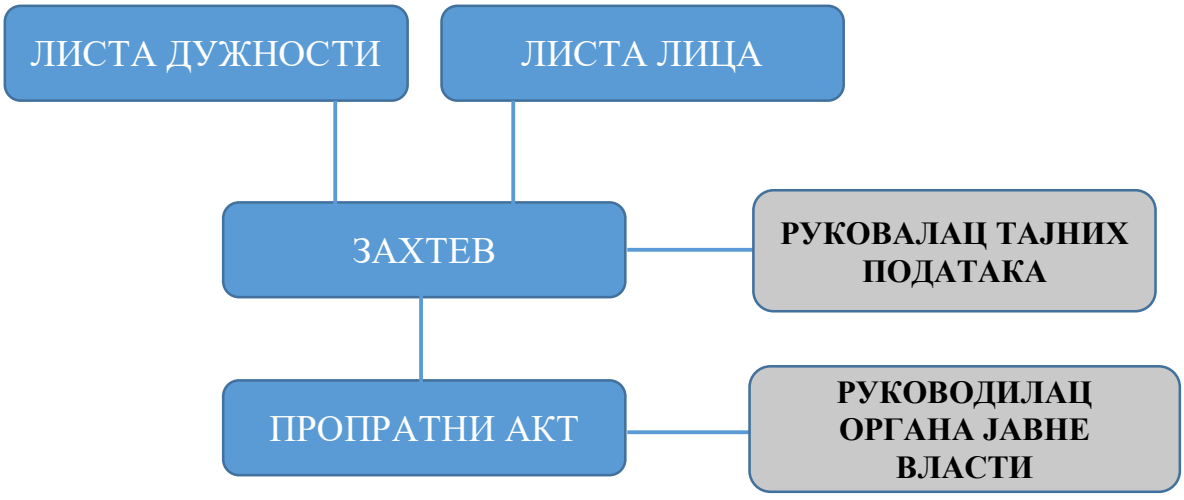

ЗАКОН О ТАЈНОСТИ ПОДАТАКА
УПИТНИК
ЗАХТЕВ ЗА ПРОВЕРЕ
ЗАКОН О ЗАШТИТИ ПОДАТАКА О ЛИЧНОСТИ
КАНЦЕЛАРИЈА САВЕТА ПОКРЕЋЕ ПОСТУПАК
УЛОГА ПОВЕРЕНИКА И ЗАШТИТНИКА
ФОРМЕ?
ИЗВЕШТАЈ СА ПРЕПОРУКОМ
ОДБИЈАЊЕ ЗАХТЕВА
ПРВОСТЕПЕНО РЕШЕЊЕ (КАНЦЕЛАРИЈА САВЕТА)
ПРОВЕРЕ (СЛУЖБЕ БЕЗБЕДНОСТИ И ПОЛИЦИЈА)
ЖАЛБА
(КО ПОРДНОСИ ЖАЛБУ)
ПРИСТУП ПОДАЦИМА (ЗДРАВСТВО, БАНКЕ ...)
ПРОЦЕДУРА ЗА ИЗДАВАЊЕ НАЦИОНАЛНОГ БЕЗБЕДНОСНОГ СЕРТИФИКАТА
ДРУГОСТЕПЕНО РЕШЕЊЕ
(МИНИСТАРСТВО ПРАВДЕ)
УПРАВНИ СПОР

ПРОЦЕС ИЗДАВАЊА БЕЗБЕДНОСНОГ СЕРТИФИКАТА

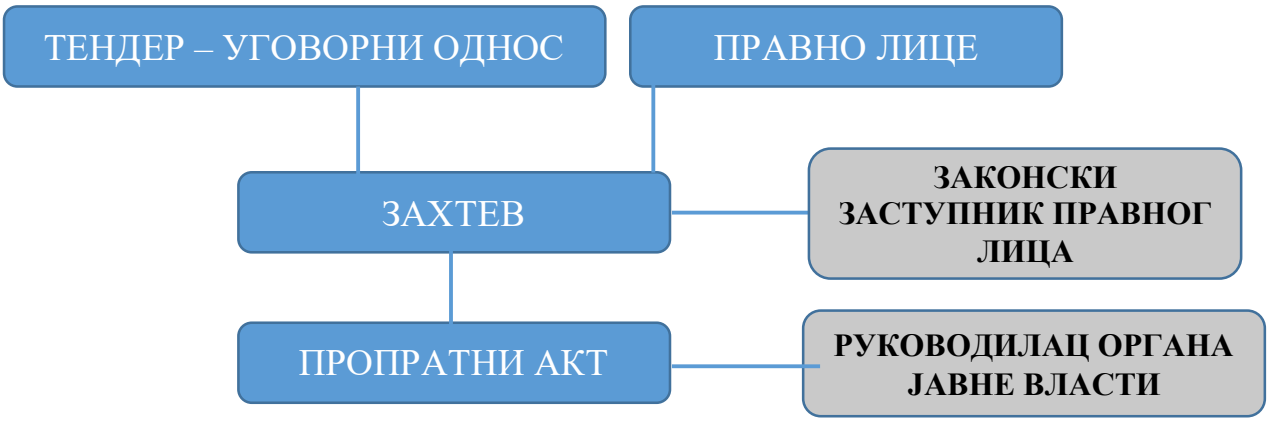
ПРОЦЕС ИЗДАВАЊА СЕРТИФИКАТА



ПОДНОШЕЊЕ ЗАХТЕВА ЗА ФИЗИЧКА ЛИЦА



ПОДНОШЕЊЕ ЗАХТЕВА ЗА ПРАВНА ЛИЦА



ИЗДАВАЊЕ СЕРТИФИКАТА ФИЗИЧКОМ И ПРАВНОМ ЛИЦУ

1. Захтев за издавање сертификата,
2. Безбедносни упитник за физичко лице обрасци:
   - ОБУ-1 (основни безбедносни упитник) подаци из члана 58. Закона о тајности података и
   - ПБУ-1 (посебан безбедносни упитник) подаци из члана 60. Закона о тајности података (за степен СТРОГО ПОВЕРЉИВО и ДРЖАВНА ТАЈНА).
3. Безбедносни упитник за правно лице обрасци:
   - ОБУ-2 и ОБУ-2_01 (основни безбедносни упитници) подаци из члана 59. Закона о тајности података и
   - ПБУ-2 (посебан безбедносни упитник) подаци из члана 60. Закона о тајности података (за степен СТРОГО ПОВЕРЉИВО и ДРЖАВНА ТАЈНА).

ЗАХТЕВ ЗА ИЗДАВАЊЕ СЕРТИФИКАТА

Попуњени и потписани упитник подносиоца захтева истовремено представља писану сагласност за вршење безбедносне провере,

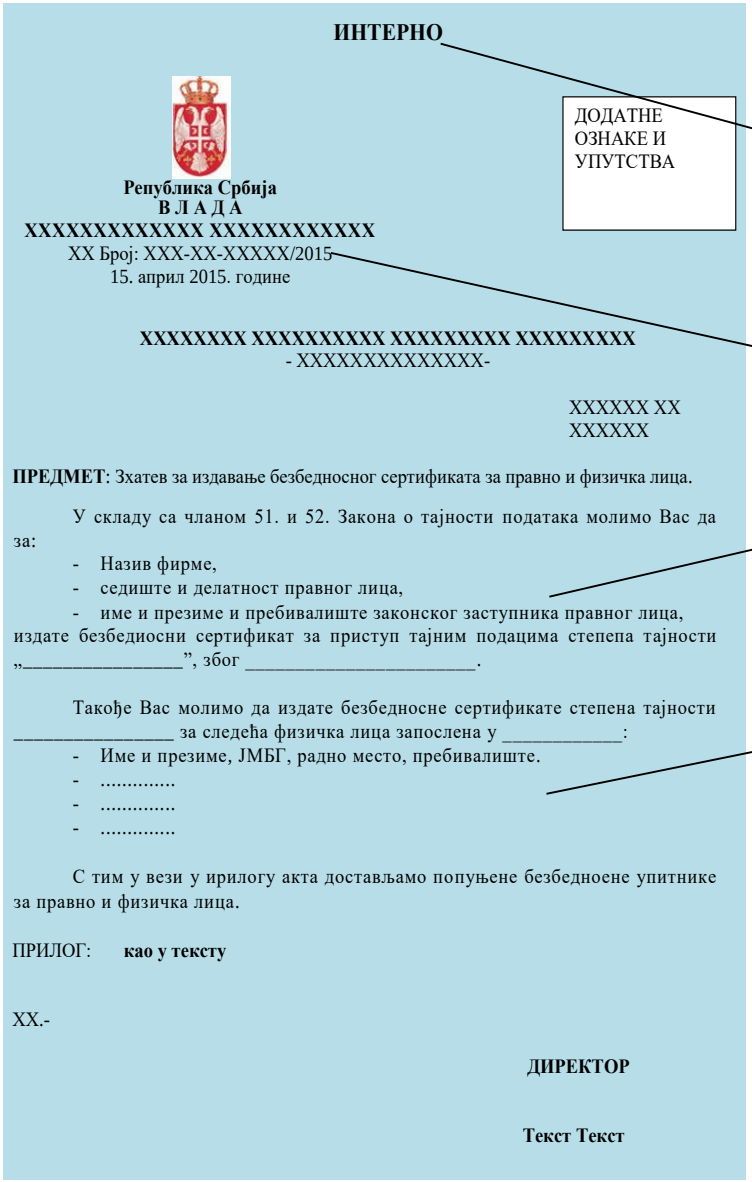
Дајем писмену сагласност да се приликом вршења **безбедносне провере** прикупљају и обрађују подаци наведени у безбедносном упитнику у складу са прописима о заштити података о личности.

Место _____

Датум _____

ПОТПИС ПОДНОСИОЦА ЗАХТЕВА

_____



ИНТЕРНО

ДОДАТНЕ ОЗНАКЕ И УПУТСТВА

Република Србија
В Л А Д А
XXXXXXXXXXXXX XXXXXXXXXXXXX
XX Број: XXX-XX-XXXXX/2015
15. април 2015. године

XXXXXXXX XXXXXXXXXX XXXXXXXXX XXXXXXXXX
- XXXXXXXXXXXXXX-

XXXXXX XX
XXXXXX

ПРЕДМЕТ: Захтев за издавање безбедносног сертификата за правно и физичка лица.

У складу са чланом 51. и 52. Закона о тајности података молимо Вас да за:

- Назив фирме,
- седиште и делатност правног лица,
- име и презиме и пребивалиште законског заступника правног лица,

издате безбедиосни сертификат за приступ тајним подацима степена тајности „_____”, због _____.

Такође Вас молимо да издате безбедносне сертификате степена тајности _____ за следећа физичка лица запослена у _____:

- Име и презиме, ЈМБГ, радно место, пребивалиште.
- .....
- .....
- .....

С тим у вези у ирилогу акта достављамо попуњене безбедноене упитнике за правно и физичка лица.

ПРИЛОГ: **као у тексту**

XX.-

ДИРЕКТОР

Текст Текст

Ознака степена тајности. На врху сваке странице на средини. Тамнијим словима и већим фонтом од слова текста документа
Члан 57. Став 3. Закона о тајности података

Подаци о органу јавне власти

Члан 52. Став 2. Закона о тајности података

Члан 52. Став 1. Закона о тајности података

БЕЗБЕДНОСНИ УПИТНИК ЗА ФИЗИЧКО И ПРАВНО ЛИЦЕ

ПРОПИСИ:

- Закон о тајности података – чл. 57, 58, 59, 60 и 61.
- Уредба о обрасцима безбедносих упитника „Службени гласник РС“, број 30 од 7. маја 2010.
- Јединствена методологија за процену безбедносног ризика код физичких лица
- УПУТСТВО ЗА ПОПУЊАВАЊЕ БЕЗБЕДНОСНИХ УПИТНИКА (nsa.gov.rs)

БЕЗБЕДНОСНИ УПИТНИК ЗА ПРАВНО ЛИЦЕ

Основни безбедносни упитник за правна лица	Образац:	ОБУ-2
	ознака степена тајности:	ИНТЕРНО

Канцеларија Савета за националну безбедност и заштиту тајних података

(Правно лице)

МБ

ПИБ

(Место и адреса)

E-mail: _____

Напомена: **Подаци из овог упитника могу се користити искључиво у сврху безбедносног проверавања правних лица за приступ тајним подацима.**

Основни безбедносни упитник за правна лица	Образац:	ОБУ-2
	ознака степена тајности:	ИНТЕРНО

Име и презиме запосленог за кога се тражи издавање сертификата	ЈМБГ	Степен тајности података за које се тражи сертификат

УПОЗОРЕЊЕ: *Чланом 69. став 1. тачка 1) Закона о тајности података, прописано је да Канцеларија Савета за националну безбедност и заштиту тајних података, решењем одбија захтев за издавање сертификата, ако се на основу извештаја безбедносне, односно допунске безбедносне провере утврди да је подносилац захтева навео неистините и непотпуне податке у основном, односно посебном безбедносном упитнику.*

Дајем писмену сагласност да се приликом вршења **безбедносне провере** прикупљају и обрађују подаци наведени у безбедносном упитнику у складу са прописима о заштити података о личности.

Место _____

Датум _____

ПОТПИС ПОДНОСИОЦА ЗАХТЕВА

_____

Основни безбедносни упитник за правна лица	Образац:	ОБУ-2 01
	ознака степена тајности:	ИНТЕРНО

ПОДАЦИ О ПОДНОСИОЦУ ЗАХТЕВА

1. НАЗИВ ФИРМЕ и седиште, као и претходни називи и седишта				
2. МБ				
3. ПИБ				
4. Име и презиме заступника				
5. Датум и место оснивања				
6. Подаци о организационим јединицама, огранцима, зависним друштвима и другим облицима повезивања				
7. Порекло оснивачког капитала укључујући и промене у последње три године				
8. Подаци о запосленима	Укупан број запослених	Подаци о запосленима за које се тражи сертификат		
		Број запослених	Врста послова које обављају	
9. Подаци о осудама за кривично дело, привредни преступ и прекршај правног лица и одговорних лица у правном лицу, као и подаци о поступцима за кривично дело, привредни преступ или прекршај против правног лица који су у току				
10. Подаци о контактима са страним службама безбедности и обавештајним службама				
11. Подаци о учешћу у активностима организације чије су активности и циљеви забрањени				
12. Подаци о одговорности за повреду прописа који се односе на тајност података				
13. Подаци о претходној безбедносној провери				
14. Подаци о праву својине или другом стварном праву на непокретностима, подаци о праву својине на другим стварима уписаним у јавни регистар, као и податак о годишњем финансијском извештају за претходну годину у складу са законом којим се уређује рачуноводство и ревизија				

Место _____

Датум _____

ПОТПИС ПОДНОСИОЦА ЗАХТЕВА

_____

Посебни безбедносни упитник за правна лица	Образац:	ПБУ-2
	ознака степена тајности:	ИНТЕРНО

ПОДАЦИ О ПОДНОСИОЦУ ЗАХТЕВА

1. НАЗИВ ФИРМЕ и седиште, као и претходни називи и седишта		
2. МБ		
3. ПИБ		
4. Име и презиме заступника		
5. Датум и место оснивања		
6. Подаци о служби у страним војскама и паравојним формацијама	Држава – име оружаних снага	Период
7. Дугови настали услед финансијских задужења или преузетих гаранција	Висина финансијских обавеза	Име финансијске институције
8. Други подаци и чињенице, осим података наведених у основном безбедносном упитнику, које правно лице чине подложним утицајима и притисцима које представљају безбедносни ризик		
9. Да ли су и када вршене безбедносне провере		
10. Да ли је раније издат сертификат и под којим бројем		

УПОЗОРЕЊЕ: *Чланом 69. став 1. тачка 1) Закона о тајности података, прописано је да Канцеларија Савета за националну безбедност и заштиту тајних података, решењем одбија захтев за издавање сертификата, ако се на основу извештаја безбедносне, односно допунске безбедносне провере утврди да је подносилац захтева навео неистините и непотпуне податке у основном, односно посебном безбедносном упитнику.*

Дајем писмену сагласност да се приликом вршења **безбедносне провере** прикупљају и обрађују подаци наведени у безбедносном упитнику у складу са прописима о заштити података о личности.

Место _____

Датум _____

ПОТПИС ПОДНОСИОЦА ЗАХТЕВА

_____

БЕЗБЕДНОСНИ УПИТНИК ЗА ФИЗИЧКО ЛИЦЕ

Безбедносни упитник за физичко лице садржи обрасце:

- ОБУ-1, Омот упитника,
- ОБУ-1_01, Подаци о подносиоцу захтева,
- ОБУ-1_02, Отац и мајка подносиоца захтева,
- ОБУ-1_03, Деца подносиоца захтева,
- ОБУ-1_04, Деда и баба по мајци подносиоца захтева,
- ОБУ-1_05, Деда и баба по оцу подносиоца захтева,
- ОБУ-1_06, Усвојилац подносиоца захтева,
- ОБУ-1_07, Старатељ, очух и маћеха, хранитељ подносиоца захтева,
- ОБУ-1_08, Лица која живе у заједничком домаћинству са подносиоцем захтева и
- ПБУ-1, Посебни безбедноси упитник „СТРОГО ПОВЕРЉИВО“ и „ДРЖАВНА ТАЈНА“

ПРОБЛЕМ У ПРАКСИ:

Дају се лични подаци супружника, родитеља, деце, без њихове писмене сагласности?

