



ПРОЦЕНА ПРЕТЊЕ ЗА БЕЗБЕДНОСТ ТАЈНОГ ПОДАТКА ИЛИ САМОПРОЦЕНА ПО ЗАКОНУ О ИНСПЕКЦИЈСКОМ НАДЗОРУ И ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

Процена претње за безбедност тајног податка (самопроцена) по Закону о тајности података представља безбедносну процену која се примењује у раду са тајним подацима.

Она обухвата:

- Анализу и процену мера безбедности
- Идентификацију ризика
- Усаглашеност са прописима

Органи јавне власти дужни су да редовно извршавају Процену претње за безбедност тајног податка (самопроцену) ради осигурања безбедног поступања са тајним подацима. За спровођење самопроцене или процене претње за безбедност тајног податка **одговоран је старешина органа јавне власти**. Он има кључну улогу у иницирању и надгледању процеса самопроцене.

Разлика између Процене претње за безбедност тајног податка код одређивања мера заштите тајних података (члан 30. Закона о тајности података) и Процене могуће штете по интересе Републике Србије код одређивања степена тајности података (члан 10, став 3. Закона о тајности података):

Критеријум	Процена претње	Процена могуће штете
Фокус	Анализа ризика и безбедносних мера	Потенцијалне последице откривања тајних података по интересе државе
Сврха	Заштита података, предузимање мера за безбедност	Процењивање последица по безбедност, одбрану, спољне односе
Кључне активности	Оценити могућности заштите података	Проценити утицај на националну безбедност и однос са другим земљама

Ова разлика између процена из члана 30. и члана 10. став 3. закона лежи у фокусу и сврси процене. Процена претње за безбедност тајног податка обухвата анализу ризика и безбедносних мера, као и могућности заштите података. Са друге стране, процена могуће штете разматра потенцијалне последице откривања тајних података по интересе државе, као што су безбедност, одбрана и спољни односи.



ПРОЦЕНА ПРЕТЊЕ ЗА БЕЗБЕДНОСТ ТАЈНОГ ПОДАТКА ИЛИ САМОПРОЦЕНА ПО ЗАКОНУ О ИНСПЕКЦИЈСКОМ НАДЗОРУ И ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

Ко спроводи процену претње за безбедност тајног податка или самопроцену?

- Старешина органа јавне власти може да одреди:
 - о **Запосленог или групу запослених** са стручним знањем који ће директно бити задужени за спровођење самопроцене.
 - о **Комисију** која укључује представнике различитих организационих јединица ради свеобухватног приступа процени.

Кључни критеријуми за процену претње - Према члану 30. Закона о тајности података, процена се заснива на следећим критеријумима:

1. **Степен тајности** – одређује ниво заштите.
2. **Природа документа** – анализира се садржај документа.
3. **Процена претњи** – идентификују се извори ризика и предлажу мере смањења.

Руководилац тајних података има важну улогу у:

- Оперативном управљању подацима у складу са законом.
- Праћењу примене безбедносних мера заштите података.
- Обезбеђивању исправности и комплетности документације.

Док је руководиоца органа одговоран за спровођење процене, руководиоц тајних података често пружа техничку и оперативну подршку у оквиру овог процеса.

Унутрашња контрола - Према Члану 84. Закона о тајности података:

- има задатак да прати и проверава спровођење Процене претње за безбедност тајних података (самопроцене) и других безбедносних процедура.
- Она се фокусира на идентификацију могућих недостатака и предлаже корективне мере како би обезбедила усклађеност са прописима.

Одговорност за унутрашњу контролу има руководиоца органа јавне власти, а у одређеним органима јавне власти (нпр. министарства унутрашњих послова, одбране, или Безбедносно-информативна агенција), постоје посебно задужене организационе јединице за ове задатке.



