ВОДИЧ ЗА ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНАТА СА ТАЈНИМ ПОДАЦИМА

веб: www.nsa.gov.rs

Проф.др Горан Д. Матић

Београд, 2025. година

Подизање безбедносне свести и културе са примарним и тежишним задатком заштите интереса Републике Србије који се односе на националну и јавну безбедност, унутрашње и спољне послове Републике Србије, одбрану, заштиту уставног поретка, као и људских и мањинских права!

САДРЖАЈ

УВОДНА РАЗМАТРАЊА

Водич за поступање у случају инцидента са тајним подацима представља кључни инструмент за адекватно управљање ситуацијама које угрожавају безбедност и интегритет заштићених података у оквиру органа јавне власти и правних лица. Овај водич је заснован на одредбама **Закона о тајности података** и **Закона о информационој безбедности**, као и на најбољим праксама из области заштите информација и тајних података, са циљем да пружи јасне смернице за откривање, управљање и извештавање о инцидентима који укључују тајне податке. Основна сврха овог водича је да омогући свим релевантним учесницима у процесу управљања инцидентима брзо, прецизно и правовремено реаговање у случају да дође до нарушавања безбедности тајних података. Водич дефинише конкретне кораке који треба да се предузму у сваком од етапа: од раног откривања инцидента и обавештавања надлежних органа, до поступања са угроженим тајним подацима и извештавања о последицама.

Закон о тајности података поставља основне принципе који регулишу начин одређивања и означавања тајности података, њихову заштиту и поступање у случају њиховог угрожавања и неовлашћеног коришћења. **Закон о информационој безбедности**, с друге стране, дефинише техничке и организационе мере које треба да буду примењене у циљу заштите информационих система и тајних података од неовлашћеног приступа, уништења или злоупотребе. У складу са овим прописима, водич обухвата све кључне аспекте процеса управљања инцидентима и обезбеђује усаглашеност са законским захтевима и међународним стандардима безбедности информација и тајних података. Поступање према овим смерницама омогућиће организацијама да убрзано идентификују и спрече даљу штету у случају инцидента, као и да осигурају поштовање права лица чији су подаци угрожени, у складу са прописима о тајним подацима, али и другим прописима. Осим тога, овај водич служи као основа за стално унапређење процеса заштите тајних података и повећање свести запослених о важности безбедности информација и тајних података.

У овом контексту, водич није само правни или технички документ, већ и алат који помаже организацијама да развију безбедносну културу и свест и дају конкретне смернице за сваког појединца који је одговоран за безбедност тајних података. Разматрање тренутних мера безбедности, идентификовање слабих тачака и усмеравање пажње на постојеће механизме заштите. Овај корак је кључан у контексту реаговања на инциденте, јер дозволава организацијама да процене своје тренутне капацитете и оперативну спремност за брзу и ефикасну реакцију. Процена такође подразумева ревизију постојећих норматива и процедура у складу са законом и најбољим безбедносним праксама.

Опис превентивних мера које организације треба да предузму како би минимизирале ризик од инцидената са тајним подацима. Ове мере обухватају увођење јасно дефинисаних процедура и правила за управљање тајним подацима, као и редовне безбедносне провере и ревизије. Такође, важно је осигурати да су сви запослени свесни важности заштите тајних података.

Нагласак на важности обуке и тренинга у контексту безбедности тајних података и одговорности свих запослених у организацији. Стална едукација запослених о процедурума поступања у случају инцидента, као и упознавање са новим претњама и техничким мерама безбедности, кључни су за превенцију и брзу реакцију. Свеобухватна обука такође помаже у стварању безбедносне културе и свести и поштовању прописа.

Разматрање нових типова инцидената, као што су сајбер напади и неовлашћени приступ, те како се они могу препознати. Овде је кључно и усмеравање система заштите на препознавање потенцијалних претњи у раним фазама. Такође, овај сегмент обухвата усвајање техника и технологија за брзо откривање инцидената који могу угрозити тајне податке. Опис улоге контроле и надзора у осигурању примене свих безбедносних мера, као и процеса ревизије. Одговорности су јасно дефинисане на свим нивоима организације, од менаџмента до оперативаца, како би се осигурала правовремена и адекватна реакција на инциденте. Контроле укључују и редовне интерне и екстерне ревизије система безбедности и складу са прописима.

Процедура за поступање у случају инцидента, која укључује правовремену комуникацију са јавности и медијима, али и са надлежним органима. Комуникација мора бити прецизна и у складу са законским захтевима, како би се смањила штета и очувала репутација организације. Овај сегмент такође обухвата активности које се предузимају како би се осигурала тајност података и правовременост у извештавању.

Поступање према смерницама из овог водича, као и усаглашавање са прописима о тајности података и стандардима националне безбедности, омогућиће органима јавне власти и правним лицима да адекватно управљају инцидентима и спрече потенцијалне штете. Стална едукација, надзор и усавршавање система заштите тајних података играју кључну улогу у минимизацији ризика и одржавању високих стандарда њихове заштите.

1. Безбедносни инцидент у раду са тајним подацима

Безбедносни инцидент је сваки догађај, радња или пропуст који је довео или може довести до неовлашћеног приступа, откривања, измене, уништења или губитка тајних података. Такође, инцидентом се сматра и свако одступање од прописаних мера заштите података, утврђених законом, подзаконским актима, безбедносним политикама и интерним процедурама. У случају постојања **сумње или сазнања** о следећим догађајима у вези са тајним подацима или страним тајним подацима:

- **губитак** (нпр. физичко одсуство документа или уређаја са подацима),
- **крађа** (нпр. неовлашћено преузимање од стране трећег лица),
- **оштећење** (нпр. физичко или логичко оштећење носача података),
- **уништење** (без спровођења прописане процедуре за уништавање),
- **неовлашћено откривање** (нпр. приступ или увид лица без одговарајућег степена овлашћења),

свако лице (запослени, сарадник, ангажовано лице), које дође до таквог сазнања, **дужно је да без одлагања** обавести старешину органа јавне власти, руковаоца тајних података или **овлашћено лице за заштиту тајних података у оквиру свог органа**.

Ова обавеза произилази из принципа **одговорности (accountability)** и **обавезе пријављивања безбедносног инцидента**, у складу са чланом 35. и 36. Закона о тајности података.

Карактеристике безбедносног инцидента:

- Може бити **намерног** (злонамерне радње) или **ненамерног** карактера (нехат, немар).
- Увек представља **одступање од прописаних правила** заштите тајних података.
- Може имати **правне последице** као прекршај или кривично дело, у зависности од тежине и последица.