Покојници нису спорни

Малолетна лица, деца подносиоца – претпоставка је да је подносилац захтева њихов законски старатељ?

БЕЗБЕДНОСНИ УПИТНИК ЗА ФИЗИЧКО И ПРАВНО ЛИЦЕ

Наведене обрасце потребно је:

- испунити читко, штампаним словима и искључиво хемијском оловком,
- један од понуђених одговора мора бити заокружен,
- све рубрике из образаца морају бити попуњене,
- у рубрикама за које нема података мора се ставити коса црта "/",
- на сваком обрасцу мора се написати датум попуњавања и место,
- сваки образац мора бити својеручно потписан од стране подносиоца захтева.

БЕЗБЕДНОСНЕ ПРОВЕРЕ

ИСТОРИЈАТ

У доба комунизма постојао је израз морално-политичка подобност, као тековина комунистичког режима за контролисање интелектуалаца и осталих, који је имао крајње негативну конотацију и односио се на тестирање појединца за вршење неке функције, или за рад на неким радним местима, али крајње нетранспарентним критеријумима (нпр. припадност четничком покрету – родитеља, рођака...).

Углавном су овакве провере вршене с циљем дискредитовања неке особе и њеног елиминисања са одређених друштвених позиција. Бити морално-политички подобан значило је бити идеолошки и политички истоветан владајућој гарнитури, лојалан и ангажован. Често је подобан значило супротно од способан, односно неко ко је без знања и умећа, али зато веран, послушан и беспоговоран.

Представља концепт који обухвата:

- примену одговарајућих прописа, метода, техника и алата од стране једног или више органа (обавештајних и безбедносних служби, полиције и слично), који омогућава етичко и легално прикупљање, обраду и анализу информација или сазнања о предмету или субјекту безбедносне провере

Појам безбедносног проверавања се односи на:

- службене мере, активности, послове и задатке којима овлашћени орган безбедности, у законом предвиђеној процедури, уз уважавање професионалне етике, утврђује безбедносну подобност лица и даје му или ускраћује безбедносну дозволу за остваривање неког његовог права (права привилеговано школовање у сектору безбедности и одбране, на рад у специфичним државним органима, за бављење одређеним делатностима у промету наоружања и војне опреме, за набављање и држање оружја или приступ тајним подацима)

ПОЈАМ БЕЗБЕДНОСНЕ ПРОВЕРЕ

Терминолошки појам безбедносна провера физичких лица, вуче паралелу са енглеским термином security vetting, односно овај појам се односи искључиво на приступ државним или владиним тајним подацима.

У Великој Британији - Провера има за циљ да увери владине органе да појединац није био умешан у шпијунажу, тероризам, саботажу или акције које имају за циљ рушење или подривање парламентарне демократије политичким, индустријским или насилним средствима.

Такође уверава национални орган да појединац није био члан или повезан са организацијом која је заговарала такве активности или је показала недостатак поузданости кроз непоштење, недостатак интегритета или друга понашања. Коначно, процес уверава национални орган да појединац неће бити подвргнут притиску или неприкладном утицају кроз претходно понашање или личне околности.

Безбедносна провера је поступак који пре издавања сертификата за приступ тајним подацима спроводи надлежни орган, у циљу прикупљања података о могућим **безбедносним ризицима** и сметњама у погледу поузданости за приступ тајним подацима;

Безбедносна сметња представља чињеницу која онемогућава издавање сертификата;

Безбедносни ризик је поступак процене од органа који врши проверу чињеница које указују на проблем постојања лојалности организацији – Републици Србији;

Методолошки могу се поделити на:

1. проверу по месту становања и по месту запослења;
2. проверу из јавних и других евиденција и оперативних евиденција којима располажу органи јавне власти, полиција и службе безбедности;
3. проверу евиденција која располажу правна лица – тзв. Комерцијалне евиденције
4. проверу података на основу међународне сарадње из евиденција које се налазе у иностранству.

ПОСЕБНО ПИТАЊЕ:

- Провера друштвених и социјалних мрежа на интернету и испољених интересовања, ставова, понашања и слично....
- Ово се већ деценијама сагледава за рад у великим компанијама

Члан 3. Правилника о безбедносим проверама лица које обавља Војнобезбедносна агенција

Сврха безбедносне провере је процена безбедносног ризика код лица за које се обавља безбедносна провера на основу оцене навода у упитнику за основну безбедносну проверу.

Предмет одговарајуће безбедносне провере су подаци из упитника за основну безбедносну проверу прописани законом и овим правилником.

ПРОЦЕНА РИЗИКА

Процена ризика је одређивање квантитативних и квалитативних вредности ризика који се односе на конкретну ситуацију и признато претње (назива опасност).

Квантитативна процена ризика захтева прорачуне две компоненте ризика (Р):, величина потенцијалног губитка (Л), а вероватноћа (п) да ће доћи до губитка.

Безбедносни ризик је стварна могућност нарушавања безбедности тајних података;

Процена ризика се састоји од објективне процене ризика у којима су претпоставке и неизвесности јасно представљене и разматране.

Део тешкоћа у управљању ризиком је да је мерење и од количине у којима процена ризика у питању - потенцијални губитак и вероватноћа појаве - може бити веома тешко мерити.

Могућност грешке у мерењу ова два концепта је велика.

Ризик са великим потенцијалним губитком и веома малу вероватноћу дешавају се често третира другачије од оног са ниским потенцијалне губитке и са већом вероватноћом од дешавају.

У теорији, обе су од скоро исти приоритет, али у пракси то може бити веома тешко управљати када се суоче са недостатком ресурса, посебно време, у коме се спроведе процес управљања ризицима.

Када је реч о проценама ризика код физичких и правних лица, онда је битно указати на следеће:

- процену личности кандидата (правног или физичког лица)
- процена безбедносног ризика

Процену личности кандидата:

- лични идентификациони подаци, имовинског стања, његовог друштвеног понашања, запослења, личних особина, образовања, положаја у друштву, социјалног окружења и контаката са другим лицима, здравственог стања, његове породице (супружника, деце, рођака и слично) и лица са којима живи у заједничком домаћинству, раније осуђиваности и слично.

Ова процена се обавља на основу јавних и других података и евиденција које воде државни органи.

Процена безбедносног ризика

- своди се на податке које оперативним радом прикупљају службе безбедности на основу индикатора угрожавања безбедности, али и процену могућег стања безбедносног ризика које би проверавано лице могло имати на националну безбедност омогућавањем приступа тајним подацима највишег нивоа.

СТЕПЕНИ:

1. НИЗАК 2. СРЕДЊИ 3. ВИСОК
1а. НИЗАК КА СРЕДЊЕМ 2а. СРЕДЊИ КА ВИСОКОМ

Члан 3. Правилника о безбедносим проверама лица које обавља Војнобезбедносна агенција

Безбедносни ризик, у смислу овог правилника, постоји када постоји стварна могућност нарушавања безбедности тајних података, односно када на страни лица за које се обавља безбедносна провера постоје такве чињенице и околности које доводе у сумњу његову поверљивост и поузданост.

ПРАВНИ ОСНОВ

НАЦИОНАЛНИ	МЕЂУНАРОДНИ
- ЗАКОН О ТАЈНОСТИ ПОДАТАКА - ЗАКОН О БИА - ЗАКОН О ВБА И ВОА - ЗАКОН О ПОЛИЦИЈИ - УРЕДБА О ОДРЕЂИВАЊУ ПОСЛОВА БЕЗБЕДНОСНЕ ЗАШТИТЕ ОДРЕЂЕНИХ ЛИЦА И ОБЈЕКАТА	СПОРАЗУМИ СА НАТО, ЕУ, БИЛАТЕРАЛНИ....

Безбедносно информативна агенција (БИА)

Одредбама закона о БИА, није предвиђено вршење безбедносних провера, као што је то у прописима о раду полиције и ВБА. Међутим, одредбама члана 20. и 20в. Закона о БИА, предвиђена је безбедносна провера кандидата за пријем у радни однос у БИА.

Поред тога, у одредбама више посебних закона предвиђене су безбедносне провере лица које обавља БИА.

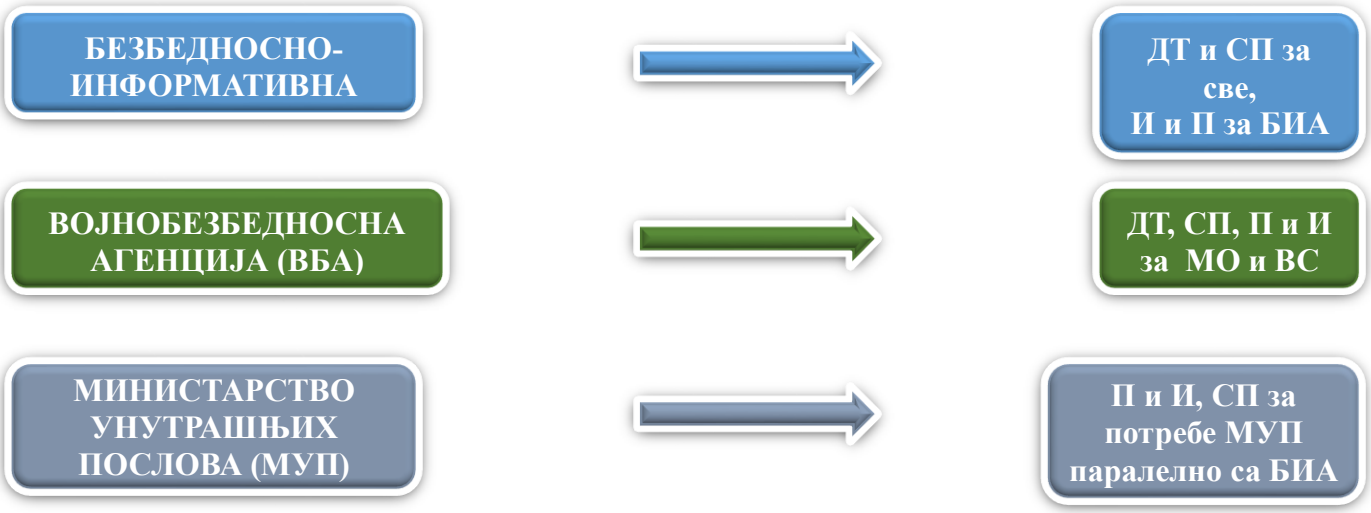
Војнобезбедносна агенција (ВБА)

Рад ВБА на вршењу безбедносних провера физичких лица, правно је уоквирен одредбама Закона о одбрани, Закона о Војсци и Закона о ВБА и ВОА, односно додатно је прецизиран Правилником о безбедносним проверама лица које обавља Војнобезбедносна агенција

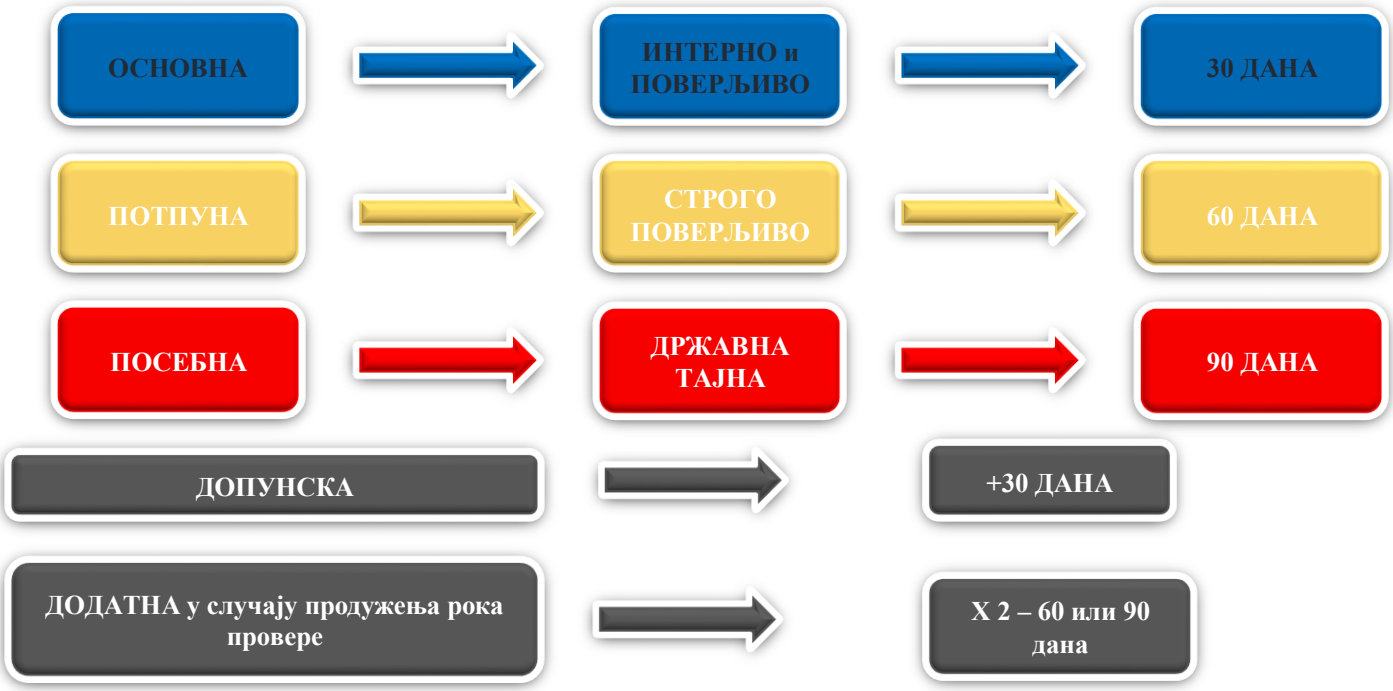
Министарство унутрашњих послова – полиција

Безбедносно проверавање лица, које обавља полиција, као посебно полицијско овлашћење, уређено је одредбама члана 64. и 102., као и одредбама члана 137. став 1. (приликом заснивања радног односа у полицији и Министарству унутрашњих послова) Закона о полицији.

БЕЗБЕДНОСНЕ ПРОВЕРЕ



ВРСТЕ БЕЗБЕДНОСНИХ ПРОВЕРА



Основна и потпуна безбедносна провера

- Попис критеријума за безбедносне ризике и сметње које проистичу из члана 58, 59 и 60. ЗТП:
  - Кривична осуђиваност (безбедносна сметња)
  - Кривични поступци у току (безбедносна сметња)
  - Прекршајна осуђиваност (безбедносна сметња)
  - Прекршајни поступци у току (безбедносна сметња)
  - Контакти са страним службама безбедности и обавештајним службама (безбедносни ризик)
  - Учешће у активностима организације чије су деловање и циљеви забрањени (безбедносни ризик)
  - Подаци о одговорности за повреду прописа који се односе на тајност података (безбедносна сметња)
  - Подаци о праву својине или другом стварном праву на непокретностима, подаци о праву својине на другим стварима уписаним у јавни регистар, као и податак о годишњем финансијском извештају за претходну годину у складу са законом којим се уређује рачуноводство и ревизија (безбедносни ризик)
  - Служба у страним војскама и паравојним формацијама (безбедносна сметња)
  - Други подаци и чињенице који физичко и правно лице чине подложним утицајима и притисцима који представљају безбедносни ризик; (безбедносни ризик)
  - Дуговима насталим услед финансијских задужења или преузетих гаранција. (безбедносна сметња)

Додатни критеријуми за правна лица (чл. 59), поред оних претходно наведених би обухватали и оне (из тач. 9) које се односе на:

- податке о осудама за кривично дело,
- привредни преступ и прекршај правног лица и одговорних лица у правном лицу, као и
- податке поступцима за кривично дело, привредни преступ или прекршај против правног лица који су у току.

СВЕ ТРИ КАТЕГОРИЈЕ ПОДАТАКА ПРЕДСТАВЉАЈУ БЕЗБЕДНОСНУ СМЕТЊУ...

Посебна безбедносна провера

1. Критеријуми за потребе посебне безбедносне провере – за утврђивање безбедносног ризика приступ тајним подацима (чл. 62) обухватају, поред оних из потпуне безбедносне провере и проверу чињеница, околности и догађаја из приватног живота подносиоца захтева, најмање у последњих десет година од дана подношења захтева за издавања сертификата, које би, у случају, представљале основ за сумњу у његову поверљивост и поузданост, а нарочито ако су његове активности у супротностима са интересима Републике Србије или ако је повезан са станим лицима која могу да угрозе безбедност и међународне интересе Републике Србије. (БЕЗБЕДНОСНИ РИЗИК)

Допунска безбедносна провера (члан 66.)