ПРОЦЕНА ПРЕТЊЕ ЗА БЕЗБЕДНОСТ ТАЈНОГ ПОДАТКА ИЛИ САМОПРОЦЕНА ПО ЗАКОНУ О ИНСПЕКЦИЈСКОМ НАДЗОРУ И ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

Образовање и обука: Основни елементи заштите тајних података - представља кључну компоненту у изградњи свести запослених о заштити тајних података и развоју безбедносне културе:

1. **Разумевање процедура:** Обука доприноси бољем познавању и примени прописаних процедура у раду са тајним подацима.
2. **Умањење људских грешака:** Стечена знања и вештине омогућавају запосленима да:
 - о Препознају и избегну опасности.
 - о Адекватно реагују на претње.
 - о Осигурају исправно поступање са подацима.
3. **Спремност и одговорност:** Безбедносна активност подразумева:
 - о Спремност деловања у складу са усвојеним знањима, вештинама и вредносним ставовима.
 - о Препознавање претњи и реаговање на њих.
 - о Ангажовање надлежних органа у случају потребе.

Континуирана обука: Кључне области - укључују:

- **Рад са тајним подацима:** Разумевање безбедносних процедура.
- **Информациону културу и свест:** Праксе заштите информација и управљања ризицима.
- **Организациону безбедност:** Развој заједничких вредности и стандарда.
- **Сајбер хигијену:** Одржавање дигиталне безбедности кроз превенцију и заштиту система.

Значај и циљеви - доприносе заштити кључних вредности:

- Националне безбедности.
- Одбране и унутрашњих послова.
- Људских слобода и права.
- Поверљивости информација и података.



ПРОЦЕНА ПРЕТЊЕ ЗА БЕЗБЕДНОСТ ТАЈНОГ ПОДАТКА ИЛИ САМОПРОЦЕНА ПО ЗАКОНУ О ИНСПЕКЦИЈСКОМ НАДЗОРУ И ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

За едукације, обуке и тренинге у вези са применом Закона о тајности података надлежна је Канцеларија Савета за националну безбедност и заштиту тајних података.

Технолошка подршка - Употреба савремених технолошких алата као што су:

- Енкрипциони софтвери
- Системи за праћење

Ови алати омогућавају прецизнију идентификацију претњи. Усклађеност са међународним стандардима као што је **ISO/IEC 27001** доприноси успостављању најбољих пракси у примене мера информационе безбедности тајних података.

Самопроцена по Закону о инспекцијском надзору - Обухвата:

- Редовно праћење процедура
- Идентификацију неправилности
- Корекцију ако је потребно

Инспекцијски и стручни надзор - спроводе:

- Министарство правде – инспекцијски надзор.
- Канцеларија Савета за националну безбедност и заштиту тајних података (КСНБиЗТП) – стручни надзор који укључује:
 - о Контролу рада са тајним подацима.
 - о Унутрашњу контролу у складу са стандардима.



ПРОЦЕНА ПРЕТЊЕ ЗА БЕЗБЕДНОСТ ТАЈНОГ ПОДАТКА ИЛИ САМОПРОЦЕНА ПО ЗАКОНУ О ИНСПЕКЦИЈСКОМ НАДЗОРУ И ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

Примена у пракси:

Пример 1: Чување и обрада тајних података ("Строго поверљиво") Орган јавне власти који ради са документима у папирној форми открио је недостатке у примени мера физичке безбедности. **Мере корекције:**

- Инсталација видео-надзора.
- Ограничење приступа само овлашћеним лицима.
- Замена сефа вишим нивоом заштите.

Пример 2: Дигитална размена уз стране стандарде Органи јавне власти приликом спровођења мера информационе безбедности користе платформе са неактуелним протоколима. **Мере корекције:**

- Прелазак на платформе усклађене са најновијим међународним стандардима (нпр. ENISA препоруке).
- Обука службеника за правилно коришћење дигиталних алата.
- Континуирано праћење ефикасности система.
- Сарадња са међународним експертима за информациону безбедност.

Закључак

Процена претње за безбедност тајног податка или самопроцена није само идентификација неправилности, већ и континуиран процес унапређења. Комбинација редовне процене, обуке, технолошких решења, унутрашње контроле и надзора осигурава највиши ниво заштите.

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

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

web: www.nsa.gov.rs