Примери безбедносних инцидената:

- Увид неовлашћених лица у документе са тајним подацима.
- Разговор о тајним подацима у необезбеђеном простору или преко несигурне комуникације.
- Губитак или крађа уређаја (нпр. USB, лаптоп) са тајним садржајем.
- Слање тајних података без криптографске заштите.
- Неовлашћено копирање, умножавање или уништавање тајног податка.

Компромитација штићених података у најширем смислу (тајних података, личних података, банкарске тајне, пореске тајне, пословне и професионалне тајне) настаје када дође до неовлашћеног откривања, приступа, измене, уништења или губитка података, чиме се угрожава њихова поверљивост, интегритет или доступност. Такви догађаји могу проузроковати озбиљну штету по орган јавне власти, правно лице, организацију или појединца.

Облици компромитације

- 🔓 Откључан и ненадгледан сеф са поверљивим подацима
- 👁 Увид у податке од стране неовлашћених лица
- 📡 Небезбедан пренос поверљивих информација
- 🚪 Изношење ван заштићеног простора
- 🗑 Уништавање без прописане процедуре

Уобичајени узроци компромитације:

- Људска грешка, непажња или немар.
- Недовољна стручност и обука.
- Губитак носача података.
- Сајбер напади, шпијунажа, хактивизам.
- Злоупотреба приступа или база података.

Компромитација података (Data Breach): Инцидент у ком штићени или осетљиви подаци постају доступни, копирани, украдени или искоришћени од стране неовлашћених лица.

Најчешће угрожени штићени подаци, поред тајних података:

- Идентификациони и лични подаци
- Финансијске информације
- Медицинска документација
- Пословне тајне и интелектуална својина

Кључни узроци:

1. Пропусти у понашању и обуци особља
2. Злонамерни софтвер (нпр. рансомвер)
3. Недостатак физичке и друге заштите
4. Непоштовање безбедносних процедура

Компромитација тајних података – конкретни ризици:

1. **Ненамерни инциденти:**
   - Грешке у контроли приступа
   - Прекорачење принципа need to know
   - Технички пропусти у конфигурацији система
2. **Намерне злоупотребе:**
   - Шпијунажа, диверзије, корупција
   - Сајбер напади, крађа идентитета
   - Хактивизам и идеолошки мотивисане акције
3. **Техничке неправилности:**
   - Немар у руковању опремом или подацима
   - Губитак или крађа уређаја са осетљивим садржајем

2. Ко има обавезу обавештавања о инциденту у раду са тајним подацима?

У складу са чланом 35. став 3. Закона о тајности података и важећим интерним актима, **обавезу обавештавања у случају инцидента има свако лице које је на било који начин дошло у контакт са тајним подацима**, односно које је уочило или проузроковало повреду мера њихове заштите.

Обавезу обавештавања имају:

- ✓ **Сва запослена лица, ангажована лица и функционери** у органу јавне власти који рукује тајним подацима;
- ✓ **Лица која су вршила пренос, обраду или чување тајних података**, укључујући и случајеве када се податак налазио ван службених просторија или информационог система органа;
- ✓ **Лице задужено за физичко, логичко или организационо обезбеђење тајних података**, ако је уочило повреду мера;
- ✓ **Руковалац тајних података или овлашћено лице за заштиту тајних података у правном лицу**, уколико му је инцидент пријављен или га је само открило.

Посебно:

- Уколико је тајни податак **преношен ван просторија органа**, лице које га је преносило има **обавезу да одмах обавести овлашћено лице или старешину органа**, као и орган јавне власти од којег је податак потекао

(изворни орган), без обзира на степен штете или привидну безначајност инцидента.

Напомена: Ова обавеза обавештавања је **неодложна и непосредна**. Одлагање или прикривање инцидента може се сматрати тежом повредом радне обавезе, а у одређеним случајевима и основом за покретање прекршајног или кривичног поступка.

Принципи одговорности: - Одговорност за поступање је распоређена на свим нивоима управљања, уз обавезно поштовање следећих принципа:

- **Need to know** (*„потреба за знањем“*) – приступ тајним подацима дозвољен је искључиво лицима којима су ти подаци неопходни за обављање конкретних послова, односно задатака у оквиру овлашћених надлежности.

Accountability (*„одговорност и праћење поступања“*) – свако лице које рукује тајним подацима мора бити у потпуности одговорно за своје поступке у вези са тим подацима, а орган је у обавези да обезбеди систем надзора, праћења и евидентирања активности.

3. Класификација инцидената у систему заштите тајних података

Сагласно одредбама Закона о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона:

1. Повреда радне дисциплине (Дисциплинска одговорност): Инцидент који **не доводи до компромитације тајних података**, али представља **незаконито или несавесно поступање у вршењу службене дужности**, као што су:

- непоштовање прописаних процедура за руковање тајним подацима,
- немар у примени мера физичке, техничке или организационе заштите,
- непријављивање губитка документа или уређаја са тајним подацима,
- приступ тајним подацима без потребе засноване на службеној функцији („потреба да се зна“).

➞ **Правни основ**:

- **Закон о државним службеницима**, чл. 107–109: теже повреде службене дужности.
- **Закон о раду**, чл. 179: разлози за отказ уговора о раду.
- **Закон о Војсци Србије**, чл. 145-170.: дисциплински грешке и преступи професионалних припадника Војске Србије.
- **ПЗакон о полицији**, чл. 202–217: лаке и тешке повреде службене дужности.

➞ **Санкције**: дисциплински поступак, мера упозорења, смањење плате, премештај, разрешење или отказ.

2. Прекршај (Прекршајна одговорност): Инцидент који **није довео до компромитације тајних података**, али указује на **пропусте у примени прописаних мера заштите**, као што су:

- неправилно означавање степена тајности података (члан 11, став 2),
- изостанак образложења о одређивању тајности (члан 11, став 4),
- непредузимање прописаних мера заштите од стране руковаоца тајних података (члан 34),
- одсуство унутрашње контроле и процене ризика (чланови 22, 84),
- достављање података неовлашћеним субјектима без компромитације самог садржаја (члан 46).

➞ **Прекршајна одговорност** сноси се у складу са члановима **99. и 100.** Закона, и новчана казна износи **од 5.000 до 50.000 динара**.

3. Кривично дело (Кривична одговорност): Инцидент који је **довео или могао довести до компромитације тајних података**, укључујући:

- неовлашћено саопштавање, предаја или омогућавање приступа тајним подацима,
- губитак, уништење или откривање докумената који садрже тајне податке,
- прибављање тајних података без одобрења.