2. ако се из извештаја о резултатима безбедносне провере, али и из препоруке не може утврдити да ли су испуњени законом прописани услови за издавање сертификата физичком или правном лицу, или је после обављене безбедносне провере дошло до битне измене провераваних података која би могла бити од утицаја на издавање сертификата, Канцеларија Савета ће захтевати од надлежног органа из члана 54. овог закона да изврши допунску проверу, односно допуну извештаја и израду нове препоруке, најкасније у накнадном року од 30 дана.

Додатна безбедносна провера (члан 63. став 2 и 3 ЗТП)

3. Изузетно, ако за то постоје оправдани разлози, рокови из става 1. тач. 2) и 3) овог члана се могу продужити најдуже за временски период утврђен у овим тачкама.

У случају из става 2. овог члана надлежни орган је дужан да о продужењу рока обавести руководиоца органа јавне власти који је доставио захтев за безбедносну проверу и Канцеларију Савета.

Зако о детективској делатности у члану 3. тачка 14, као и Закон о приватном обезбеђењу у члану 12. дефинише опште услове за издавање лиценце, али и безбедносне сметње.

Безбедносна сметња постоји:

1. ако је лице правноснажно осуђено на казну затвора или се против њега води поступак за кривична дела:
    - против живота и тела, против слобода и права човека и грађанина, против полне слободе, против брака и породице, против имовине, против здравља људи, против опште сигурности људи и имовине, против уставног уређења и безбедности Републике Србије, против државних органа, против јавног реда и мира, против човечности и других добара заштићених међународним правом, односно
    - ако му је правноснажном одлуком изречена мера безбедности: забрана вршења позива, делатности и дужности, обавезно психијатријско лечење и чување у здравственој установи, обавезно психијатријско лечење на слободи, обавезно лечење наркомана или алкохоличара, за време на које је мера изречена;
2. ако је лице правноснажно кажњавано у последње четири године за прекршаје из области јавног реда и мира за које је прописана казна затвора и прекршаје прописане законом којим се уређује оружје и муниција, односно ако му је правноснажном одлуком изречена заштитна мера: забрана вршења одређених делатности или забрана одговорном лицу да врши одређене послове, обавезно лечење зависника од алкохола и психоактивних супстанци и обавезно психијатријско лечење за време на које је мера изречена;
3. ако је на основу безбедносно-оперативне провере у месту пребивалишта, боравишта или месту рада утврђено да лице, својим понашањем, навикама и склоностима указује да ће представљати опасност за себе или друге и јавни ред и мир.

Безбедносне сметње предвиђене су и у члану 138. Закона о полицији, као елиминаторни фактор за заснивање радног односа у Министарству унутрашњих послова.

Безбедносна сметња за пријем у радни однос у Министарству унутрашњих послова постоји у следећим случајевима:

1. против лица се води кривични поступак за кривична дела која се гоне по службеној дужности;
2. лице је осуђивано због кривичног дела за које се гони по службеној дужности;
3. лице је осуђивано на казну затвора у трајању од најмање шест месеци;
4. лицу је радни однос у државном органу престао по основу правноснажне одлуке надлежног органа због тешке повреде службене дужности, односно теже повреде радне дужности;
5. лицу је радни однос у правном лицу са јавним овлашћењима престао због повреде радне обавезе или непоштовања радне дисциплине;
6. лице је правноснажно кажњено за прекршаје из области јавног реда са елементима насиља и за прекршаје у области прописа којима се уређује набављање, држање и ношење оружја и муниције;

7. Лице својим навикама, понашањем или склоностима указује да неће бити достојно за рад у Министарству;
8. Лице, које се проверава, у поступку безбедносне провере о себи даје неистините податке ради прикривања чињеница које би представљале безбедносну сметњу

ПРОБЛЕМ У ПРАКСИ:

Приликом попуњавања рубрике у колони контакти са страним обавештајним службама, има се у виду сваки легалан контакт у оквиру међународне сарадње...

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

ДОКУМЕНТИ СА ОЗНАКОМ ТАЈНОСТИ!

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

ПРОВЕРЕ ЗА ПОТРЕБЕ БИА И ВБА

- БИА врши безбедносне провере и издаје сертификате за потребе запослених у БИА
- ВБА врши безбедносне провере и издаје сертификате за потребе запослених у ВБА и ВОА.

ПОЗИТИВНА ПРЕТПОСТАВКА

Ако се безбедносна провера не изврши у роковима утврђеним ЗТПом, сматра се да не постоји безбедносни ризик приступа тајним подацима подносиоца захтева.

Решење у супротности са политикама ЕУ и НАТО

ЈЕДНИСТВЕНА МЕТОДОЛОГИЈА ЗА ПРОЦЕНУ БЕЗБЕДНОСНОГ РИЗИКА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА КОД ФИЗИЧКИХ ЛИЦА

Органи надлежни за вршење безбедносне провере из ЗТПа (БИА, ВБА и МУП), достављају Канцеларији Савета извештај о резултатима безбедносне провере, односно посебне безбедносне провере, укључујући и попуњени безбедносни упитник, са препоруком за издавање или ускраћивање сертификата.

У овом извештају не наводе се извори безбедносне провере.

Извештај и препорука означавају се степеном тајности „ПОВЕРЉИВО”.

ПРОБЛЕМ У ПРАКСИ - СТРАНКА НЕМА ПРИСТУП ОВИМ ПОДАЦИМА!

ЗНАЧАЈ ПРОВЕРЕ МЕДИЦИНСКИХ ПОДАТАКА ЗА ДОБИЈАЊЕ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА

Провера медицинских података је **кључан аспект безбедносне провере** јер омогућава процену да ли кандидат има **менталне, неуролошке или друге здравствене сметње** које могу утицати на његову способност да **поуздано, свесно и одговорно рукује тајним подацима и информацијама**.

1. Основни циљеви провере медицинских података

1. **Процена когнитивне способности**
   - Особа која има приступ тајним подацима мора бити у стању да **разумно расуђује, логички размишља, памти важне информације и правилно доноси одлуке**.
   - Болести попут деменције (F00–F03), тешких облика епилепсије (G40), или цереброваскуларних поремећаја (I67) могу нарушити ове способности.
2. **Процена психичке стабилности и контроле над понашањем**
   - Кандидат мора бити **емоционално стабилан, одговоран и самоконтролисан** како би избегао ризике попут намерног или ненамерног одавања тајних података.
   - Озбиљни психијатријски поремећаји (нпр. шизофренија – F20, биполарни поремећај са психотичним епизодама – F31.2) могу утицати на **реалност перцепције, поузданост и предвидивост понашања**.
3. **Процена ризика од зависности од психоактивних супстанци**
   - Особе које имају проблем са **алкохолизмом (F10.2), зависношћу од дрога (F11–F19) или злоупотребом лекова** могу бити склоне **непоузданом понашању, неетичким поступцима или чак коруптивним утицајима**.
   - Зависност повећава ризик од **угрожавања тајних података због могућих уцена или непредвидивог понашања**.
4. **Одржавање безбедности и интегритета система за заштиту тајних података**
   - Ако особа није психофизички способна да **разликује поверљиве од јавних информација**, може угрозити безбедност података.
   - Лица која имају тешке поремећаје концентрације, пажње или импулсивности (нпр. тешки облици ADHD-а – F90.0) могу ненамерно компромитовати поверљиве информације.

2. Како се врши провера медицинских података?

1. **Анализа здравствене документације кандидата**

- Кандидат може бити у обавези да достави **лекарско уверење или извештај психијатра/неуролога**.
- Уколико постоји сумња на одређену болест, могу се тражити **детаљнији здравствени извештаји**.

2. **Психијатријска и психолошка процена**
   - Ако постоје индиције о психичким или когнитивним сметњама, кандидат се може упутити на **психолошко тестирање, процену личности и когнитивних функција**.
   - Психијатар процењује да ли особа има психичку болест која је **контраиндикација за добијање сертификата**.
3. **Медицинско вештачење по налогу безбедносног органа**
   - Ако постоје контрадикторни подаци или сумње, спроводи се **званично медицинско вештачење** од стране комисије специјализованих лекара.

3. Које су последице ако кандидат има медицинске сметње?

1. **Апсолутне сметње** – Сертификат **не може бити одобрен**
   - Тешке менталне болести (F20 – шизофренија, F31.2 – биполарни поремећај са психозом).
   - Неуролошке болести са когнитивним поремећајима (G30 – Алцхајмерова болест, F01 – васкуларна деменција).
   - Тешке зависности од алкохола и наркотика (F10.2, F11.2).
2. **Релативне сметње** – Сертификат се може одобрити под одређеним условима
   - Ако је особа **под сталном терапијом и стабилна**, а болест не утиче на безбедносне аспекте.
   - Ако медицинско вештачење утврди да болест **не представља директан ризик** за руковање поверљивим подацима.
3. **Повлачење већ издатог сертификата**
   - Ако особа након добијања сертификата развије болест која угрожава психофизичку стабилност.
   - Ако безбедносни орган добије нове информације о здравственом стању кандидата.

Провера медицинских података је неопходна ради заштите националне **безбедности, тајних података и стабилности лица које раде са тајним подацима**. Неопходно је осигурати да **ниједна особа са тешким психофизичким поремећајима не добије приступ тајним подацима** јер би то могло довести до **озбиљних безбедносних ризика**.

УПОРЕДНИ ПРИКАЗ ПРАКСИ

Када је у питању обрада медицинских података у контексту безбедносних провера, изузетно је важно да се поступа са дужним поштовањем права лица и да се обезбеди максимална заштита приватности. Применом најбољих пракси у погледу транспарентности, сигурности и етичности, могу се минимизирати потенцијални ризици и злоупотребе, што ће осигурати праведност и безбедност целог система.

Директива 488/2001/ЕЦ Европског парламента и Савета односи се на **заштиту класификованих информација** које се стварају и обрађују у Европској унији, и представља правни оквир за регулисање безбедности и размене класификованих података између држава чланица и институција ЕУ.

Ова директива поставља стандарде који се односе на обраду класификованих информација у државама чланицама, као и на поступке везане за безбедност, комуникацију и размену тих информација.

Директива прописује правила за приступ класификованим информацијама, што подразумева да особе које имају приступ класификованим подацима морају проћи безбедносне провере. Ове провере укључују, али не ограничавају се на:

- **Провере здравственог стања**, које се користе као део безбедносних провера.
- **Процена способности кандидата** за рад на позицијама које подразумевају приступ класификованим информацијама.

Директива 488/2001/ЕЦ, која се односи на безбедност класификованих информација у Европској унији, поставља низ безбедносних стандарда и процедура, али не обухвата у потпуности све аспекте који се односе на провере здравственог стања конкретних лица за приступ класификованим информацијама. Међутим, ова директива даје основе за безбедносне провере и могућност укључивања здравствених провера у процес издавања сертификата за приступ тајним подацима.

Директива 488 наглашава потребу за безбедносним проверама које обезбеђују да особе које имају приступ класификованим информацијама буду поуздане, одговорне и способне да се носе са тајним подацима, без опасности по безбедност информација. То укључује, али није ограничено на:

- **Провере кривичне историје** и остале безбедносне провере, које утврђују да ли особа има историју која може угрожавати безбедност.
- **Здравствене провере** које су важан део безбедносног процеса, како би се утврдило да ли постоје здравствени проблеми који могу утицати на способност особе да одржи потребан ниво концентрације, стабилности или психолошке контроле у критичним ситуацијама.

Здравствене провере су неопходне како би се осигурало да особа која добија приступ класификованим информацијама не пати од здравствених проблема који би могли угрожавати њену способност да ради са тајним подацима. Ово укључује:

- **Психијатријске процене**: Особе које су подложне психијатријским поремећајима, као што су тешке депресије, психозе, биполарни поремећаји или зависности, могу представљати ризик за безбедност, јер њихово здравствено стање може утицати на њихову способност да разумеју или адекватно реагују на опасности.
- **Нервни и когнитивни поремећаји**: Стања као што су деменција, Алцхајмерова болест или Паркинсонова болест, која могу утицати на когнитивне способности особе, могу представљати потенцијалну опасност у контексту рада са класификованим информацијама.
- **Тешке зависности**: Алкохолизам или зависност од психоактивних супстанци може довести до непредвидивог понашања и смањене способности да се одржи поверљивост података.

У Европској унији, национални безбедносни органи који управљају приступом класификованим информацијама у складу са Директивом 488 често укључују:

- **Медицинске и психијатријске процене**: Ове процене могу бити обавезне као део безбедносне провере, у зависности од врсте посла и нивоа тајности информација којима ће особа имати приступ.
- **Редовне медицинске провере**: За раднике који имају сталан приступ класификованим информацијама, обавезне су редовне медицинске провере које се могу проводити у одређеним интервалима, како би се осигурало да њихово здравствено стање не угрожава безбедност информација.

Поштујући начела **Генералног закона о заштити података о личности** (ГДПР), све медицинске провере морају се вршити уз строг поштовање приватности и заштите података. За размену и обраду медицинских података који се користе у контексту безбедносних провера, морају бити обезбеђени одговарајући услови за заштиту и контрола приступа овим подацима.

Уколико се утврди да лице има здравствене проблеме који могу угрожавати његову способност да одржи поверење и безбедност информација, приступ класификованим подацима може бити одбијен или ограничен. У неким случајевима, ако је здравствени проблем привремен, могуће је поново размотрити одлуку након што се стање поправи.

У складу са **Директивом 488/2001/ЕЦ**, провере здравственог стања су важан део безбедносних процедура за добијање приступа класификованим информацијама у Европској унији. Ове провере осигуравају да особе које имају приступ осетљивим подацима не представљају здравствени ризик који би могао угрожавати тајност информација. Поступци морају бити у складу са принципима заштите података о личности, те се морају проводити уз поштовање приватности и у складу са националним и европским законодавством.

НАТО стандард С-М (2002) 49 (у даљем тексту НАТО С49) подразумева да безбедносне провере обухватају различите аспекте кандидата, укључујући:

- **Кривичну историју**.
- **Психолошке процене**.
- **Медицинске процене** (као што је физичко и психијатријско здравље).

НАТО С49 захтева да кандидати за позиције које укључују приступ класификованим информацијама буду психолошки и физички способни да обављају своје задатке без угрожавања безбедности или интегритета података.

У контексту НАТО-а, медицински подаци кандидата се разматрају у складу са строгим процедурама заштите података, али не може се потпуно искључити преглед здравственог стања ако постоји оправдан интерес за процену способности кандидата да обавља задатке који укључују приступ класификованим информацијама.

Медицинска провера у овим случајевима обухвата:

- **Психијатријске процене**: За утврђивање да ли особа има било какве поремећаје који би могли угрожавати безбедност (на пример, психозе, депресије, или друге болести које могу утицати на способност за рад са осетљивим информацијама).
- **Физичке процене**: Које укључују процену способности особе да физички издржи захтевне услове рада који се могу поставити у оквиру НАТО активности.

Заштита личних података је од велике важности, али у контексту НАТО С49 и безбедносних провера, **права на приватност** могу бити ограничена уколико је потребно да се осигура национална безбедност или интегритет НАТО система. Медицински подаци се разматрају само у оквиру потребе да се утврди да ли кандидат може обављати дужности које укључују приступ тајним или класификованим информацијама.

Провере се обављају уз уважавање националних прописа који се односе на заштиту здравствених података, али са напоменом да, ако кандидат ради у НАТО, те провере треба да буду у складу са стандардима које НАТО прописује у С49. То значи да у неким случајевима, локални закони о заштити података неће бити потпуно изједначени са стандардима НАТО, али и даље се поштују основна права кандидата на заштиту приватности.

Када се разматрају медицински подаци у овом контексту, НАТО С49 се може сматрати као оквир који дефинише какви се здравствени подаци могу проверити, али и како се ти подаци требају обрадити уз поштовање **права на приватност** и **етичких принципа**. Такође, државе чланице НАТО-а су обавезне да поступају у складу са локалним законима о заштити података и заштити приватности, али са циљем да обезбеде највиши безбедносни стандард у смислу приступа класификованим информацијама.

У складу са **НАТО стандардима С49**, медицинске провере су важан део безбедносних провера, али оне морају бити балансиране са етичким аспектима заштите приватности

и здравља кандидата. Провере обухватају и психијатријске и физичке процене, али са строгим поштовањем права на приватност у складу са националним и међународним прописима.

Обрада медицинских података у контексту безбедносних провера у САД, Великој Британији, Француској и Немачкој се разликује у зависности од правних, етичких и безбедносних стандарда који су специфични за сваку земљу. Испод су наведене опште карактеристике како је ова област уређена у тим земљама:

САД - У САД, безбедносне провере за приступ тајним подацима (Executive Order 13526—Classified National Security Information из 2009. године), укључујући здравствене провере, регулисани су кроз различите прописе, али најважнији документ је **Федерални закон о приватности и заштити података (HIPAA)** који се примењује на медицинске податке и њихову обраду. Уз то, специфични закони и процедуре, као што су:

- **National Security Agency (NSA)** и **Federal Bureau of Investigation (FBI)** користе безбедносне провере за одређене положаје, али медицински подаци су сачувани као поверљиви и могу се открити само уз јасно одобрење или у оквиру правно оправданих процедура.
- **Executive Order 12968** дефинише стандарде за обавезне безбедносне провере за владине службенике који приступају тајним информацијама. То укључује процену физичког и менталног здравља, али само у случајевима који указују на потенцијални ризик.

Велика Британија - У Великој Британији, обрада медицинских података у контексту безбедносних провера такође подлеже строгим прописима. Основни пропис у овом контексту је **Закон о заштити података из 2018. године** (Data Protection Act 2018) који је усклађен са **ГДПР** прописима, као и смерницама за обраду осетљивих података.

- **The Security Vetting Agency (SVT)** је главни орган за спровођење безбедносних провера и прегледа здравствених и психолошких података ако је то неопходно за процену способности кандидата да управља тајним информацијама.
- Лица која се подвргавају безбедносним проверама, на пример, у оквиру обавештајних служби, имају право да се жале ако сматрају да је њихова приватност нарушена, а обрада медицинских података без њиховог пристанка може бити законски изазвана.
- У Великој Британији, овакве провере су под строгим надзором независних тела као што је **Information Commissioner's Office (ICO)** који надзире поступање са осетљивим подацима.

Француска - У Француској, обрада медицинских података регулисана је **Законом о заштити података** (Loi Informatique et Libertés) и **ГДПР-ом**. За безбедносне провере, посебан значај имају тајност података и строго законско усмеравање процене људских ресурса:

- **Direction Générale de la Sécurité Extérieure (DGSE)** и **Direction de la Protection et de la Sécurité de la Défense (DPSD)** имају овлашћења да провере здравствено стање кандидата за рад на позицијама које укључују тајне информације. Обрада здравствених података је дозвољена у оквиру безбедносних провера само уз пристанак кандидата и у складу са законским ограничењима.
- Француски закон о приватности и заштити података наглашава да било каква обрада осетљивих података, као што су медицински подаци, мора бити ограничена на оно што је стриктно неопходно и да особа има право на информисани пристанак.

Немачка - има веома стриктне прописе у вези са заштитом података, нарочито када су у питању медицински подаци. Основни пропис који регулише ову област је **Закон о заштити података** (Bundesdatenschutzgesetz), као и **ГДПР** који се примењује у целој Европи. Безбедносне провере у Немачкој такође укључују процену медицинског стања лица које има приступ тајним подацима.

- **Federal Office for the Protection of the Constitution (BfV)** и друге безбедносне агенције спроводе безбедносне провере кандидата, али строго поштују право на приватност и слободу од дискриминације. Медицински подаци могу бити обрађени само ако су неопходни за процену способности кандидата да ради са осетљивим информацијама.
- Обрада медицинских података треба да буде заснована на **информисаном пристанку** и **неопходности**, а особама које се подвргавају безбедносним проверама треба бити обезбеђена адекватна правна средства за оспоравање одлука које се доносе на основу тих података.

У свим овим земљама, обрада медицинских података у контексту безбедносних провера строго је регулисана и треба да буде у складу са правима на приватност и заштиту података. Често је потребан **информисани пристанак** кандидата, а све провере морају бити засноване на принципу **неопходности**. Важно је да безбедносни органи поштују законске границе и етичке принципе, као и да постоји надзор и механизми за оспоравање одлука.

Руска Федерација - У Русији, обрада медицинских података у контексту безбедносних провера такође подлеже строгим правним и етичким правилима, али се ослања на различите националне прописе који регулишу ову област. Основни закони и смернице који се односе на обраду медицинских података за потребе безбедносних провера у Русији укључују:

- **Закон о заштити података о личности** из 2006. године (Federal Law No. 152-FZ), који је доносио правни оквир за обраду података о личности, укључујући и медицинске податке. Овај закон предвиђа да се подаци о личности, укључујући осетљиве податке (као што су медицински подаци), могу обрађивати само у складу са строго дефинисаним правима, као што је пристанак субјекта података.

- **Сагласност** субјекта података је обавезна, али постоје изузеци када се медицински подаци могу обрађивати без изричитог пристанка, на пример у случају безбедносних провера када је то неопходно за процену ризика.

- **Закон о националној безбедности Руске Федерације** из 1999. године регулише опште безбедносне провере, укључујући и оне који се односе на здравствено стање појединаца који приступају тајним информацијама. Овај закон, као и сродни прописи, омогућава да се медицински подаци користе за процену способности кандидата да се носи са радом који захтева приступ осетљивим или тајним информацијама.
  - Овде се посебно истиче обавеза процене менталног и физичког здравља кандидата који желе да обављају послове у обавештајним службама, војсци или другим високоризичним областима које подразумевају рад са тајним подацима.

- **Уредбе које се односе на безбедносне провере за особе које се запошљавају у државним органима, органима безбедности и другим органима Руске Федерације** дефинишу процедуре које су потребне за одобрење приступа тајним информацијама у Русији. У овим прописима може бити предвиђено да безбедносне провере укључују медицинске податке, али само када је то неопходно за процену способности кандидата за рад на безбедносно осетљивим позицијама.
  - **Федерална служба безбедности (ФСБ)** и друге безбедносне агенције користе овај оквир за обављање провера, али све обраде медицинских података морају бити у складу са важећим правним и етичким правилима.

- У пракси, медицински подаци за безбедносне провере могу бити захтевани од кандидата за рад на позицијама које захтевају приступ тајним информацијама, али су овај процес и обраду података строго регулисани.
  - Обрада података мора бити **неопходна**, што значи да медицински подаци не могу бити коришћени ако нису релевантни за процену способности кандидата за посао са тајним подацима.
  - Важно је да кандидати буду информисани о обради својих података и да имају право на жалбу ако сматрају да је обрада незаконита или непотребна.

- **Право на приватност** у складу са Уставом Руске Федерације и међународним конвенцијама је још један важан аспект. Лица која се подвргавају безбедносним проверама морају бити свесна својих права, а обрада медицинских података мора бити ограничена на оно што је строго неопходно.
  - У Русији, као и у другим земљама, постоје механизми за пријаву злоупотреба и заштиту права субјеката података.

- У Русији, као и у другим земљама, надзор над овим процесима обављају релевантне државне агенције, али и судови и независна тела која могу оспорити одлуке ако се сматра да су права појединаца нарушена.
    - Етички аспекти су веома важни у овим поступцима, и стручњаци из области здравља и правници морају бити укључени у процес да би се обезбедило да се права кандидата поштовањем закона не нарушавају.

У Русији, као и у другим земљама, обрада медицинских података у контексту безбедносних провера мора бити у складу са строгим законским и етичким прописима. Иако безбедносне агенције имају право да обраде здравствене податке када су потребни за процену способности кандидата за рад на тајним и безбедносно осетљивим позицијама, свака таква обрада мора бити у складу са законом и мора бити обављена уз пристанак кандидата, осим у случајевима када је другачије законом прописано.

У свим земљама из окружења, обрада медицинских података за потребе безбедносних провера је регулисана као осетљиво питање, али се мора извршавати у складу са међународним стандардима као што су **ГДПР** и локалним законодавством. Обрада медицинских података је дозвољена само ако је то **неопходно** за процену способности кандидата за рад на позицијама које подразумевају приступ тајним подацима, уз **информисани пристанак** и у складу са правима на приватност и заштиту података.

Тако се на пример у Босни и Херцеговини предвиђа лекарски преглед одредбама 54. Закона о заштити тајних података да:

(1) Ако се поступком безбедносног проверавања утврди сумња у овисност о алкохолу, дроги или други непримерени облици овисности, генерални директор ОБАБиХ писаним актом може да упути проверавано лице на обављање лекарског прегледа у надлежну институцију.

(2) Ако проверавано лице не прихвати предлог из става (1) овог члана, лице надлежно за издавање дозволе донеће решење о одбијању издавања дозволе за приступ тајним подацима.

СТАЊЕ У РЕПУБЛИЦИ СРБИЈИ

Република Србија - У Србији, при процени безбедносне подобности лица за добијање сертификата за приступ тајним подацима, посебна пажња се посвећује здравственом стању, нарочито у вези са **болестима зависности** и **душевним поремећајима**.

Провере медицинских података, уколико су наведене у упитнику, врше се у складу са Законом о тајности података и Законом о заштити података о личности, као обрада података о личности уз писмену сагласност провераваног лица, за које радње није потребна изричита сагласности и одобрење суда.

На основу члана 58. тачка 13. Закона о тајности података, у основни безбедносни упитник уносе се следећи подаци о подносиоцу захтева:

„***медицински подаци*** у вези са болестима зависности (алкохол, опојне дроге и др.), односно душевним болестима;“.

Поред тога, на основу члана 61. овог закона, подаци из упитника из чл. 58. до 60. овог закона представљају предмет одговарајуће безбедносне провере.

Релевантне болести и медицински подаци - Према Закону о тајности података („Службени гласник РС”, бр. 104/2009, 36/2011 и 104/2013) и пратећим подзаконским актима, приликом безбедносне провере узимају се у обзир следеће категорије болести:

1. **Болести зависности**
    - Алкохолизам (дијагнозе из Ф10 групе према Међународној класификацији болести – МКБ-10)
    - Зависност од опојних дрога (Ф11-Ф19)
    - Зависност од психоактивних супстанци које утичу на расуђивање и понашање
2. **Душевне болести и поремећаји**
    - Шизофренија и слични поремећаји (Ф20-Ф29)
    - Афективни поремећаји (тешке форме депресије, биполарни поремећај – Ф30-Ф39)
    - Озбиљни облици анксиозних и неуротских поремећаја (Ф40-Ф48), ако утичу на расуђивање и способност обављања поверљивих послова
    - Поремећаји личности и понашања (Ф60-Ф69), ако представљају ризик за безбедност
    - Епизодични или пролазни психотични поремећаји

У Србији **не постоји јавно доступна листа апсолутних и релативних сметњи** у вези са здравственим стањем за приступ тајним подацима. Међутим, на основу здравствених

прописа, општих принципа безбедносних провера и страних пракси, могуће је разликовати **апсолутне** и **релативне** сметње.

1. Апсолутне сметње (непосредни разлог за ускраћивање сертификата) - Ово су здравствени проблеми који **аутоматски** дисквалификују особу, јер представљају трајан или тежак ризик по безбедност:

А. Озбиљни психијатријски поремећаји

- **Шизофренија и други психотични поремећаји (Ф20-Ф29)**
    - Халуцинације, заблуде, дезорганизовано размишљање, губитак контакта са стварношћу.
- **Биполарни поремећај – тежи облици (Ф31)**
    - Нарочито тип I, где маничне епизоде могу довести до губитка контроле.
- **Тешке форме деменције и неуродегенеративних болести (Ф00-Ф03)**
    - Алцхајмерова болест, Паркинсонова болест са психозом, фронтотемпорална деменција.
- **Антисоцијални поремећај личности (Ф60.2)**
    - Недостатак емпатије, манипулативно понашање, криминална склоност.
- **Неизлечиви облик зависности од алкохола или дрога (Ф10-Ф19)**
    - Документовани хронични алкохолизам или наркоманија, уз рецидиве и немогућност одржавања апстиненције.

Б. Тешка когнитивна и неуролошка оштећења

- **Органски ментални поремећаји (Ф00-Ф09)** који значајно утичу на когнитивне способности.
- **Епилепсија са тешким психијатријским симптомима** (ако доводи до промене свести и неуропсихијатријских проблема).
- **Пролазне или хроничне психозе** које нису изазване дрогама, али утичу на перцепцију стварности.

2. Релативне сметње (процена појединачног случаја) - Ово су стања која **не морају аутоматски** водити дисквалификацији, али могу представљати безбедносни ризик у зависности од тежине, учесталости симптома и начина лечења.

А. Афективни и анксиозни поремећаји

- **Биполарни поремећај тип II (блажи облици)**
    - Ако су симптоми добро контролисани терапијом и особа нема историју импулсивних одлука.
    -

- **Тешки облици депресије (Ф32, Ф33)**
  - Нарочито ако су праћени суицидалним мислима или честим рецидивима.
- **Гранични поремећај личности (Ф60.3)**
  - Ако особа има историју нестабилних емоционалних реакција, али је под терапијом.
- **Опсесивно-компулзивни поремећај (Ф42) – тежи облици**
  - Ако ритуали или анксиозност значајно утичу на радну способност.

Б. Поремећаји зависности (ако нису у активној фази)

- **Алкохолизам или злоупотреба дрога у анамнези**
  - Ако је лице у вишегодишњој апстиненцији и има стабилну историју рада.
- **Лечење на психијатрији због зависности у прошлости**
  - Процена зависи од рецидива, времена од последњег лечења и стабилности.

В. ПТСП и реакције на стрес (Ф43)

- Ако особа има **блаже облике ПТСП-а**, али нема честе флешбекове или агресивне реакције.
- Тежи облици са дисоцијативним епизодама или губитком контроле над понашањем могу бити разлог за одбијање.

- **Апсолутне сметње** (психоза, тешки облици зависности, деменција) **увек** воде дисквалификацији.

- **Релативне сметње** (афективни поремећаји, ПТСП, анксиозност) процењују се индивидуално.

БОЛЕСТИ ЗАВИСНОСТИ ОД КОЦКЕ (ПАТАЉИЈА), СЕКСА И ТЕШКА БОЛЕСТ У ПОРОДИЦИ

У контексту безбедносних провера за приступ тајним подацима, болести зависности од коцке (патаљија) и зависности од информационо-комуникационих технологија (ИТ), као и тешка болест у породици представљају релевантне аспекте које могу бити узете у обзир, иако нису увек специфициране у свим прописима.

1. Зависност од коцке (патаљије) - може бити проблем који утиче на појединца у различитим аспектима живота, укључујући и његов радни учинак и понашање у

ситуацијама које захтевају висок ниво одговорности и пажње, као што је рад са класификованим информацијама. Зависност може довести до **непажње, неразумности**, и потенцијалне **манипулације** подацима ако се појединац нађе у тешкој финансијској ситуацији или изложен већим ризицима од злоупотребе поверења.

- **Безбедносни ризик**: Особа која се бори са зависношћу од коцке може бити подложна манипулацијама, уценама или претњама које могу угрозити безбедност података. Могућа је и појава **непажљивог понашања** или **погрешних одлука** које могу утицати на безбедност информација којима се управља.
- **Провера зависности**: Психијатријске или психолошке процене могу бити коришћене у контексту утврђивања да ли постоји зависност од коцке. Лице које показује знаке зависности може бити сматрано као висок ризик за добијање приступа класификованим подацима, јер зависност може утицати на процену ризика, емоционалну стабилност и одговорност.

2. **Зависност од информационо-комуникационих технологија (ИТ) -** подразумева прекомерну употребу дигиталних алата, као што су мобилни телефони, рачунари, друштвене мреже или видео игре, која може довести до **поремећаја концентрације**, **смањене продуктивности** или чак **психолошких проблема**.

- **Безбедносни ризик**: Зависност од ИТ технологија може утицати на способност појединца да управља осетљивим информацијама. Прекомерна употреба интернета и друштвених мрежа може повећати ризик од изложености **сајбер нападима** или **друштвеним манипулацијама**, што би могло угрожавати безбедност података.
- **Психолошки аспекти**: Вишак времена проведеног у дигиталном свету може довести до **anxiety** (анксозности), **дисторзије перцепције** или **неадекватних реакција** на стресне ситуације, што може утицати на појединца када је изложен раду са важним или тајним подацима.
- **Оцењивање ризика**: Психијатријске или психолошке процене могу обухватити и тестирање зависности од технологије, али и утицаја који ова зависност има на способност кандидата да обавља своје обавезе без угрожавања безбедности података.

3. **Како се то односи на безбедносне провере? -** У контексту безбедносних провера за приступ тајним подацима, зависности (од коцке и ИТ) представљају **релативне безбедносне сметње**, што значи да су фактори који могу утицати на процену појединца као „поверљивог“ за рад са тајним информацијама. Уколико постоје знаци зависности који утичу на психичко и физичко здравље кандидата, проценитељи могу сматрати да особа представља **ризик** и може бити одбијена за приступ тајним подацима.

- **Психијатријске и медицинске процене**: Уколико зависност може озбиљно утицати на когнитивне способности, оцењивање способности појединца да адекватно доноси одлуке у високо одговорним ситуацијама, као што је рад са

класификованим информацијама, може довести до негативног резултата безбедносне провере.

- **Друштвене и психолошке последице**: Зависности, било да су везане за коцку или ИТ, могу довести до социјалних проблема, конфликата, као и потенцијално угрозити интегритет кандидата, што може довести до његовог одбацивања у процесу безбедносне провере.

Како зависност од коцке и ИТ технологија може озбиљно утицати на стабилност и способност појединца да адекватно обавља задатке који подразумевају рад са тајним информацијама, она се мора узети у обзир као потенцијални ризик у безбедносним проверама. Важно је проћи **психолошке и медицинске процене** које ће одредити да ли зависност представља опасност по безбедност класификованих података.