➞ У складу са чланом **98. Закона**, кривично дело се квалификује према ознаци тајности података:

- За „ИНТЕРНО“ или „ПОВЕРЉИВО“ → **затвор од 3 месеца до 3 године**
- За „СТРОГО ПОВЕРЉИВО“ → **затвор од 6 месеци до 5 година**

- За „ДРЖАВНА ТАЈНА“ → **затвор од 1 до 10 година**

У тежим облицима (из користољубља, у иностранству, у ратном стању), казне се крећу до **15 година затвора**.

За **дела из нехата**, законом су прописане блаже санкције — у распону од **новчаних казни до пет година затвора**, у зависности од степена тајности података.

4. Процена околности настанка инцидента у раду са тајним и његова правна квалификација

Процена околности настанка безбедносног инцидента у раду са тајним подацима, као и његова правна квалификација, један је од најважнијих корака у обради и одређивању даљег поступања у складу са прописима. У зависности од врсте инцидента, различито ће се реаговати надлежни органи и применити одговарајући правни механизми. Ова процена има велике правне и безбедносне импликације, јер погрешна квалификација може довести до пропуста у поступању, што може имати озбиљне последице по безбедност и правни систем.

1. **Тип инцидента**: Прва ствар коју треба размотрити је сам тип инцидента. У питању могу бити:
    - **Повреда радне дисциплине** – када је инцидент изазван нехатом или нестручним радом, али без намере или озбиљних последица по безбедност података.
    - **Прекршај** – ако су прекршени прописани правни или технички оквири у раду са тајним подацима, али не постоји директна намера да се угрози национална безбедност или сигурност.
    - **Кривично дело** – ако постоји намера или свесно кршење закона које резултира озбиљним последицама, као што је откривање, злоупотреба или неовлашћено откривање тајних података.
2. **Фактори који утичу на квалификацију**: Да би се правилно квалификовао инцидент, неопходно је узети у обзир неколико важних фактора:
    - **Тежина инцидента** – колика је штета настала и која је врста података угрожена? Ако је угрожен податак високог степена тајности (на пример, државна тајна), инцидент ће вероватно бити квалификован као озбиљан, могуће и као кривично дело.
    - **Намера починиоца** – да ли је инцидент настао због ненамерне грешке или због свесног деловања које је имало за циљ да се компромитују тајни подаци? Намера ће имати пресудну улогу у квалификацији инцидента.

- **Штета и ефекти инцидента** – која је стварна штета? Да ли је инцидент имао озбиљне последице по безбедност, интегритет или доступност података? Ако је настала озбиљна штета, као што је откривање државне тајне или компромитација безбедности, то може указивати на кривично дело.

3. **Поступци који следе у зависности од правне квалификације**:
   - **Повреда радне дисциплине**: Ако инцидент не резултира значајном штетом и ако није било свесне злоупотребе података, може се сматрати повредом радне дисциплине. У том случају, формира се посебна дисциплинска комисија која разматра одговорност појединца, а поступак се води у складу са прописима о радној дисциплини.
   - **Прекршај**: Ако су прекршени прописани закони и процедуре, али није дошло до озбиљне штете, инцидент може бити квалификован као прекршај. У том случају, пријава се упућује надлежном судији за прекршаје, који доноси одлуку о даљем поступку.
   - **Кривично дело**: Ако постоји основ сумње да је извршено кривично дело (нпр. свесно откривање тајних података или њихова злоупотреба), надлежни тужилац ће покренути истрагу у складу са Законником о кривичном поступку. У овом случају, поступак ће обухватити све радње које су потребне за доказивање кривичног дела, укључујући форензичке анализе и прикупљање доказа.

Процена утицаја и ризика од инцидента у раду са тајним подацима важан је корак у разумевању степена угрожавања који је наступио. То подразумева не само процену настанка материјалне штете, већ и потенцијалне последице по националну безбедност, права лица или организацију. Када се процењује да ли је инцидент могао имати међународне импликације, важно је узети у обзир степен осетљивости података, као и могућност да се повреда изазове преко граница.

Мере које треба предузети у случају инцидента - У зависности од квалификације инцидента, примењују се различите мере:

- **Блокада приступа**: За спречавање даљих оштећења, неопходно је ограничити приступ угроженим подацима и предузети техничке мере као што су lock-out и повлачење докумената.
- **Активирање containment мера**: Ове мере подразумевају брзу реакцију како би се инцидент изолово и спречило даље ширење оштећења.
- **Обавештавање надлежних органа**: Без одлагања треба обавестити Канцеларију СНБиЗТП, БИА, као и органе који су одговорни за информациону безбедност, у складу са прописима (нпр. GDPR, NIS2).

Правилна процена околности настанка инцидента и његова правна квалификација од суштинске су важности за успешну обраду инцидента у раду са тајним подацима. На основу прецизне процене, надлежни органи могу донети одговарајуће одлуке и применити адекватне правне поступке. Погрешна квалификација може довести до пропуста у заштити безбедности података и нарушавања правних процедура, што може имати озбиљне последице по организацију и друштво.

Јасно препознавање природе инцидента је од пресудног значаја за одређивање поступка који ће се применити. У зависности од тога да ли се ради о повреди радне дисциплине, прекршају или кривичном делу, поступак и одговорност надлежних органа се разликују. Важно је да сваки инцидент буде адекватно процењен како би се одредио прави правни оквир у којем ће се наставити поступак.

5. Поступање у случају инцидента са тајним подацима

Сваки инцидент који се односи на заштиту тајних података сматра се **безбедносним инцидентом високог ризика** и захтева **хитну, координисану и документовану реакцију**, у складу са Законом о тајности података („Сл. гласник РС“, бр. 72/2009).

Основне мере и обавезе поступања:

- **Хитна пријава и документација инцидента** руководиоцу органа јавне власти и надлежном руковаоцу тајних података или овлашћеном лицу у органу.
- **Састављање писаног извештаја о инциденту**, у складу са чланом 36. и 84. Закона о тајности података.
- **Спровођење унутрашње контроле**, са проценом узрока, степена ризика и евентуалне компромитације података.
- **Примена мера санације и заштите**, укључујући техничке, организационе и кадровске корективне мере.
- **Ревизија постојећих мера заштите** како би се спречило понављање инцидента.
- У зависности од карактера повреде, **покретање дисциплинског, прекршајног или кривичног поступка**, у складу са важећим прописима.