3. Зависност од секса или сексуална зависност, која се карактерише прекомерном и неконтролисаном потребом за сексуалним активностима која може бити психолошки и физички штетна, може се разматрати као фактор у безбедносним проверама за приступ класификованим информацијама, али као и код других зависности, њен утицај зависи од озбиљности и последица које она има на појединца.

Психолошке последице зависности од секса - Зависност од секса може имати различите психолошке и социјалне последице које могу утицати на појединца и његову способност да безбедно управља осетљивим подацима:

- **Импулсивност и контролисано понашање**: Сексуална зависност може довести до **импулсивног понашања** које укључује неадекватне одлуке или недостајућу способност за контролисање личног понашања у друштвеним и радним ситуацијама. Ово може повећати ризик од **непажљивог понашања** које може угрожавати сигурност тајних података/информација.
- **Психолошка нестабилност**: Ако зависност доводи до **психолошке нестабилности**, то може утицати на способност појединца да донесе рационалне одлуке и да се емоционално носи са стресним ситуацијама, што је критично за особе које раде са тајним подацима.
- **Ризик од манипулације или изнуде**: Сексуална зависност може довести до ситуација у којима се појединац може лако **манипулисати** или бити подложан **изнуди**, што повећава ризик од угрожавања безбедности података. Особа која је изложена оваквим ризицима може бити под претњама које се односе на своје личне или професионалне слабости.

Како се зависност од секса разматра у безбедносним проверама? - У безбедносним проверама, зависност од секса може бити процењена као **релативна безбедносна сметња**, што значи да се разматра у контексту како она утиче на когнитивне способности, емоционалну стабилност и способност појединца да адекватно обавља задатке који укључују рад са тајним информацијама.

- **Психијатријске процене**: Ако зависност од секса доводи до озбиљних психолошких или социјалних проблема, психијатријска процена може бити потребна. Психијатри може утврдити да ли зависност представља озбиљан фактор који угрожава безбедност података.
- **Негативни резултати у безбедносним проверама**: У зависности од степена зависности и њених последица, овај фактор може довести до **неповољне процене** или чак **негирања приступа класификованим информацијама**. У случају да зависност доводи до значајних поремећаја у психолошком или социјалном функционисању, може се сматрати да појединац представља превелики ризик за рад са тајним информацијама.

Могући етички и правни аспекти:

- **Приватност и заштита података**: Лице које показује знаке сексуалне зависности може бити подложно већим проверама, али важно је да се ове процене спроводе уз поштовање његових права на приватност. Лични подаци о зависности, као и сви други медицински или психолошки подаци, морају бити обрађени у складу са прописима о заштити података.
- **Право на приступ**: Лице са зависношћу од секса има право на поштовање својих основних људских права, али у контексту безбедносних провера, та права могу бити ограничена ако постоји оправдана опасност по безбедност информација.

Зависност од секса може представљати **релативну безбедносну сметњу** у безбедносним проверама, али процена ће зависити од степена зависности и њених последица по појединца. Ако зависност доводи до значајних психолошких или социјалних проблема који угрожавају способност појединца да безбедно управља осетљивим информацијама, она може довести до **одбијања издавања сертификата** за приступ тајним подацима. Свака провера мора бити спроведена уз поштовање приватности и етичких стандарда, са циљем заштите националне безбедности и интегритета система заштите тајних података.

Иако неки од ових медицинских података нису експлицитно обухваћени прописима, они могу утицати на безбедносне провере ако утичу на појединчеву способност да адекватно обавља своје обавезе у контексту рада са тајним подацима. Свако здравствено стање које може довести до смањене когнитивне способности, психолошке стабилности, импулсивности или ризика од неадекватних одлука треба пажљиво размотрити током безбедносних провера.

3. **Тешка болест у породици** може бити релевантна у контексту добијања сертификата за приступ тајним подацима, али утицај такве ситуације зависи од различитих фактора. Уопштено, сама болест у породици не би требало да буде аутоматски разлог за одбијање сертификата, али постоје ситуације у којима она може утицати на процену безбедности.

Емоционални и психолошки утицај:

- **Тешка болест чланова породице** може довести до стреса, анксиозности или депресије код особе која аплицира за сертификат. Ако је болест озбиљна и ако особа не може да се носи са стресом који она доноси, то може утицати на њену способност да се концентрише или да доноси рационалне одлуке, што представља ризик у контексту рада са осетљивим информацијама.
- Психолошка оптерећења, попут анксиозности због бриге о болесном члану породице, могу утицати на пажњу и способност да се одговорно приступи класификованим подацима.

Потенцијални облик уцене:

- У неким случајевима, ако члан породице има озбиљну болест која захтева скупу или специфичну медицинску негу, то може створити ситуацију у којој особа може бити изложена **притисцима или уценама**. На пример, особа која има особу у породици која захтева скупе третмане може бити подложна манипулацијама или понудама које компромитују њену одговорност при раду са тајним подацима.

Дискреционо право надлежног органа:

- У складу са прописима о безбедносним проверама, надлежни органи имају дискреционо право да процене све релевантне околности, укључујући **породичне факторе** који могу утицати на појединца.
- **Тешка болест у породици** може бити узета у обзир као додатни фактор у процесу процене способности појединца да безбедно и одговорно приступа класификованим информацијама.
- Ако је болест члана породице озбиљна и ако се сматра да то значајно утиче на личну стабилност апликанта, то може бити основа за одлуку да се сертификат не изда. Међутим, то не мора бити аутоматска одлука и треба размотрити све релевантне чињенице и доказе.

Прелазне ситуације:

- У случајевима када је особа изложена великом стресу због болести у породици, али то није дугорочно или трајно утицало на њену способност да обавља свој посао, може бити могуће одложити одлуку или поново размотрити ситуацију у будућности.
- На пример, ако болест члана породице траје само привремено и не утиче на радну способност особе на дужи рок, то може бити разлог да се одложи издавање сертификата или да се изврши додатна процена после извесног периода.

Прописи и приватност:

- Здравствени подаци и породица уопште спадају под заштиту приватности. У складу са прописима, као што су Закон о заштити података о личности и међународне обавезе (као што је **GDPR**), не би требало да се дају детаљи о

здрављу чланова породице ако то није неопходно. Процена треба да буде заснована на општем утицају који болест може имати на апликанта и његову способност да испуни захтеве у вези са приступом класификованим информацијама.

Тешка болест у породици може бити релевантна у контексту безбедносних провера ако утиче на емоционалну или психолошку стабилност појединца, или ако ствара ситуације које повећавају ризик од уцене или манипулације. Међутим, сама болест не мора бити аутоматски разлог за одбијање сертификата. На основу свих релевантних чињеница, надлежни органи ће донети одлуку која ће бити у складу са безбедносним интересима.

ОСТАЛЕ БОЛЕСТИ КОЈЕ НИСУ ОБУХВАЋЕНЕ БЕЗБЕДНОСНИМ УПИТНИКОМ АЛИ МОГУ ИМАТИ УТИЦАЈ НА БЕЗБЕДНОСНЕ ПРОВЕРЕ

Код безбедносне провере за издавање сертификата за приступ тајним подацима, неуролошке болести које могу утицати на когнитивне способности кандидата обухватају следеће дијагнозе према **Међународној класификацији болести (МКБ-10 и МКБ-11),** као и тешке хроничне болести које утичу на **психофизичку стабилност** кандидата за добијање сертификата за приступ тајним подацима обухватају болести које значајно нарушавају когнитивне способности, свест, концентрацију, самоконтролу или општу функционалност:

А) НЕУРОЛОШКЕ БОЛЕСТИ

1. Дегенеративне болести централног нервног система (ЦНС) са когнитивним оштећењем

- **G30.0 – G30.9 → Алцхајмерова болест** (у свим стадијумима)
- **G31.0 → Фронтотемпорална деменција (Пикова болест)**
- **G31.2 → Деменција код Паркинсонове болести**
- **G31.82 → Деменција код Хантингтонове болести**
- **G31.83 → Деменција код мултипле склерозе (когнитивни облик)**
- **G23.1 → Прогресивна супрануклеарна парализа (ПСП)**

2. Васкуларне болести мозга са когнитивним оштећењем

- **I67.3 → Прогресивна васкуларна леукоенцефалопатија (Бинсвангерова болест)**
- **F01.0 – F01.9 → Васкуларна деменција (узрокована можданим ударима или хроничном исхемијом мозга)**

3. Неуроинфекције и метаболички поремећаји који изазивају когнитивне сметње

- **A81.0 → Крецфелд-Јаковљева болест (прионска болест)**

- **B22.1 → ХИВ-асоцирана деменција**
- **E75.4 → Наследне метаболичке болести са когнитивним оштећењем (нпр. Ниман-Пикова болест, Гошеова болест)**

4. Епилепсије са значајним когнитивним последицама

- **G40.2 → Епилепсија са честим генерализованим нападима и когнитивним последицама**
- **G40.4 → Епилептична енцефалопатија (нпр. Ленокс-Гасто синдром, Ландау-Клефнеров синдром)**

5. Друге болести ЦНС које могу довести до когнитивног оштећења

- **G35 → Мултипла склероза са прогресивним когнитивним оштећењем**
- **G12.2 → Амиотрофична латерална склероза (АЛС) са когнитивним поремећајем**
- **G93.4 → Енцефалопатија различите етиологије (токсична, метаболичка, посттрауматска)**

Б) ТЕШКЕ ХРОНИЧНЕ БОЛЕСТИ

1. Кардиоваскуларне болести са утицајем на когнитивне функције и свест

- **I60 – I69 → Последице можданог удара (исхемијског или хеморагичног) са неуролошким оштећењима**
- **I67.9 → Цереброваскуларна болест, неспецифицирана (укључујући хроничну церебралну исхемију)**
- **I95.1 → Ортостатска хипотензија са честим несвестицама**
- **I50.0 – I50.9 → Срчана инсуфицијенција са епизодама губитка свести**

2. Ендокринолошки и метаболички поремећаји са утицајем на психофизичку стабилност

- **E10.64 / E11.64 → Дијабетес мелитус са честим хипогликемијама и когнитивним последицама**
- **E03.9 → Тешки хипотиреоидизам са когнитивним оштећењем (микседемска енцефалопатија)**
- **E22.0 → Акромегалија са неуропсихолошким последицама**
- **E27.1 → Адисонова болест са кризама које утичу на свест и когнитивне функције**

3. Хроничне болести бубрега и јетре са неуропсихолошким последицама

- **N18.5 / N18.6 → Терминална бубрежна инсуфицијенција са уремијском енцефалопатијом**

- **K72.0 / K72.1 → Акутна и хронична јетрена инсуфицијенција са хепатичном енцефалопатијом**

4. Плућне болести са утицајем на оксигенацију мозга

- **J96.1 → Хронична респираторна инсуфицијенција са хипоксијом**
- **J44.9 → Хронична опструктивна болест плућа (ХОБП) у узнапредовалом стадијуму**
- **G47.3 → Синдром опструктивне апнеје у сну са тешком дневном поспаношћу**

5. Болести мишићно-коштног система са утицајем на моторичке и когнитивне способности

- **G71.0 → Прогресивна мишићна дистрофија са тешким утицајем на општу функционалност**
- **M32.1 → Неуролошке манифестације системског еритемског лупуса (СЕЛ)**
- **M35.3 → Миастенија гравис са честим кризама**

Све ове болести могу довести до когнитивних оштећења која могу бити разлог за негативну безбедносну процену, у зависности од тежине и стадијума болести и могу значајно утицати на **поузданост, способност концентрације, доношење одлука и контролу над понашањем**, што су кључни фактори приликом безбедносне провере.. Приликом провере, уколико постоје индиције о постојању когнитивних сметњи и тешких хроничних болести, може се захтевати додатно неуропсихијатријско вештачење. Коначна одлука зависи од **медицинског вештачења**, тежине симптома и потенцијалног ризика за компромитовање тајних података.

МЕДИЦИНСКО ВЕШТАЧЕЊЕ И МИШЉЕЊЕ ПСИХИЈАТРА

Вештачење и мишљење психијатра - У пракси, безбедносне службе БИА, ВБА и Министарство унутрашњих послова могу затражити **медицинско мишљење психијатра**, чак и ако особа нема документовану историју лечења, односно могу указати Канцеларији Савета за националну безбедност и заштиту тајних података да такви проблеми постоје у извештају о безбедносној провери.

Медицинско вештачење треба спроводити **у свим случајевима када постоји основана сумња** да кандидат има **апсолутне медицинске контраиндикације** за добијање сертификата за приступ тајним подацима. Ово се односи на болести које **неизоставно утичу на психофизичку стабилност, когнитивне функције, самоконтролу и способност да поуздано рукује тајним подацима**.

Како се проверава здравствено стање?

- Кандидат приликом безбедносне провере даје сагласност за увид у медицинску документацију.
- Ако се у личним подацима, изјави или достављеној медицинској документацији појаве индиције о постојању тешке болести.
- Ако се прикупљене информације (из разговора са кандидатом, сведочења надређених или резултата тестирања) доведу у питање због сумње у когнитивне способности или психофизичку стабилност.
- Ако постоје нове медицинске околности које су настале након издавања претходног сертификата.
- Ако се у међувремену кандидат лечио од болести које могу утицати на безбедност (нпр. психијатријска стања, епилепсија, неуродегенеративне болести).
- Ако се код особе са сертификатом појаве индикације о психичкој нестабилности, необичном или ризичном понашању.
- Ако радне способности особе постану упитне због хроничних болести које утичу на когнитивне функције или контролу над понашањем.
- Уколико постоје индиције, безбедносне службе могу тражити додатне податке од здравствених установа.
- Лица која су лечена или се лече од болести зависности или душевних поремећаја могу бити проглашена **безбедносно неподобним** за приступ тајним подацима.
- У неким случајевима, могуће је прибавити мишљење специјалисте психијатра, који процењује да ли је лице стабилно и способно за одговорно поступање са тајним подацима.

У пракси се само на основу мишљења **психијатра специјалисте не може** аутоматски утврдити безбедносна сметња која се односи на медицинске податке у поступку безбедносне провере. Одлука се заснива на **опширној процени**, коју могу укључивати додатна вештачења и безбедносна анализа других фактора.

Медицинско вештачење је неопходно када постоји сумња да кандидат има **апсолутне контраиндикације** за добијање сертификата. Ако се болест потврди и процени да угрожава психофизичку стабилност, особа не може добити или обновити сертификат.

ПРОБЛЕМИ У ПРАКСИ ПРОВЕРЕ МЕДИЦИНСКИХ ПОДАТАКА

Проблем у пракси је да медицинске установе у Србији најчешће **не дају** податке о лечењу без **судског налога**, чак и када лице да свој пристанак. Ово произилази из Закона

о правима пацијената („Сл. гласник РС”, бр. 45/2013 и 25/2019), који прописује да су **медицински подаци поверљиви** и да се могу дати само:

1. **Лично пацијенту**
2. **Овлашћеном лицу на основу писмене сагласности пацијента**
3. **На основу судског налога**
4. **Надлежним државним органима у законом предвиђеним случајевима**

Пракса медицинских установа да **не прихватају пристанак лица као довољан основ** за давање података без судског налога **у колизији је** са **Законом о заштити података о личности („Службени гласник РС”, бр. 87/2018)** и **ГДПР-ом** (који је узет као модел за домаћи закон).

Правни основи за обраду медицинских података

Према Закону о заштити података о личности:

1. **Члан 15. став 1** – Податке о личности (укључујући здравствене податке) је дозвољено обрађивати **уз пристанак лица**.
2. **Члан 17. став 2** – Податке о здрављу могу обрађивати само овлашћена лица (лекари, здравствене установе), али **ако постоји пристанак лица**, онда не би требало да буде додатних ограничења.
3. **Члан 45.** – У случају безбедносних провера, државни органи могу добити податке ако је то неопходно за **закониту сврху**, али и тада морају испунити услове заштите података.

ГДПР принципи (General Data Protection Regulation)

Према **члану 9 ГДПР-а**, медицински подаци спадају у **осетљиве категорије**, али могу бити обрађени ако:

- Лице да **изричит пристанак** (члан 9(2)(а))
- Обрада је неопходна за **јавни интерес у области здравља** или **правне обавезе** (члан 9(2)(г))

Колизије у пракси

- Ако особа добровољно да пристанак за увид у своје здравствене податке, **не постоји правни основ да здравствена установа то одбије**, осим ако постоји специфичан закон који прописује другачије.
- Судски налог би требало да буде **потребан само ако особа не да пристанак**.
- Принцип **минималне обраде података** из ГДПР-а каже да се подаци не смеју прикупљати више него што је потребно – а у овом случају, ако постоји пристанак, судски налог је сувишан.

Могуће решење?

- **Здравствене установе би требало да ускладе праксу са Законом о заштити података о личности** и да поштују пристанак лица као довољан основ.
- Ако нека здравствена установа инсистира на судском налогу, **могуће је поднети притужбу Поверенику за информације од јавног значаја и заштиту података о личности**.
- Министарство здравља би могло издати **инструкцију** здравственим установама да поштују пристанак лица у складу са Законом и ГДПР-ом.

У суштини, постојећи проблем је више **питање погрешне праксе** него закона, али је чињеница да ово отежава безбедносне провере у Србији.

Поред изнетих проблема, потребно је уакзати да се у пракси здравствене институције у Републици Србији не понашају на одговарајући професионалан начин када је у питању процена здравственог стања за кандидате за добијање сертификата за приступ тајним подацима и да најчешће одбијају да узму активно учешће.

Практична примена у безбедносним проверама у Србији:

- Безбедносне службе, попут **БИА** и **ВБА** унутар Министарства одбране, као и Министарство унутрашњих послова (полиција), узимају у обзир психијатријску стабилност кандидата.
- **Присуство дијагнозе са списка није аутоматски разлог за дисквалификацију**, али ако постоје докази о **нестабилности, импулсивности или смањеној когнитивној функцији**, особа може бити проглашена безбедносно неподобном.
- Уколико безбедносна служба сумња у ментално здравље кандидата, може тражити **стручну процену психијатра**.
- Код **зависности од психоактивних супстанци**, чак и ако особа није у активном зависничком статусу, постоји могућност да се процењује ризик од рецидива.

Промена здравственог стања након добијања сертификата - Ако у току поседовања безбедносног сертификата лице које га поседује, дође до промене здравственог стања и добије одређене здравствене проблеме који могу утицати на његову способност да одређује, ради, управља или приступа тајним подацима, постоје одређене процедуре које се примењују у складу са прописима о безбедности и заштити тајних података.

Могуће последице и поступци:

1. **Обавештавање надлежних органа**

   Лице које поседује сертификат има обавезу да обавести надлежни орган, као што је Канцеларија Савета за националну безбедност или друга надлежна институција, ако се појаве здравствени проблеми који могу утицати на његову способност да адекватно обавља послове који захтевају приступ тајним подацима. Ово обавештење може бити добровољно, али је од изузетне важности.

2. **Процена утицаја здравствених проблема**

   Канцеларија Савета за националну безбедност, у сарадњи са надлежним здравственим установама, може организовати додатне медицинске процене како би утврдила утицај здравствених проблема на способност лица да приступа тајним подацима. Ако се утврди да здравствени проблеми представљају ризик за безбедност, могу се применити одређене мере.

3. **Привремена суспензија сертификата**

   У случајевима када здравствено стање лица може довести до ризика по безбедност, органи који су надлежни за безбедносне сертификате могу привремено суспендовати сертификат. Ово може бити један од корака ако се утврди да лице није у стању да адекватно обавља своје обавезе које захтевају приступ тајним подацима, као што су озбиљни психијатријски поремећаји, зависност или друге озбиљне болести које угрожавају безбедност.

4. **Тиме се одлучује о могућем поништењу сертификата**

   Ако се утврди да здравствени проблеми озбиљно угрожавају способност да се обављају дужности у оквиру приступа тајним подацима, сертификат може бити поништена. Ово се обично дешава након процене и разматрања свих релевантних информација, укључујући и медицинске извештаје.

5. **Опција за поновну проверу и обнављање сертификата**

   Ако је сертификат привремено суспендован или поништена, лице може поново поднети захтев за издавање сертификата након што се опорави или ако се његово здравствено стање побољша и више не представља ризик за безбедност. Ово подразумева поновну безбедносну проверу, која укључује процену здравственог стања лица.

РИЗИЦИ И ЕТИКА

Поступци који се односе на безбедносне сертификате и здравствено стање морају бити вођени са великом пажњом и одговорношћу. Увек треба поштовати права појединаца, али истовремено се морају увести безбедносне мере које спречавају угрожавање тајних података.

У оваквим случајевима, важно је осигурати да процесе спроводи стручан тим који може објективно проценити утицај здравствених проблема на безбедност и да свака одлука буде у складу са законом, етиком и правима лица.

Етички аспекти безбедносних провера медицинских података су веома важни, јер ова област утиче на осетљива лична права, као и на заштиту здравствених података који су по својој природи осетљиви. Разматрање етичких питања укључује балансирање

између потребе за безбедношћу и заштитом права појединаца. Неки од кључних етичких аспеката укључују:

1. Приватност и поверење

- **Приватност здравствених података**: Етички је неприхватљиво да се здравствени подаци користе или деле без пристанка особе на коју се ти подаци односе, осим ако закон не наложи другачије. Особа која се подвргава безбедносној провери треба да буде обавештена о томе шта ће се с њеним подацима радити, као и да има право да контролише њихово коришћење.
- **Поверење у медицинске професионалце**: Особе које траже приступ тајним подацима имају право да буду уверене да се њихови медицински подаци третирају са поштовањем и у складу са етичким и правним стандардима. Ово подразумева да медицински стручњаци и органи који спроводе безбедносне провере морају поштовати поверљивост и интегритет здравствених информација.

2. Недискриминација

- **Ризик од дискриминације**: Постаје етички проблем ако се безбедносне провере користе као основа за дискриминацију људи са одређеним медицинским стањима, као што су психијатријски поремећаји. Овакав приступ може створити неједнаке услове за приступ одређеним правима или радним местима. Здравствено стање не би требало да буде основ за дискриминацију, већ би требало разматрати у контексту безбедносних ризика.
- **Применљивост критеријума**: Безбедносне провере треба да буду засноване на јасним и праведним критеријумима који су усклађени са правима особа, како би се избегла дискриминација или злоупотреба система.

3. Информисаност и пристанак

- **Информираност лица**: Особа која подлеже безбедносној провери мора бити потпуно обавештена о томе како ће њени медицински подаци бити коришћени, који подаци ће бити обухваћени и које су последице њиховог откривања. Ово укључује дужност органа који врше безбедносне провере да пруже јасне и доступне информације о поступку.
- **Пристанак**: Пристанак особе треба да буде слободан и недвосмислен, и она треба да има могућност да одбије да пружи одређене информације, ако не постоји законски обавезан разлог за њихово откривање. Сваки притисак који се врши на лице да достави податке без стварне слободе избора представља кршење етичких стандарда.

4. Јасноћа у циљевима безбедносне провере

- **Циљ провере**: Етички је важно да циљ безбедносне провере буде јасан и да се ограничава на оно што је неопходно за утврђивање способности лица да приступи тајним подацима. Прекорачење ових граница може бити етички проблематично,

као што је коришћење података у друге сврхе које нису директно повезане са безбедносном проценом.

5. Пропорционалност и минимизација интервенције

- **Пропорционалност**: Етички аспект овде подразумева да се подаци о здрављу користе само у мери која је неопходна за безбедносну проверу. Након што се процени ризик, подаци који нису релевантни за безбедност не би требало да буду обрађивани или чувани. Ово је у складу са принципима минимизације података.
- **Надокнада штете**: Ако се утврди да је дошло до неправедне употребе медицинских података, важно је да постоји механизам за исправку и компензацију, као и правна заштита која ће осигурати права особе.

6. Приступ правди

- **Право на правичан поступак**: Лице које је подвргнуто безбедносној провери треба да има могућност да се жали на одлуку или поступак који се односи на њихово здравствено стање и медицинске податке. Право на правичан поступак је кључно како би се осигурало да ниједан појединац не буде неправедно дискриминисан или оштећен због своје медицинске историје.

Етички аспекти безбедносних провера медицинских података укључују заштиту приватности, избегавање дискриминације, осигурање информисаног пристанка, јасне и праведне циљеве, као и минимизацију интервенције. Праведно и транспарентно поступање са овим подацима у складу са људским правима и етичким стандардима је кључно за избегавање злоупотреба и заштиту појединаца од неправедних последица.

Закон о заштити особа са менталним сметњама (из 2013. године) и поступци безбедносне провере и издавања сертификата за приступ тајним подацима могу бити у супротности, јер се у контексту безбедносних провера често захтева процена менталног здравља, али ова процена мора бити у складу са правима и заштитом особа са менталним сметњама, што може довести до конфликта између два закона.

Члан 2. у тачки 1. овог закона дефинише:

„лице са менталним сметњама је недовољно ментално развијено лице, лице са поремећајима менталног здравља, односно лице оболело од болести зависности;“

Главне тачке конфликта:

1. **Поступак безбедносне провере**:
    - Безбедносне провере, које подразумевају процену здравственог стања, укључују психијатријске провере како би се утврдило да ли лице може безбедно приступити тајним подацима. Међутим, ова процена може довести до ситуације у којој особе са одређеним менталним сметњама или психијатријским болестима не би могле добити сертификат за приступ тајним подацима.
2. **Закон о заштити особа са менталним сметњама**:

- Овај закон штити права особа са менталним сметњама, укључујући забрану дискриминације на основу менталног здравља, као и право на приватност у погледу здравствених података. Он спречава да се људима са менталним сметњама одбијају права на основу њихових здравствених стања у ситуацијама које нису у директној вези са безбедношћу.

Конфликт:

- **Безбедносне провере** могу захтевати отворен приступ личним здравственим подацима, укључујући психијатријску историју, што је у супротности са **Закон о заштити особа са менталним сметњама**, који може обавезивати да особе са менталним болестима имају право да сакрију одређене здравствене податке. Ово може створити правни амбис када се праве процене да ли неко може приступити тајним подацима.

Потенцијална решења:

- **Прилагођавање поступака**: Може бити потребно прилагодити процедуре за процену менталног здравља које су део безбедносних провера тако да буду у складу са правима на заштиту података о личности и правима особа са менталним сметњама.
- **Јасно дефинисање критеријума**: Требало би да се разјасни када се менталне сметње сматрају безбедносним ризиком и на који начин се процена ових фактора врши, како би се избегла дискриминација и непотребно одбијање приступа тајним подацима.

Ово је, дакле, сложено питање које се односи на баланс између безбедносних захтева и заштите људских права.

БАЛАНС ИНТЕРЕСА НАЦИОНАЛНЕ БЕЗБЕДНОСТИ И ЉУДСКИХ ПРАВА

Проблем баланса интереса заштите људских права и безбедносних провера, кроз утврђивање здравственог стања?

У овом случају, могу се кршити нека од основних људских права која су гарантована како националним законима, тако и међународним конвенцијама и документима. Најважнија људска права која могу бити угрожена у контексту безбедносних провера и издавања сертификата за приступ тајним подацима су:

1. Право на приватност (Члан 8 Европске конвенције о људским правима):

- Особама са менталним сметњама може бити онемогућено да заштите своје здравствене и личне податке, јер поступак безбедносне провере обухвата откривање осетљивих информација о здравственом стању, укључујући психијатријску историју. Ово може бити у супротности са правом на приватност

ако се подаци о здрављу откривају без одговарајућег пристанка или ако је процес неповољан за особе које су у менталним и здравственим потешкоћама.

2. Право на недискриминацију (Члан 14 Европске конвенције о људским правима и Члан 2 Протокола бр. 12):

- Ако се одбија приступ тајним подацима или издавање сертификата само због менталног здравља, то може довести до дискриминације на основу физичког или менталног стања. Ово је забрањено како националним законодавством тако и међународним конвенцијама које штите права људи са инвалидитетом, укључујући менталне болести.
- Закон о заштити особа са менталним сметњама из 2013. године наглашава да особе са менталним болестима не би требало да буду дискриминисане на основу њиховог здравственог стања, али поступак безбедносних провера може довести до њихове дискриминације у погледу приступа тајним подацима.

3. Право на слободу и сигурност (Члан 5 Европске конвенције о људским правима):

- Ако се због менталног стања људима одбије приступ одређеним правима, попут приступа тајним подацима, то може утицати на њихову професионалну слободу и сигурност, што може имати негативне последице на њихов радни статус или каријеру.

4. Право на рад (Члан 23 Универзалне декларације о људским правима):

- Одбијање сертификата за приступ тајним подацима може имати озбиљне последице на права људи да обављају одређене радне функције, посебно у државним или безбедносним институцијама, што представља повреду њиховог права на рад и професионални развој.
- Ово је посебно релевантно ако је одбијање сертификата везано за ментално здравље, што може водити ка занемаривању способности особа које имају дијагностиковане менталне поремећаје, али су и даље способне да обављају своје дужности.

5. Право на здравље (Члан 12 Међународног пакта о економским, социјалним и културним правима):

- Закон о заштити особа са менталним сметњама настао је да би се осигурала адекватна здравствена заштита особама са менталним болестима. Ако се ове особе дискриминишу у контексту безбедносних провера, то може довести до неједнаке доступности ресурса и услуга које су им потребне, као што је здравствена заштита у одређеним областима рада.

У контексту безбедносних провера и издавања сертификата за приступ тајним подацима, ако се поступци спроводе на начин који није у складу са прописима и људским правима, могу се кршити следећа **људска права по Уставу Србије**:

1. Право на приватност (Члан 41 Устава Србије):

- Устав гарантује сваком лицу право на приватност, укључујући и право да се његови лични подаци, као и здравствени подаци, обрађују само уз пристанак или у строго прописаним случајевима. Ако безбедносне провере или издавање сертификата захтевају откривање осетљивих личних или здравствених података без пристанка, то може представљати повреду права на приватност.

2. Право на недискриминацију (Члан 21 Устава Србије):

- Устав Србије забрањује дискриминацију по било којој основи, укључујући ментално здравље. Ако се безбедносне провере користе као основа за дискриминацију лица са менталним болестима или поремећајима, то може бити повреда права на једнак третман и слободу од дискриминације.

3. Право на рад (Члан 60 Устава Србије):

- Устав гарантује право на рад сваком грађанину. Ако се безбедносна провера користи као разлог за одбијање приступа тајним подацима или одбијање запошљавања због здравствених или психијатријских проблема, то може нарушити право на рад, посебно у јавним или безбедносним секторима.

4. Право на живот (Члан 10 Устава Србије):

- Иако се ово право односи на заштиту живота, може се косити са правима која се односе на ментално здравље, јер неправилно спроведене безбедносне провере могу довести до неправедних санкција или дискриминације особа са психијатријским поремећајима, што може негативно утицати на њихову животну ситуацију.

5. Право на здравствену заштиту (Члан 68 Устава Србије):

- Ово право обезбеђује свим грађанима право на здравствену заштиту, а свако ограничење у овом праву, нарочито ако се односи на здравствене податке особа које се подвргавају безбедносним проверама, може представљати повреду права на здравље.

6. Право на правичан поступак (Члан 32 Устава Србије):

- Устав Србије гарантује сваком грађанину право на правичан поступак, који укључује право на изузетно поступање у управним и судским процесима. Ако се поступци безбедносне провере не спроводе транспарентно, праведно и у складу са прописима, то може бити повреда права на правичан поступак.

7. Право на слободу и сигурност (Члан 27 Устава Србије):

- Ово право обезбеђује слободу грађана од произвољног задржавања или ограничења. Ако поступци безбедносних провера доведу до ограничења слободе лица на основу њиховог менталног здравља, без одговарајућих правних основа, то би могло представљати повреду овог права.

Повреда права на приватност, недискриминацију и рад, као и потенцијално право на здравље ако процес безбедносне провере није у складу са принципима права и заштите људских права. Овај конфликт се може решити ако се поступак провере изврши у складу са правима особа са менталним сметњама, уз пажљиво разматрање свих релевантних прописа који осигуравају заштиту њихових основних права. Ово уједно у пракси може представљати озбиљну повреду људских права гарантованих Уставом Србије. У случајевима када безбедносне провере и издавање сертификата доводе до дискриминације или других неправилности, то може бити правни основ за захтеве заштите ових основних права.

ПРИМЕНА ЗАКОНА О ОПШТЕМ УПРАВНОМ ПОСТУПКУ – ПОНАВЉАЊЕ ПРАВОСНАЖНОГ ОКОНЧАНОГ ПОСТУПКА

Понављање поступка по ЗУП-у? - У складу са законом о општем управном поступку, постоје одређене ситуације када може доћи до понављања окончаног поступка, због промене здравственог стања лица које поседује сертификат, али ово није аутоматски подразумевано, осим ако постоје специфични разлози или услови који то оправдавају.

У случају када се разматрају здравствени проблеми лица које поседује безбедносни сертификат, може доћи до ситуације која подразумева сходну примену Закона о општем управном поступку, који се односи на поступке унутар јавних органа. У овом контексту, одлуке које се донесу у управном поступку могу се поништити или поново разматрати ако се појаве нови факти који нису били познати у тренутку одлуке, као што су озбиљне здравствене промене које утичу на способност лица да обавља дужности у вези са приступом тајним подацима.

Разлози за понављање окончаног поступка:

Поновно разматрање или понављање поступка може бити оправдано у следећим ситуацијама:

- **Нови чињенице или доказни материјали:** Ако се појаве нови здравствени подаци који значајно утичу на процену способности лица да обавља своје обавезе које захтевају приступ тајним подацима.
- **Неверификовани подаци:** Ако су првобитни подаци били нетачни или непотпуни у тренутку доношења одлуке.

Поништење првостепеног решења (Канцеларије Савета за националну безбедност и заштиту тајних података) од стране другостепеног органа (Министарство правде):

Уколико се установи да је у првостепеном поступку дошло до пропуста или неправилности које утичу на одлуку, другостепени орган (у овом случају Министарство правде) може да поништи првостепено решење. Разлози за поништај могу бити:

- Ако су у поступку дошло до кршења законских процедура.