Напомена: Спровођење унутрашње контроле и израда извештаја су **обавезни** у свим случајевима – **без обзира на тежину последица** инцидента. Извештај мора да садржи:

- опис инцидента,
- анализу узрока и последица,
- процену ризика по безбедност података,
- предложене предузете мере заштите и превенције, као и покренутих дисциплинских, прекршајних или кривичних поступака.

Овим се осигурава да сваки инцидент буде третитан на озбиљан, законит и системски начин, уз документовано праћење и извештавање, што је основа за ефикасну заштиту тајних података и јачање безбедносне културе у организацији.

Улога овлашћеног лица или старешине органа - Надлежно овлашћено лице или старешина органа има кључну улогу у управљању безбедносним инцидентима који укључују тајне податке. Њихова одговорност није само да се одмах реагује на инцидент, већ и да се осигура да се предузму све мере које ће спречити поновно дешавање сличних инцидената у будућности. У складу са Законом о тајности података, као и Законом о информационој безбедности, улога ових лица укључује неколико основних корака који су неопходни да се адекватно поступи у случају безбедносног инцидента.

1. Утврђивање свих релевантних чињеница - Надлежно овлашћено лице или старешина органа има обавезу да у сарадњи са релевантним стручним тимовима, као што су стручњаци за безбедност информација и правници, утврди све околности које су довеле до инцидента. Ово подразумева детаљно истраживање који су фактори изазвали инцидент и који су били његови главни узроци. Поступак утврђивања чињеница треба бити систематичан и укључивати све аспекте инцидента, од техничких до људских фактора.

Пример: Ако је дошло до неовлашћеног приступа тајним подацима, овлашћено лице мора утврдити како је до тога дошло — да ли је у питању људска грешка, техничка манипулација, или намерна злоупотреба.

2. Процена степена и врсте штете - После утврђивања чињеница, овлашћено лице је дужно да процени степен и врсту штете коју је инцидент проузроковао. Ова процена мора обухватити не само непосредну материјалну штету (нпр. уништене или компромитоване податке), већ и дугорочне последице по националну безбедност, интегритет система, и могуће међународне импликације. Степен штете може варирати од локализоване штете која не угрожава безбедност земље, до већих безбедносних претњи које захтевају хитне мере.

Пример: Ако је инцидент подразумевао излагање државних тајни које би могле бити искоришћене од стране страних влада или агенција, процена штете укључује ризике од ескалације међународних сукоба или дипломатских последица.

3. Предузимање хитних мера ради ублажавања последица - Надлежно овлашћено лице или старешина органа мора одмах предузети све хитне мере које су неопходне да се ублаже последице инцидента. Ово укључује техничке и оперативне кораке, као што су блокирање приступа угроженим подацима, поновно обезбеђивање приступа подацима који нису угрожени, као и обустављање активности које су допринеле инциденту. Овакве мере су од пресудне важности да би се смањила могућа штета и да се спречи даље ширење инцидента.

Пример: Ако је дошло до напада на информациони систем, хитне мере могу укључивати онемогућавање даљег приступа систему, изолацију угрожених делова мреже, као и опоравак са резервних копија.

4. Иницирање мера за спречавање понављања инцидента - Један од најважнијих задатака овлашћеног лица је да иницира мере које ће спречити понављање сличних инцидената у будућности. Ове мере могу обухватати ревизију и унапређење безбедносних политика, техничких мера и процедура које су биле на снази пре инцидента. Такође, треба предузети кораке за едукацију и обуку запослених у вези са најновијим безбедносним ризицима и како да их избегну. Мере могу укључивати и промене у процесима, као и побољшање физичке и логичке безбедности.

Пример: Уколико је инцидент резултат људске грешке, треба организовати додатне обуке о управљању подацима и безбедносним процедурама како би се спречиле сличне грешке у будућности.

5. Извештавање Канцеларији Савета за националну безбедност и заштиту тајних података - Када је инцидент разјашњен и мере су предузете, овлашћено лице је дужно да обавести Канцеларију Савета за националну безбедност и заштиту тајних података о свим детаљима инцидента, мерама које су предузете и резултатима. Ова извештаја имају кључну улогу у координацији са другим државним органима и међународним партнерима, као и у спровођењу даљих мера ако је потребно.

Пример: Канцеларија СНБ треба бити обавештена о природи инцидента, предузетим мерама и било којим могућим правним или безбедносним последицама које су настале као резултат инцидента.

Уклањање последица безбедносног инцидента са тајним подацима и спречавање будућих инцидената захтева правовремено, организовано и координисано поступање од стране овлашћеног лица или старешине органа. Њихова одговорност је кључна за минимизирање штете, обезбеђивање даљег сигурног руковања тајним подацима и одржавање поверења у систем заштите

података. У складу са Законом о тајности података и другим релевантним прописима, ове мере морају бити строго примењене да би се обезбедила висока безбедност података и спречили потенцијални ризици по националну безбедност.

6. Препоручене мере — поступање по препоруци Канцеларије СНБиЗТП

У складу са чланом 35, став 3. Закона о тајности података, као и са општим принципима заштите тајних података, препоручене мере за поступање у случају безбедносног инцидента у вези са тајним подацима морају бити изведене са високим степеном пажње и у складу са прописаним правним и безбедносним процедурама. У наставку су детаљно објашњене све релевантне мере које треба предузети, као и поступак пријема и обраде инцидента:

1. Обавештавање органа јавне власти од којег потиче тајни податак - Када се утврди да је дошло до безбедносног инцидента који укључује тајне податке, први корак је обавештавање органа јавне власти од којег потиче тајни податак. Ово обавештење има за циљ да омогући правовремено реаговање и преузимање мера од стране надлежних органа, што укључује идентификацију и елиминацију узрока инцидента. Такође, орган који управља подацима мора бити обавештен како би могао да процени потенцијалне последице по безбедност података и њихову класификацију, као и да се пружи помоћ у одређивању степена угрожености.

Пример: Ако инцидент укључује тајне податке везане за одбрану или националну безбедност, орган који је задужен за тајне податке мора бити обавештен о свим детаљима, како би могао предузети кораке за даље поступање.

2. Покренути поступак унутрашње (ванредне) контроле - Покретање поступка унутрашње контроле представља обавезан корак у свим случајевима безбедносног инцидента. У складу са Законом о тајности података, одговорна лица у организацији морају покренути ванредну контролу која ће испитати све околности инцидента. Циљ ове контроле је да се утврди како је дошло до инцидента, који су фактори допринели његовом настанку, и да се идентификују сви недостаци у систему заштите података.