- Ако су нови подаци који могу бити пресудни утицали на правни основ одлуке.

Другостепени орган не мора аутоматски поништити одлуку, али ако утврди да је првостепена одлука донета на основу непотпуних или нетачних података, може наредити поновни поступак или корекцију.

Шта се дешава ако је поступак поновљен?

Уколико поступак буде поновљен, све релевантне чињенице ће се поново разматрати, укључујући нове здравствене процене. Ако нови подаци потврде да лице више није способно за рад са тајним подацима, безбедносни сертификат може бити привремено суспендован или поништен.

Ако се здравствени проблеми лица које поседује безбедносни сертификат јаве након што је поступак окончан, тада би Министарство правде као другостепени орган могло поништити првостепено решење и наложити поновни поступак. Ово је у складу са принципима општег управног поступка који омогућавају преглед одлука ако се појаве нови докази који могу утицати на исход поступка.

НА КРАЈУ

Када су у питању провере медицинских података за потребе приступа тајним подацима, не само да је важно поштовати правне и етичке стандарде, већ и усмерити се на најбоље праксе које ће осигурати да цео процес буде транспарентан, праведан и безбедан за све укључене.

Коначна процена личности кандидата у вези са медицинским подацима у безбедносним проверама заснива се на **комплетној анализи психофизичке стабилности, когнитивних способности и опште поузданости особе**.

1. Основни критеријуми за процену личности кандидата

1. **Когнитивна способност**
    - Кандидат мора бити способан да **логички размишља, обрађује информације и доноси исправне одлуке**.
    - Тешке неуролошке или психијатријске болести које **угрожавају памћење, расуђивање или перцепцију стварности** представљају озбиљну сметњу.
2. **Психичка стабилност**
    - Личност кандидата мора бити **стабилна, уравнотежена и отпорна на стрес**.
    - Поремећаји личности, импулсивност, агресивност или психотичне епизоде могу бити **сигнал ризика**.
3. **Контрола над понашањем**
    - Кандидат мора бити **самоконтролисан, дисциплинован и одговоран**.

- Болести које узрокују губитак контроле над понашањем (нпр. биполарни поремећај у маничној фази, зависност од алкохола или дрога) могу представљати **озбиљну безбедносну сметњу**.

4. **Поузданост и одговорност**
   - Особа мора бити **поуздана, дискретна и лојална**.
   - Непредвидиво или неодговорно понашање може довести до угрожавања поверљивих података.

2. Улога медицинских података у коначном закључку

На основу медицинских података, кандидат може бити сврстан у једну од три категорије:

1. **Медицински подобан – Нема сметњи за добијање сертификата**
   - Кандидат је потпуно здрав или има **стабилно медицинско стање које не утиче на његове когнитивне и безбедносне способности**.
   - Нема психијатријских, неуролошких или других болести које би угрожавале поверљивост података.
2. **Медицински условно подобан – Потребно додатно вештачење или надзор**
   - Кандидат има **одређене здравствене проблеме**, али они **не представљају тренутну безбедносну сметњу**.
   - Може бити потребан **додатни медицински надзор или периодична провера** (нпр. ако је кандидат био на лечењу од депресије, али је стабилан и под терапијом).
3. **Медицински неподобан – Озбиљне здравствене сметње које угрожавају безбедност**
   - Кандидат има **менталне, неуролошке или зависничке поремећаје који утичу на његову способност да безбедно рукује поверљивим подацима**.
   - Безбедносни орган доноси одлуку о **ускраћивању или повлачењу сертификата**.

✅ **Безбедносна провера узима у обзир медицинске податке, али коначна одлука зависи од свеукупне процене личности кандидата.**

✅ **Медицинско стање кандидата мора гарантовати да је особа способна да одговорно и безбедно приступа поверљивим информацијама.**

❌ **Ако особа има тешке медицинске сметње које утичу на когнитивне способности, психичку стабилност или контролу понашања, сертификат се не може издати.**

⚖️ **У случајевима када постоји сумња, одлука се доноси на основу медицинског вештачења и додатних безбедносних анализа.**

ОРГАН ЈАВНЕ ВЛАСТИ

ОРГАН ЈАВНЕ ВЛАСТИ (чл. 2 т. 7 ЗТП)

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;

ОРГАН ЈАВНЕ ВЛАСТИ (чл. 30 ЗТП)

Орган јавне власти, у складу са овим законом и прописима донетим на основу овог закона, успоставља систем поступака и мера заштите тајних података према следећим критеријумима:

1. степену тајности;
2. природи документа у коме је садржан тајни податак;
3. процени претње за безбедност тајног податка.

ОРГАН ЈАВНЕ ВЛАСТИ (чл. 31 ЗТП)

Орган јавне власти примењује опште и посебне мере заштите у складу са законом и прописом донетим на основу закона, ради заштите тајних података који се налазе у његовом поседу.

КАТАЛОГ ОРГАНА ЈАВНЕ ВЛАСТИ

1. Органи Републике Србије
2. Органи аутономне покрајине
3. Органи општине, града, градске општине
4. Јавна предузећа, установе, организације и друга правна лица чији је оснивач орган Републике Србије, аутономне покрајине или општине/града
5. Привредна друштва чији је оснивач или члан Република Србија, аутономна покрајина, јединица локалне самоуправе
6. Правна лица чији је оснивач претходно описано привредно друштво (под 5.)
7. Правна лица које обавља делатности од општег интереса у смислу закона којима се уређује положај јавних предузећа
8. Правна лица које оснива или финансира у целини, односно у претежном делу, неки од државних органа

НАПОМЕНА:

Правна лица са капиталом, који не потиче из буџета у претежном делу, не могу бити у статусу органа јавне власти, не могу креирати тајне податке, нити «самостално» могу покретати поступке безбедносних провера за физичка и правна лица...

Ово представља облик контроле од стране органа јавне власти над коришћењем и чувањем тајних података на основу уговорног односа

- члан 2. тачка 7. ЗТП – дефиниција органа јавне власти
- члан 9, 10, 11 и 12. ЗТП – овлашћено лице, поступак и одлука за одређивање тајности података;
- члан 31. ЗТП – врсте мера заштите
- члан 46. ЗТП – достављање тајних података на основу уговорног односа;
- члан 51. став 4. ЗТП – подношење захтева;
- 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)

ДРЖАВНИ ОРГАНИ

1. Народна скупштина
2. Председник Републике
3. Министарства, органи управе у саставу министарства, посебне организације образоване у складу са законом којим се уређују министарства
4. Посебне организације образоване у складу са посебним законом (јавне агенције, заводи, дирекције, фондови и друге организације)
5. Правосудни органи – судство, тужилаштва и правобранилаштва
6. Самостални и независни државни органи:
    - Заштитник грађана
    - Државна ревизорска институција
    - Републичка изборна комисија
    - Агенција за борбу против корупције
    - Повереник за слободан приступ информацијама од јавног значаја и заштиту података о личности
    - Повереник за заштиту равноправности
    - Комисија за заштиту конкуренције
    - Комисија за испитивање одговорности за кршење људских права
    - Комисија за спровођење Програма заштите
    - Републичка комисија за заштиту права у поступцима јавних набавки
    - Комисија за хартије од вредности
    - Социјално-економски савет Републике Србије
    - Национални савет за високо образовање
    - Регулаторна агенција за електронске комуникације и поштанске услуге
    - Регулаторно тело за електронске медијеж
    - Народна банка Србије
    - Фискални савет

СУДСТВО

1. ОСНОВНИ СУДОВИ
2. ВИШИ СУДОВИ
3. ПРИВРЕДНИ СУДОВИ
4. УПРАВНИ СУДОВИ
5. АПЕЛАЦИОНИ СУДОВИ
6. ВРХОВНИ КАСАЦИОНИ СУД

Специјализовани судови

ЈАВНО ТУЖИЛАШТВО

1. Врховно јавно тужилаштво
2. Апелациона тужилаштва
3. Виша тужилаштва
4. Основна тужилаштва

Специјализована тужилаштва

ПРАВОБРАНИЛАШТВО

- Државно правобранилашво Републике Србије
- Правобранилаштво Аутономне покрајине Војводине
- Градска правобранилаштва
- Општинска правобранилаштва

ОРГАНИ АУТОНОМНЕ ПОКРАЈИНЕ

1. Скупштина аутономне покрајине
2. Извршни органи аутономне покрајине
3. Покрајинска управа
4. Покрајински заштиник грађана –омбудсман
5. Организације аутономне покрајине

ОРГАНИ ЛОКАЛНЕ САМОУПРАВЕ

1. Органи и организације општине; скупштине општина; председник општине; општинско веће и општинска управа.
2. Органи и организације града; скупштине градова; градоначелник; градско веће и градска управа.

ЈАВНА ПРЕДУЗЕЋА И ПРАВНА ЛИЦА

У зависности од оснивача/оснивачког капитала, могу бити:

1. На републичком нивоу - РЕПУБЛИКА СРБИЈА
2. На нивоу покрајине - АУТОНОМНА ПОКРАЈИНА ВОЈВОДИНА
3. На нивоу локалне самоуправе – ГРАД и ОПШТИНА

1. У области енергетике – нафтна и гасна привреда, рудници угља, електоенергетика, као и децентрализовани систем градских топлана и индустријске енергетике
2. Поштански саобраћај – ЈП ПОШТА, Агенција за поштанске услуге
3. У области саобраћаја
4. У области електронских комуникација
5. У области наоружања и војне опреме
6. коришћења, управљања, заштите, уређивања и унапређивања добара од општег интереса и добара у општој употреби (воде, путеви, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја и др.)
7. Нуклерни објекти
8. У области издавање службеног гласила Републике Србије и издавање уџбеника
9. Управљања отпадом и другим областима
10. Комуналне делатности
11. Друге делатности одређене законом као делатности од општег интереса.

БЕЗБЕДНОСНИ СЕРТИФИКАТИ

УСЛОВИ ЗА ПРИСТУП ТАЈНОМ ПОДАТКУ

„ПОВЕРЉИВО“ И ВИШЕ

„ИНТЕРНО“

УСЛОВИ ЗА ИЗДАВАЊЕ БЕЗБЕДНОСНОГ СЕРТИФИКАТА

- **физичко лице**
  - држављанство Републике Србије;
  - пунолетство;
  - пословну способност;
  - неосуђиваност за кривично дело за које се гони по службеној дужности, односно за прекршај предвиђен овим законом;
  - постојање одговарајуће безбедносне провере (осим у случајевима када то није предвиђено чл. 37 и 38. став 1.);
- **правно лице**
  - регистровано седиште на територији Републике Србије;
  - обављање делатности у вези са интересима из члана 8. овог закона;
  - постојање одговарајуће безбедносне провере;
  - ако није у поступку ликвидације или стечаја;
  - није кажњавано мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мере безбедности забране обављања одређених регистрованих делатности или послова;
  - уредно измирење пореских обавеза и доприноса;
- **страно физичко и правно лице**
  - поседовање одговарајућег сигурносног сертификата издатог од стране државе чији је држављанин, односно у којој правно лице има седиште или од стране међународне организације чији је члан.

Приступ тајним подацима- изузетно:

- Уз привремени сертификат који издаје Канцеларија Савета (чл. 64 ЗТПа)
- Изузетно приступ физичким и правним лицима која поседују сертификат непосредно вишем степену тајности (чл. 42 ЗТП) уз потписивање посебне изјаве и одлуку надлежног старешине органа...

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

1. На основу одлуке председника Републике, Владе, старешине органа јавне власти...
2. На основу законског овлашћења, описа радног места и конкретне ситуације...

Имају само за лица која:

- 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.		ИНТЕРНО		ДА
2.		ДРЖАВНА ТАЈНА		ДА
3.		СТРОГО ПОВЕРЉИВО		ДА
4.		ДРЖАВНА ТАЈНА		ДА
5.		ПОВЕРЉИВО		ДА
6.		ИНТЕРНО		ДА
7.		ПОВЕРЉИВО		ДА

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!

БЕЗБЕДНОСНИ СЕРТИФИКАТ
-за физичка лица-

Република Србија

Канцеларија Савета за националну безбедност и заштиту тајних података

СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА СТЕПЕНА

ДРЖАВНА ТАЈНА

Број сертификата ЈМБГ

Име и презиме

Назив органа јавне власти или правног лица

Датум издавања Важи до

М.П. Директор

ОВАЈ СЕРТИФИКАТ ИЗДАЈЕ СЕ У СКЛАДУ СА ЧЛАНОМ 87. ЗАКОНА О ТАЈНОСТИ ПОДАТАКА ("СЛУЖБЕНИ ГЛАСНИК РС" БРОЈ 104/09) И ИМАЛАЦ ОВОГ СЕРТИФИКАТА ИМА ПРАВО ПРИСТУПА ПОДАЦИМА СТЕПЕНА ТАЈНОСТИ "ДРЖАВНА ТАЈНА" ПРИ ОБАВЉАЊУ ДУЖНОСТИ У ОКВИРУ РАДНИХ ЗАДАТАКА.

ИМАЛАЦ ОВОГ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА УПОЗНАТ ЈЕ СА ЗАКОНОМ И ДРУГИМ ПРОПИСИМА КОЈИМА СЕ УРЕЂУЈЕ ТАЈНОСТ ПОДАТАКА И ОБАВЕЗАН ЈЕ ДА ТАЈНЕ ПОДАТКЕ КОРИСТИ У СКЛАДУ СА ТИМ ПРОПИСИМА

ПОТПИС КОРИСНИКА СЕРТИФИКАТА

Република Србија

Канцеларија Савета за националну безбедност и заштиту тајних података

СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА СТЕПЕНА

СТРОГО ПОВЕРЉИВО

Број сертификата ЈМБГ

Име и презиме

Назив органа јавне власти или правног лица

Датум издавања Важи до

М.П. Директор

ОВАЈ СЕРТИФИКАТ ИЗДАЈЕ СЕ У СКЛАДУ СА ЧЛАНОМ 87. ЗАКОНА О ТАЈНОСТИ ПОДАТАКА ("СЛУЖБЕНИ ГЛАСНИК РС" БРОЈ 104/09) И ИМАЛАЦ ОВОГ СЕРТИФИКАТА ИМА ПРАВО ПРИСТУПА ПОДАЦИМА СТЕПЕНА ТАЈНОСТИ "СТРОГО ПОВЕРЉИВО" ПРИ ОБАВЉАЊУ ДУЖНОСТИ У ОКВИРУ РАДНИХ ЗАДАТАКА.

ИМАЛАЦ ОВОГ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА УПОЗНАТ ЈЕ СА ЗАКОНОМ И ДРУГИМ ПРОПИСИМА КОЈИМА СЕ УРЕЂУЈЕ ТАЈНОСТ ПОДАТАКА И ОБАВЕЗАН ЈЕ ДА ТАЈНЕ ПОДАТКЕ КОРИСТИ У СКЛАДУ СА ТИМ ПРОПИСИМА

ПОТПИС КОРИСНИКА СЕРТИФИКАТА

Република Србија

Канцеларија Савета за националну безбедност и заштиту тајних података

СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА СТЕПЕНА

ПОВЕРЉИВО

Број сертификата ЈМБГ

Име и презиме

Назив органа јавне власти или правног лица

Датум издавања Важи до

М.П. Директор

ОВАЈ СЕРТИФИКАТ ИЗДАЈЕ СЕ У СКЛАДУ СА ЧЛАНОМ 87. ЗАКОНА О ТАЈНОСТИ ПОДАТАКА ("СЛУЖБЕНИ ГЛАСНИК РС" БРОЈ 104/09) И ИМАЛАЦ ОВОГ СЕРТИФИКАТА ИМА ПРАВО ПРИСТУПА ПОДАЦИМА СТЕПЕНА ТАЈНОСТИ "ПОВЕРЉИВО" ПРИ ОБАВЉАЊУ ДУЖНОСТИ У ОКВИРУ РАДНИХ ЗАДАТАКА.

ИМАЛАЦ ОВОГ СЕРТИФИКАТА ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА УПОЗНАТ ЈЕ СА ЗАКОНОМ И ДРУГИМ ПРОПИСИМА КОЈИМА СЕ УРЕЂУЈЕ ТАЈНОСТ ПОДАТАКА И ОБАВЕЗАН ЈЕ ДА ТАЈНЕ ПОДАТКЕ КОРИСТИ У СКЛАДУ СА ТИМ ПРОПИСИМА

ПОТПИС КОРИСНИКА СЕРТИФИКАТА

БЕЗБЕДНОСНИ СЕРТИФИКАТИ

ИНДУСТРИЈСКА БЕЗБЕДНОСТ

Представља мулти-дисциплинаран приступ заштити тајних података који се уступају компанијама.

Представља примену мера ради обезбеђења заштите тајних података, од стране извођача или подизвођача, у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора.

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 обавежу 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.

ОСНОВНИ БЕЗБЕДНОСНИ УПИТНИК ЗА ПРАВНА ЛИЦА

1. назив фирме и седиште, као и претходни називи фирми и седишта;
2. матични број правног лица и пореско-идентификациони број;
3. име и презиме заступника;
4. датум и место оснивања;
5. подаци о организационим јединицама, огранцима, зависним друштвима и другим облицима повезивања;
6. порекло оснивачког капитала укључујући и промене у последње три године;
7. број запослених;
8. број запослених за које се тражи сертификат и врста послова које обављају;
9. подаци о осудама за кривично дело, привредни преступ и прекршај правног лица и одговорних лица у правном лицу, као и подаци о поступцима за кривично дело, привредни преступ или прекршај против правног лица који су у току;
10. подаци о контактима са страним службама безбедности и обавештајним службама;
11. подаци о учешћу у активностима организације чије су активности и циљеви забрањени;
12. подаци о одговорности за повреду прописа који се односе на тајност података;
13. подаци о претходној безбедносној провери;
14. подаци о праву својине или другом стварном праву на непокретностима, подаци о праву својине на другим стварима уписаним у јавни регистар, као и податак о годишњем финансијском извештају за претходну годину у складу са законом којим се уређује рачуноводство и ревизија.

Уз попуњени упитник, заступник правног лица доставља и попуњени основни безбедносни упитник за физичка лица којима је предвиђен приступ тајним подацима.

УСЛОВИ ЗА ПОДНОШЕЊЕ ЗАХТЕВА ЗА ИЗДАВАЊЕ СЕРТИФИКАТА

1. има регистровано седиште на територији Републике Србије;
2. обавља делатност у вези са интересима утврђеним у члану 8. овог закона;
3. прође одговарајућу безбедносну проверу;
4. није у поступку ликвидације, односно стечаја;
5. није кажњен мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мера безбедности забране обављања одређених регистрованих делатности или послова;
6. уредно плаћа порезе, односно доприносе.

члан 8. ЗТП – податак који се може одредити као тајни

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 из става 1. овог члана 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.**

ОСНОВ ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА

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

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

УГОВОРНИ ОДНОС:

- Уговор о поверљивој набавци
- Уговор о пружању услуга на објектима који носе ознаку тајности
- Уговор о раду на пројектима од интереса за безбедност, одбрану, спољне послове...
- Уговор о пружању консултатских услуга, који подразумева упознавање са тајним подацима
- **Планирање одбране** - Уговорни однос на основу члана 82. став 2. у вези са чланом 65. Закона о одбрани (уговори са органима јавне власти)

НАПОМЕНА:

ПРАВНО ЛИЦА – у статусу органа јавне власти из члана 2. тачке 7. ЗТП:

- Мора имплементирати Закон о тајности података као орган јавне власти.
- Ова правна лица могу добити сертификат за правна лица само када је у питању међународна економска сарадња или учешће на страним тендерима....

ПОСТУПАК ИЗДАВАЊА СЕРТИФИКАТА ЗА ПРАВНА ЛИЦА

БЕЗБЕДНОСНЕ ПРОВЕРЕ ЗА ПРАВНА ЛИЦА

- 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

Напомена: ВБА не врши провере правних лица!

РЕПУБЛИКА СРБИЈА
КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ
БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

СЕРТИФИКАТ ЗА ПРИСТУП ТАЈНИМ ПОДАЦИМА ЗА ПРАВНО ЛИЦЕ

Канцеларија Савета за националну безбедност и заштиту тајних података, дана .....године, издаје.....(назив правног лица), са адресом.....(седиште правног лица), чији је законски заступник .....(име и презиме законског заступника правног лица), сертификат за приступ тајним подацима степена тајности ....., са роком важења .....(датум), у складу са одредбама Закона о тајности података.

Канцеларија Савета за националну безбедност и заштиту тајних података потврђује да правно лице:

* поседује капацитете за чување тајних података до степена тајности....., које предвиђају подзаконска акта и Закон о тајности података.

* не поседује капацитете за чување тајних података које предвиђају подзаконска акта и Закон о тајности података.

Број сертификата _____
Датум издавања _____

Директор

М.П.

_____

/потпис/

*Обрисати по потреби

СЛУЖБЕНЕ ЕВИДЕНЦИЈЕ ВЕЗАНЕ ЗА СЕРТИФИКАТЕ, БЕЗБЕДНОСНЕ ПРОВЕРЕ И ДОЗВОЛЕ ...

СЛУЖБЕНЕ ЕВИДЕНЦИЈЕ

Канцеларија Савета води:

- јединствену централну евиденцију издатих сертификата и дозвола,
- решења о издавању сертификата и дозвола,
- решења о одбијању издавања сертификата и дозвола,
- решења о продужењу важења сертификата и дозвола и
- решења о ограничењу или престанку важења сертификата и дозвола, као и
- потписане изјаве лица којима је издат сертификат, односно дозвола.

Канцеларија Савета чува захтеве за издавање сертификата, односно дозволе, безбедносне упитнике и извештаје о безбедносној провери са препоруком.

Орган надлежан за вршење безбедносне провере из ЗТП (БИА, ВБА и МУП), води:

- евиденцију безбедносних провера и
- чува документа о безбедносној провери са примерком извештаја и препоруке.

Подаци из безбедносне провере могу се користити само за намене за које су прикупљени.

Руковалац тајним подацима (члан 34 ЗТП-а), води евиденцију корисника тајних података у органу јавне власти за који је задужен. Поред тога, потребно је да има евиденције издатих сертификата, као и размене тајних података (+ страних тајних података). Све то се исказује у годишњем извештају о раду са тајним подацима који се прослеђује Канцеларији СНБиЗТП.

Примена прописа о заштити података о личности

У податке из своје безбедносне провере, прикупљене у складу са овим законом, лице има право увида и друга права на основу увида у складу са законом који уређује заштиту података о личности, изузев у податке који би открили методе и поступке коришћене у прикупљању података, као и идентификовали изворе података из безбедносне провере.

ПРОБЛЕМ УПУТСТВА О ЧУВАЊУ ТАЈНИХ ПОДАТАКА (ДЕБРИФИНГА) ИЛИ ПРЕСТАНАК ПОТРЕБЕ ПРИСТУПА ТАЈНИМ ПОДАЦИМА

ДЕБРИФИНГ

Проблем у пракси:

ЗТП не предвиђа шта се дешава са физичким и правним лицима којима је престала потреба за приступ тајним подацима.

У ЗТП је јасно уређен начин престанка тајности, опозив тајности и одобрење за изношење тајних података....

За физичка лица најчешћа ситуација је престанак радног односа због:

- одласка у пензију;
- проглашења технолошким вишком, стечаја и ликвидације
- отказа (скривљеног или добровољног);
- промене радног места.

У том случају послодавац одузима сертификат...

Поред ових околности, постоје и следеће:

- Покретање кривичног и дисциплинског поступка;
- Промене здравственог стања;
- Постојање околности које омогућавају ускраћивање приступа тајним подацима (без губитка сертификата);
- Укидање безбедносног сертификата.

За правна лица и запослене у њима, карактеристични су:

- Завршетак реализације поверљивог уговора;
- Раскид поверљивог уговора;
- Стечај;
- ЛИКВИДАЦИЈА - Престанак постојања правног лица.

Отворено питање у пракси је како поступа руковалац тајних података у органу јавне власти од кога потичу тајни подаци?

КОНСТАТАЦИЈА:

Физичка и правна лица и по престанку потребе за приступом тајним подацима по различитим основама, имају обавезу чувања тајних података, на основу ЗТП-а.

Ова обавеза престаје уколико:

- престане ознака тајности на основу ЗТП или
- орган јавне власти скине ознаку тајности

Изузетно, за потребе судских и дугих поступака, физичко лице може износити тајне податке, али само уз писмено одобрење старешине органа јавне власти!

ПРЕПОРУКА:

ЗА ФИЗИЧКА ЛИЦА КОЈИМА ЈЕ ПРЕСТАЛА ПОТРЕБА ПРИСТУПА ТАЈНИМ ПОДАЦИМА ПОТРЕБНО ЈЕ ИЗРАДИТИ ПОСЕБНО УПУТСТВО О ЧУВАЊУ ТАЈНИХ ПОДАТАКА И УЗЕТИ ИМ ИЗЈАВЕ НА ТЕ ОКОЛНОСТИ У ПИСАНОЈ ФОРМИ.

ПРЕСТАНАК РАДНОГ ИЛИ УГОВОРНОГ ОДНОСА НЕ АБОЛИРА ОД КРИВИЧНЕ ОДГОВОРНОСТИ ФИЗИЧКО ЛИЦЕ КОЈЕ ЈЕ ИМАЛО ПРИСТУП ТАЈНИМ ПОДАЦИМА, БИЛО ДА ЈЕ УРЕЂЕН ДЕБРИФИНГ, БИЛО ДА НИЈЕ....

КРИВИЧНО ДЕЛО И ПРЕКРШАЈИ ПО ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

Чл. 98 и 99 ...

КОМПРОМИТАЦИЈА ТАЈНИХ ПОДАТАКА

- Ненамеран неовлашћени приступ и коришћење
- Неовлашћена употреба базе тајних података
- Проблем идентификације и чувања података
- Нестручно и немарно руковање техником и подацима
- Губитак носача података
- Инсајдерске активности
- Шпијунажа, диверзија, хактивизам…
- Сајбер криминал, организовани криминал…

ОБЛИЦИ ОДГОВОРНОСТИ

- Кривично правна
- Прекршајна
- Радно правна и дисциплинска
- Облигационо правна (за накнаду штете)
- Морална(???)

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.

ПРЕКРШАЈ

Новчана казна у износу од 5.000 до 50.000 динара ако:

1) податак и документ који се очигледно не односе на заштићене интересе, означи као тајне;
2) овлашћење за одређивање тајности података пренесе на треће лице;
3) означи тајне податке садржане у документу неодговарајућим степеном тајности;
4) донесе одлуку о одређивању тајности податка без образложења;
5) не опозове тајност податка после наступања датума или догађаја после кога престаје тајност податка;
6) не опозове тајност податка после истека законског рока за престанак тајности податка;
7) не спроведе периодичну процену тајности податка;
8) не опозове тајност податка на основу решења Повереника за информације од јавног значаја и заштиту података о личности или одлуке надлежног суда;
9) промени степен тајности документа супротно одредби члана 27. закона;

10) пропусти да органе јавне власти обавести о промени степена тајности;
11) не пропише, организује и надзире опште и посебне мере заштите тајних података који одговарају степену њихове тајности;
12) лицу коме је издат сертификат за приступ тајним подацима не да на потписивање изјаву;
13) тајне податке достави правним и физичким лицима супротно одредби закона;
14) не води евиденцију решења о сертификату за приступ тајним подацима;
15) решење за приступ тајним подацима не чува у посебном делу досијеа;
16) не организује унутрашњу контролу над заштитом тајних података;
17) не предузме мере да се образује, води и обезбеђује посебан регистар страних тајних података.

ЗАКЉУЧАК РАЗМАТРАЊА

СЕРТИФИКАТИ ЗА ФИЗИЧКА ЛИЦА

Од оснивања Канцеларије Савета издато је 12419 безбедносних сертификата физичким лицима за приступ националним тајним подацима

	ДРЖАВНА ТАЈНА	СТРОГО ПОВЕРЉИВО	ПОВЕРЉИВО	УКУПНО
2011	25	13	3	41
2012	37	86	3	126
2013	35	15	17	67
2014	43	45	10	98
2015	126	131	186	443
2016	65	212	200	477
2017	121	181	296	598
2018	104	280	200	584
2019	109	458	371	938
2020	146	432	119	697
2021	433	852	305	1590
2022	488	4505	1767	6760
УКУПНО	1732	7210	3477	12419

У периоду од 2009. до 2023. године, на основу безбедносних сертификата, издато је 387 НАТО и ЕУ потврда, за физичка лица.

СЕРИФИКАТИ ЗА ПРАВНА ЛИЦА

Од оснивања Канцеларије Савета издато је 331 безбедносних сертификата за приступ националним тајним подацима ПРАВНИМ ЛИЦИМА.

	ДРЖАВНА ТАЈНА	СТРОГО ПОВЕРЉИВО	ПОВЕРЉИВО	ИНТЕРНО	УКУПНО
2015	0	2	50	0	52
2016	0	4	73	0	77
2017	2	7	27	0	35
2018	2	11	23		36
2019	1	3	2	0	6
2020	3	7	7	1	18
2021	1	17	23	1	42
2022	1	22	20	0	43
2023	0	10	21	0	31
УКУПНО	10	73	226	2	331

Приликом обављања безбедносних провера и процена, односно вођења поступака издавања сертификата, задире се у област обраде података о личности (тежишно приватности) за потребе националне безбедности, одбране, унутрашњих и спољних послова, вођење судских поступака и слично, тако да то може представљати највећи проблем у пракси код обраде података о личности са пристанком, дефинисање односа нормирано стање – дискрециона процена надлежног органа.

“ПРИСТУП ТАЈНИМ ПОДАЦИМА БЕЗ ОДГОВАРАЈУЋЕГ СЕРТИФИКАТА И ПРОЦЕДУРЕ ПРЕДСТАВЉА КРИВИЧНО ДЕЛО ИЛИ ПРЕКРШАЈ ...”

КОНСТАТАЦИЈА:

НЕ ПОСТОЈИ САВРШЕНА ЗАШТИТА ТАЈНИХ ПОДАТАКА И ИНФОРМАЦИЈА!

“ЧОВЕК ЈЕ УВЕК НАЈСЛАБИЈА КАРИКА СВАКОГА СИСТЕМА ...”

О АУТОРУ

Проф. др Горан Матић

Директор Канцеларије Савета за националну безбедност и заштиту тајних података Републике Србије, ванредни професор за област безбедност Универзитета УНИОН – „НИКОЛА ТЕСЛА'' и стални судски вештак за безбедност информација.

Учествовао је у процесу израде предлога више закона, Стратегије за супротстављање и борбу против тероризма, Стратегије националне безбедности и Стратегије одбране и у раду Радних група Владе Републике Србије за имплементацију акционих планова за поглавља 10, 24 и 31 за приступање Републике Србије ЕУ.

Од 2015. до 2019. године руководио је Сталном мешовитом радном групом за борбу против тероризма (СМРГ) – формиране одлуком Бироа за координацију рада служби безбедности, од 2019/2021. године обављао и дужност заменика националног координатора Националног координационог тела (НКТ) за спречавање и борбу против тероризма Републике Србије.

У оквиру међународне сарадње Републике Србије на плану заштите тајности података учествовао је као шеф делегације у преговорима за потписивање 14 међународних споразума и био потписник више споразума које је Р. Србија потписала са међународним телима и страним државама у области заштите тајних података. Такође, са Мисијом ОЕБС-а у Београду учествовао је у више пројеката око заштите тајних података, сајбер безбедности и обраде и заштите личних података у сектору безбедности и одбране.

Од 2012. године учествује у раду Форума директора националних безбедносних органа за заштиту тајних података земаља Југоисточне Европе (СЕЕНСА), као и у оквиру Иницијативе „6С'' која окупља директоре националних безбедносних органа земаља региона.

Аутор је више објављених научних и стручних радова и учесник више научних конференција, као и научне монографије „Политички деликти – атентат и побуна'' и коаутор књиге „Тактика и методика деловања обавештајно-безбедносних служби'' у издању Медија центра Одбрана у Београду, и „Основи безбедности'' у издању Факултета за пословне студије и право у Београд

Предавач је на основним академским студијама Војне академије Универзитета одбране и на Факултету за пословне студије и право Универзитета Никола Тесла Унион у Београду.

Гостујући је предавач на Факултету безбедности и Факултету организационих наука Универзитета у Београду, као и на Криминалистичко-полицијском универзитету, Академији за националну безбедност и на Високим студијама безбедности и одбране при Универзитету одбране у Београду. Поред тога предавач је на кратким струковним

студијама на Факултету безбедности: "Заштита тајних података и пословне тајне" и "Заштита личних података" од 2022. године. Био је гостујући предавач на мастер студијама Универзитета у Београду – Тероризам, организовани криминал и безбедност до 2024. године

Акредитовани је предавач Националне академије за јавну управу. Учествује је у раду посебних стручних тела те институције, и то као члан Сталне програмске комисије за електронску управу и дигитализацију (2022-2023) и Сталне програмске комисије за јавну управу (2023-2024).

Члан је Испитне комисије за државни испит (високо образовање) државних службеника и за комуналне милиционере у оквиру министарства државне управе и локалне самоуправе.

Председник је Савета „САМКБ – Српске асоцијације менаџера корпоративне безбедности'' у Београду; члан удружења „ИТ вештак'' у Београду и „Удружења за међународно кривично право'' у Београду. У Привредној комори Србије и Привредној комори Београда више година изводи едукације на тему корпоративне безбедности и обраде и заштите података.

ЛИТЕРАТУРА

nsa.gov.rs

Примена-закона-о-тајности-података.pdf (cups.rs)

Закон о тајности података: 104/2009-13 (pravno-informacioni-sistem.rs)