Пример: Ако је инцидент последица техничке грешке у систему заштите, истраживање ће обухватити анализу инцидента, форензичку анализу података и ревизију безбедносних мера које су биле на снази у том тренутку.

3. Обавештавање надлежног тужилаштва (ако постоји основана сумња на кривично дело) - У случају да током истраге инцидента постоји основана сумња да је извршено кривично дело (нпр. неовлашћено откривање тајних података, злоупотреба или други видови намерног кршења закона), надлежно тужилаштво

мора бити обавештено. Закон о тајности података и други релевантни прописи наложе на надлежне органе обавезу да, ако постоји кривично дело, поступе у складу са Законником о кривичном поступку, што подразумева покретање истраге и, ако је потребно, подношење кривичне пријаве.

Пример: Уколико се утврди да је неко свесно открио државну тајну или дистрибуирао осетљиве податке без дозволе, надлежно тужилаштво треба бити обавештено како би могло покренути поступак истраге.

4. Обавештавање Канцеларије СНБиЗТП - У складу са чланом 35 Закона о тајности података, сваки инцидент који укључује повреду безбедности тајних података мора бити одмах пријављен Канцеларији за безбедност националних података (СНБ). Канцеларија СНБ игра кључну улогу у координацији и надзору поступања у случају инцидента, обезбеђујући да све мере буду усклађене са националним и међународним стандардима заштите података. Обавештавање Канцеларије СНБ је такође важно за координацију са другим релевантним органима, као што су БИА и друге службе за безбедност.

Пример: Канцеларија СНБиЗТП треба бити обавештена када постоји било какво померање у статусу тајних података, као и када се утврди да је безбедност података угрожена.

5. По потреби, обавештавање Безбедносно-информативне агенције (БИА) - У ситуацијама када инцидент укључује потенцијалне претње по националну безбедност, као што су злоупотреба тајних података у политичким или безбедносним контекстима, обавештавање Безбедносно-информативне агенције (БИА) може бити неопходно. БИА има задатак да прати и анализира претње по безбедност земље, и може бити одговорна за спречавање даљих ризика по безбедност.

Пример: Ако је инцидент довео до излагања података који могу бити искоришћени од стране страних агенција, БИА треба бити обавештена да би се покренуле контрамере.

Препоручене мере поступања по препоруци Канцеларије СНБиЗТП представљају кључне кораке у осигурању да се сваки безбедносни инцидент у вези са тајним подацима адекватно обради. Правовремено обавештавање релевантних органа и предузимање мера унутрашње контроле обезбеђује да се спрече даље последице и да се одржи интегритет безбедносног система. Применом ових мера, организација може не само минимизирати ризике од потенцијалних штета, већ и бити у складу са законским и безбедносним захтевима који регулишу рад са тајним подацима.

Управљање инцидентима у вези са тајним подацима мора се заснивати на правовременој реакцији, правној и техничкој усклађености, као и култури безбедности на свим нивоима. Документовано поступање није само законска обавеза, већ и предуслов за очување поверења у институционални систем заштите тајних података Републике Србије.

7. Допринос организације настанку штетног догађаја у раду са тајним подацима

У систему заштите тајних података, одговорност за безбедно руковање подацима, документима и информацијама од значаја за националну безбедност, одбрану, спољне и унутрашње послове, као и вођење кривичних поступака (тајних података) не лежи искључиво на појединцима, већ превасходно на самој организацији – било да је реч о органу јавне власти или правном лицу коме је омогућен приступ тајним подацима на основу претходног поступка који се спроводи од стране органа јавне власти. Организација као целина може својим пропустима, неблаговременим поступањем или непотпуним применама прописаних мера директно или индиректно допринети настанку штетног догађаја, односно безбедносног инцидента који угрожава тајне податке.

1. Неуспостављање унутрашњег система заштите тајних података

Први и најчешћи облик доприноса организације настанку штетног догађаја јесте потпуно или делимично **неуспостављање система заштите тајних података у складу са Законом о тајности података** („Службени гласник РС“, бр. 104/2009). Овакав пропуст указује на институционални недостатак у разумевању или примени основних обавеза у области заштите података од значаја за безбедност, што озбиљно угрожава унутрашњу и спољну безбедносну позицију органа или правног лица.

Најчешћи облици овог пропуста укључују:

- ✕ **Непостојање интерног акта – Плана заштите тајних података**, који представља основни нормативни документ у коме се дефинишу унутрашње мере и одговорности заштите у конкретној институцији;
- ✕ **Непостављање руковаоца тајних података** (одговорног лица за руковођење системом заштите унутар организације), као ни **овлашћеног лица за заштиту тајних података**, што доводи до изостанка контроле над приступом и обрадом података;
- ✕ **Одсуство интерних процедура и упутстава** за пријем, обраду, евиденцију, чување, уништавање и пренос тајних података, што запослене оставља без јасних смерница у свакодневном раду;

- ❌ **Неодређивање и неуспостављање физичких и техничких услова** за безбедно складиштење, приступ и контролу тајних података (нпр. одговарајући простори, сигнализација, ормари, контролисан улаз, системи видео-надзора и приступних листа).

📌 **Последице ових пропуста** су системске природе – доводе до рањивости целе институције, омогућавају неовлашћен приступ подацима, а запослени остају **недовољно информисани и недовољно обучени за правилно поступање са подацима означеним степеном тајности**.

🔍 **Процена о постојању или непостојању система заштите тајних података** доноси се на основу **стручног надзора који, на захтев органа јавне власти, периодично спроводи Канцеларија Савета за националну безбедност и заштиту тајних података**, у складу са својим овлашћењима прописаним законом и подзаконским актима.

✅ Успостављање система мора бити документовано, проверљиво и усклађено са упутствима Канцеларије, укључујући и обавезу регистрације система заштите, редовног извештавања, као и едукације запослених о мерама и процедурама заштите.

2. Пропусти у превентивним и контролним мерама

Организација такође може допринети настанку инцидента **неспровођењем превентивних мера**, као што су:

- непостојање плана управљања ризицима;
- неизвршавање редовне процене безбедносних ризика;
- занемаривање безбедносне провере лица која приступају тајним подацима;
- изостанак унутрашње контроле и ревизије примене мера заштите;
- **употреба неакредитованих ИКТ система за обраду тајних података, односно системâ који нису прошли прописану процену и одобрење од стране надлежног органа** – што обухвата:
    - одсуство техничке и физичке изолације ИКТ система од јавних и интерних мрежа;
    - непостојање механизама за контролу приступа, регистрацију активности и чување евиденција;
    - непотпуну или недовољну примену криптографских мера заштите;
    - неправилну инсталацију или конфигурацију софтвера и оперативног система који се користе за рад са тајним подацима;

- занемаривање редовног ажурирања, техничког одржавања и праћења система;
- непостојање званичне одлуке о акредитацији ИКТ система од стране руководиоца органа, у складу са прописима Канцеларије Савета за националну безбедност и заштиту тајних података.

Овакви пропусти у ИКТ домену не само да представљају кршење законских обавеза, већ директно излажу тајне податке ризику од компромитовања, неовлашћеног приступа и губитка интегритета података.

3. Недовољна обученост запослених

Један од значајних индиректних доприноса организације настанку штетног догађаја јесте одсуство или неадекватност обуке запослених, нарочито лица која имају приступ тајним подацима или учествују у њиховој обради, чувању и преносу. Недовољна едукација и неспровођење редовних обука доводи до смањене свести о ризицима, неодговарајуће процене ситуација и непримене мера заштите.

Организација која не спроводи:

- ✓ **Обавезну почетну обуку новозапослених** – у складу са прописима, сва лица која добију сертификат за приступ тајним подацима морају пре почетка рада бити упозната са законским и подзаконским актима који уређују поступање са тајним подацима, као и са унутрашњим процедурама у оквиру органа;
- ✓ **Периодичне обуке и провере знања** – редовна обука је обавеза и инструмент за подсећање, надоградњу и проверу постојећих знања, укључујући и тестирање разумевања мера заштите, техничких поступака и правних оквира;
- ✓ **Симулације безбедносних инцидената и практичне вежбе поступања** – организовање сценарија и вежби које симулирају губитак, откривање или компромитацију тајних података доприноси способности запослених да брзо, исправно и усклађено реагују у реалним ситуацијама;
- ✓ **Специјализоване едукације у складу са нивоом приступа и одговорности** – Канцеларија СНБиЗТП организује основне, напредне и специјализоване програме за лица у органима јавне власти, одговорна лица, овлашћена лица за заштиту тајних података, као и администраторе ИКТ система који раде у оквиру заштићених зона;

- ✓ **Евиденцију и верификацију похађаних обука** – организација која не води евиденцију о обукама запослених, сертификатима и редовном усавршавању, губи могућност контроле компетенција и правовременог упућивања на обнову знања.

Одсуство ових облика едукације директно смањује способност запослених да препознају безбедносни ризик, адекватно поступе у случају сумње на компромитацију, или примене процедуре које би спречиле настанак већег штетног догађаја. Са друге стране, организације које системски улажу у **безбедносну културу**, кроз континуирану едукацију, смањују ризик од инцидената и повећавају степен усаглашености са законом.

У складу са чланом 82. Закона о тајности података („Службени гласник РС“, број 104/2009), орган јавне власти дужан је да води и чува евиденцију о лицима која су прошла обуку за рад са тајним подацима, као и о издатим сертификатима за приступ подацима одређеног степена тајности. Ова евиденција представља саставни део кадровског досијеа запослених и служи као доказ о испуњености услова за приступ и поступање са тајним подацима. Подаци из евиденције морају се чувати на безбедан начин, уз поштовање мера заштите тајних података и ограничен приступ, у складу са прописаним нивоом тајности. Недовољна или непостојећа евиденција указује на недостатке у систему заштите и ускраћује основу за интерну и спољну контролу поступања са подацима од значаја за безбедност.

4. Неадекватна реакција на безбедносни инцидент

Други критичан облик организационог пропуста односи се на **непостојање јасно дефинисане процедуре реаговања у случају инцидента са тајним подацима**. Без утврђених корака за идентификацију, пријаву, анализу и отклањање последица инцидента, чак и **наизглед мањи пропусти могу ескалирати у озбиљан безбедносни ризик**, са потенцијално далекосежним последицама по интересе Републике Србије.

Типични елементи неуспостављене или неефикасне процедуре обухватају:

- ✕ **Недефинисан појам безбедносног инцидента** – одсуство прецизних критеријума шта се у конкретној организацији сматра инцидентом у вези са тајним подацима;
- ✕ **Непостојање унутрашњег механизма за пријаву инцидента** – ко је одговоран да инцидент пријави, коме се подноси пријава, у ком року и којим каналом;
- ✕ **Непријављивање инцидента надлежним органима**, пре свега **Канцеларији Савета за националну безбедност и заштиту тајних**

података, а у одређеним случајевима и **Министарству правде** у складу са законским обавезама;

- ❌ **Покушаји прикривања, одуговлачење са анализом или непотпуно документовање инцидента**, што онемогућава идентификацију узрока и спречавање сличних догађаја у будућности;
- ❌ **Изостанак предузимања хитних мера** ради спречавања ширења последица или компромитације додатних података или система.

📌 **Правовремено, транспарентно и систематизовано поступање у случају инцидента** представља један од основних стубова система заштите тајних података. Овакве процедуре морају бити део Плана заштите тајних података, укључујући и евиденцију свих пријављених инцидената, анализа узрока и извештавање према надлежним институцијама.

🔍 У оквиру **стручног надзора који спроводи Канцеларија СНБиЗТП**, често се као показатељ ниског степена зрелости система уочавају управо овакви пропусти у реаговању, што указује да организација нема унапређен механизам унутрашњег упозоравања и санације ризика.

✅ Успостављање механизама реаговања не представља само формалну обавезу, већ и практичну заштиту организације од интерне одговорности, губитка поверења и угрожавања интегритета целокупног система безбедности података.

5. Одсуство одговорности и дисциплинског поступања

Трећи значајан облик доприноса организације настанку штетног догађаја јесте **непостојање утврђених механизама за покретање дисциплинске, управне или кривичне одговорности у случају пропуста у раду са тајним подацима**.

Организације које не предвиђају јасне поступке за:

- ⚠ **утврђивање личне и функционалне одговорности** лица која су изазвала или омогућила пропуст;
- ⚠ **изрицање дисциплинских мера** у складу са интерним актима и важећим прописима;
- ⚠ **покретање управних или кривичних поступака** у случајевима тежих повреда обавеза у раду са тајним подацима;
- ⚠ **анализу и систематско учење из претходних инцидената**, кроз унапређење процедура и едукацију запослених,

остављају појединце без осећаја одговорности и подстичу понављање истих пропуста.

📌 Одсуство санкционисања ствара амбијент у којем се кршење процедура или немарно поступање са тајним подацима **не доживљава као озбиљан прекршај**, што директно угрожава безбедност целог система.

🔍 Овакав пропуст се редовно идентификује у оквиру **стручног надзора који Канцеларија Савета за националну безбедност и заштиту тајних података спроводи на захтев органа јавне власти**, као део процене ефикасности унутрашњег система контроле и заштите тајних података.

✅ Успостављање система одговорности представља кључни елемент система управљања заштитом тајних података, јер обезбеђује не само превенцију, већ и повратну информацију за стално унапређење заштитних мера.

6. Толерисање културе небезбедног поступања

На крају, али не мање важно, **организација доприноси настанку инцидената уколико не развија и не негује културу безбедности у раду са тајним подацима**. Култура безбедности представља скуп вредности, ставова и навика запослених који доприносе доследној примени мера заштите тајних података у свакодневном раду. Уколико организација занемари овај аспект, јављају се следећи ризични обрасци понашања:

- ⚠ **занемаривање процедура и интерних правила**, која се често доживљавају као пука формалност или бирократска обавеза;
- ⚠ **неовлашћено поступање са подацима**, укључујући ношење тајних података у личним торбама, фотографисање докумената мобилним телефонима или слање поверљивих садржаја путем незаштићених електронских комуникација;
- ⚠ **одсуство система за пријаву пропуста**, као и атмосфере у којој се пријављивање грешака не подстиче већ демотивише;
- ⚠ **толерисање непрофесионалног и нехатног приступа у раду са поверљивим и тајним подацима**, чиме се подривају основни безбедносни принципи.

📌 Изостанак културе безбедности доводи до тога да запослени не препознају озбиљност ризика, не осећају личну одговорност и не поступају у складу са прописаним обавезама.

✅ Успостављање културе безбедности подразумева **лидерски пример руководства, континуирану едукацију, транспарентност у поступању и подстицање одговорног понашања на свим нивоима организације.**

🔍 Ова димензија безбедности такође је предмет **стручне процене у оквиру надзора који Канцеларија Савета за националну безбедност и заштиту тајних података спроводи на захтев органа јавне власти**, при чему се посебно вреднује колико се безбедносне вредности примењују у пракси, а не само у формалним документима.

Допринос организације настанку штетног догађаја у раду са тајним подацима огледа се у пропустима који могу бити присутни на **системском**, **оперативном** и **едукативном** нивоу. Овај проблем се не односи само на појединачне грешке или намерне пропусте појединаца, већ на **целокупни контекст и приступ** који организација има према безбедности података.

Без обзира на карактер конкретног инцидента, одговорност организације се огледа у следећем:

- 🛡 **Стварању услова за безбедан рад са тајним подацима** – То подразумева успостављање система који обухвата све аспекте заштите тајних података, од правних аката до техничких мера;
- 🔧 **Обезбеђивању алата за адекватно реаговање и санкционисање** – Организација мора да има унапред дефинисане процедуре за поступање у случају инцидента, као и механизме за санкционисање пропуста, чиме се ствара систем одговорности и подстицање на пажљиво поступање са тајним подацима;
- 🌱 **Изграђивању културе безбедности** – У оквиру ове културе, безбедност података не представља само техничку или административну обавезу, већ је **професионална и законска одговорност свих чланова организације**. Према томе, изграђивање свести и ставова који подстичу одговорно понашање и континуирану обуку запослених чини основу успешне заштите тајних података.

📌 Ова системска одговорност организације подразумева не само сагледавање инцидената као индивидуалних пропуста, већ и процену да ли организација као целина има постављене механизме који спречавају настанак и ескалацију оваквих догађаја.

🔍 **Процена и надзор**, који спроводи Канцеларија Савета за националну безбедност и заштиту тајних података на захтев органа јавне власти, такође укључује анализу ових аспеката, те **периодичне контроле и савете за унапређење система заштите тајних података**.

8. ЛИСТА ЗА ПРОВЕРУ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Ова листа за проверу служи као **практичан и систематски алат** који омогућава правовремено и ефикасно реаговање у случају инцидента са тајним подацима. Она помаже у одржавању усклађености са правним и оперативним захтевима, као и у стварању осећаја одговорности унутар организације.

📌 1. Идентификација инцидента

Циљ: Брзо и прецизно утврдити основне информације о инциденту и почетне мере реаговања.

☐ Јасан и сажет опис догађаја

☐ Датум и време када је инцидент уочен

☐ Прецизна локација настанка инцидента

☐ Навођење угрожених тајних података (назив, број, степен тајности)

☐ Лица која су била у контакту са тајним подацима

☐ Процена ризика од контакта неовлашћених лица

☐ Утврђење да ли је податак напустио заштићени простор или систем (физички или електронски)

📌 2. Обавештавање надлежних

Циљ: Осигурати правовремено обавештавање свих релевантних институција ради предузимања даљих мера.

☐ Руковалац тајним подацима или овлашћено лице за тајне податке унутар правног лица

☐ Старешина органа или одговорно лице

☐ Орган јавне власти који је одредио степен тајности

☐ Канцеларија Савета за националну безбедност и заштиту тајних података

☐ Надлежно тужилаштво (уколико постоји основ за кривичну одговорност)

☐ Безбедносно-информативна агенција – БИА (ако је потребно)

☐ Обавештавање по препоруци Канцеларије СНБиЗТП (ако је већ издата или се очекује)

📌 3. Утврђивање околности и правна квалификација

Циљ: Расветљавање узрока инцидента, идентификација пропуста и одговорних лица.

☐ Покренута унутрашња (ванредна) контрола

☐ Утврђени узроци инцидента

☐ Процењена штета и потенцијални домет последица

☐ Процена да ли постоје елементи:

☐ Повреде радне дисциплине

☐ Прекршаја

☐ Кривичног дела

☐ Консултација са правним службама или тужилаштвом ради квалификације

☐ Доносена одлука о покретању поступка (дисциплински, прекршајни, кривични)

📌 **4. 🛡 Заштита и санација**

Циљ: Хитно спречавање даљег угрожавања података и побољшање мера заштите.

☐ Онемогућен даљи приступ угроженим подацима

☐ Активиране containment мере (техничке, административне, физичке)

☐ Спроведене привремене и трајне превентивне мере

☐ Одржана обука и издата упутства за запослене

☐ Ажурирана техничка и организациона документација

📌 5. 📝 Извештавање и евиденција

Циљ: Комплетна документација догађаја ради праћења, контроле и системског унапређења.

☐ Сачињен званичан извештај о инциденту

☐ Извештај достављен свим релевантним институцијама

☐ Инцидент евидентиран у:

☐ Регистар инцидената у органу

☐ Регистар у складу са NIS2 директивом (ако је применљиво)

☐ Спроведена анализа са предлозима за унапређење безбедносних мера

☐ Посебна евиденција препорука Канцеларије СНБиЗТП

9. ПРЕПОРУЧЕНЕ МЕРЕ – УСКЛАЂЕНЕ СА ЕУ ПРАКСОМ

Мера	Опис
Обавештавање	У складу са Законом о тајности података, обавештавање надлежних органа мора бити одмах по утврђивању инцидента. Ово укључује изворни орган, Канцеларију СНБиЗТП, БИА (ако је потребно), као и друге релевантне институције. Према GDPR и NIS2, релевантна тела укључују Владу Србије, ЦЕРТ и друге институције информационе безбедности.
Утврђивање околности	Форензичка анализа са детаљном временском линијом, идентификацијом свих угрожених података и евентуалних безбедносних рупа, у складу са Законом о информационој безбедности. Форензичка анализа мора обухватити све аспекте инцидента и утврдити узроке, као и евентуалне пропусте у систему заштите података.
Процена утицаја и ризика	Процена природе података (нпр. одбрамбени, лични, пословне тајне), ризика по права лица (GDPR), као и потенцијалних међународних последица, посебно у контексту ЕУ и НАТО обавеза. Ова процена укључује све аспекте као што су могућност неовлашћеног приступа, могуће оштећење угледа или финансијске последице.
Ограничење штете	Техничке и административне мере као што су блокада приступа, измене лозинки, деактивирање налога, уклањање информација са отворених платформи. Све у складу са прописима о информационој безбедности. Ове мере морају бити имплементиране одмах након утврђивања инцидента и обухватати све системе који су били у ризику.
Извештај и документација	Званични извештај о инциденту мора бити архивиран и доступан надлежним институцијама. Прати га анализа узрока и мера. Чување и евиденција у складу са Законом о тајности података. Извештај треба да садржи све битне податке, као и препоруке за унапређење мера безбедности како би се спречило поновно дешавање сличних инцидената.
Обавештавање страних партнера	Ако су угрожени подаци под контролом ЕУ, НАТО или других страних ентитета, неопходна су обавештења у складу са међународним уговорима и GDPR прописима. Обавештавање мора бити вршено у складу са уговореним процедурама и роковима који се односе на безбедност података у међународним контекстима.

Мера	Опис
● **Обавештавање јавности**	У случају инцидената од јавног значаја, обавештавање мора бити уравнотежено са прописима о слободи приступа информацијама и заштити података. Води се рачуна о степену тајности и могућим последицама по јавни интерес. Прописи о транспарентности и обавештавању јавности треба да буду усклађени са међународним правима и локалним законодавством.

10. Закључна разматрања

Поступање у случају инцидента са тајним подацима представља кључни аспект очувања безбедносне стабилности и институционалног кредибилитета органа јавне власти и правних лица који обрађују тајне податке од значаја за националну безбедност, одбрану, унутрашње и спољне послове. С обзиром на високу осетљивост ових података, од суштинске је важности да свака организација која у свом делокругу рада обрађује тајне податке има јасно дефинисане процедуре, одговорности и механизме поступања у случају настанка безбедносног инцидента.

Полазна основа овог водича јесте применљиви правни оквир, пре свега **Закон о тајности података** („Сл. гласник РС“, бр. 104/2009) и **Закон о информационој безбедности** („Сл. гласник РС“, бр. 6/2016, 94/2017 и 77/2021), који, заједно са пратећим подзаконским актима и интерним општим актима, утврђују обавезу примене мера заштите, обавештавања, поступања и контроле. Овим прописима су утврђене обавезе свих субјеката система, од руковаоца тајних података, преко руководства организација, до самих корисника тајних података.

Посебан значај има примена системских и превентивних мера, као што су дефинисање надлежности у оквиру унутрашњег система заштите тајних података, утврђивање тачних контакт тачака за пријаву инцидената, обезбеђивање техничких и организационих услова за безбедну обраду и складиштење тајних података, као и редовно спровођење обука и провера. Унапређењем интерних аката, евиденција, приступних права и безбедносне инфраструктуре, смањује се вероватноћа настанка инцидената и гради се култура одговорног поступања са свим штићеним подацима, а посебно са тајним подацима.

Оперативни поступци након инцидента морају бити прецизни, ефикасни и усмерени на ограничење штете, спречавање даљег ширења последица, идентификацију узрока и актера, као и обнову безбедносног капацитета. Процес откривања, пријављивања и реаговања мора бити правовремен, а комуникација са надлежним органима, пре свега Канцеларијом Савета за националну

безбедност и заштиту тајних података, обавезна и документована. Спровођење интерне форензичке анализе, преглед техничке и физичке безбедности, као и израда извештаја са мерама за отклањање последица, представљају неизоставан део поступка.

Не мање важно, питање **одговорности и санкционисања** мора бити јасно утврђено. Утврђивање пропуста у примени мера заштите, одговорности лица задужених за чување и обраду тајних података, као и евентуалне намерне или нехатне радње које су довеле до инцидента, морају бити предмет дисциплинских, управних, прекршајних или кривичних поступака, у складу са тежином повреде. Ово представља кључни елемент одржавања правне сигурности и поверења у систем заштите тајних података.

Истовремено, овај водич има за циљ да подстакне и ојача безбедносну свест и културу унутар органа јавне власти. То подразумева не само примену прописаних процедура, већ и подизање свести о значају заштите тајних података на свим нивоима — од највиших руководилаца до извршилаца у систему. Безбедносна култура не постиже се само актима, већ свакодневном применом правила, редовном комуникацијом о ризицима, охрабривањем пријављивања неправилности и континуираном едукацијом.

У том контексту, унапређење система заштите тајних података мора бити континуиран процес, прилагођен технолошком развоју, променама у правном и безбедносном окружењу, као и резултатима из претходно анализираних инцидената. Извештавање, евиденција, анализа и повратне информације треба да служе не само ради испуњења законске форме, већ и као полуга за реално унапређење система.

На крају, увођењем овог водича као обавезног алата у пракси, организације добијају јасну структуру поступања у кризним ситуацијама, али и стабилну основу за изградњу отпорнијег, безбеднијег и одговорнијег система руковања тајним подацима. На тај начин се не штите само тајни подаци, већ и легитимитет, интегритет и оперативна способност целокупног система националне безбедности.